The Dynamics of Military Security – Challenges and Forecasts in the Conditions of Global (in)Security

Rumen Marinov
Security and Defense Faculty
Vasil Levski National Military University
Veliko Tarnovo, Republic of Bulgaria
ramarinoff@gmail.com

***Abstract*— This study focuses on transforming military security in the context of globalization, technological advances, and emerging threats. The concept of "military security" reflects the complex and dynamic nature of the contemporary global security environment, which has evolved from the traditional protection of territorial borders and populations to integrated strategies encompassing new threats, such as cyberattacks and hybrid conflicts. The study examines five key factors shaping new approaches to military security: technological advances, geopolitical dynamics, emerging threats, societal changes, and the need for adaptive and comprehensive solutions. It concludes by emphasizing that contemporary military security requires innovative and global approaches to address the challenges of a dynamically changing world.**

Keywords – military security, globalization, cyberattacks, hybrid conflicts, geopolitical transformations

I.INTRODUCTION

Although the importance of security in the modern world is widely recognized, there is a significant gap in the scientific literature on the interaction between traditional military threats and new, non-traditional challenges (such as cyberattacks, climate change, and hybrid warfare) in the context of global insecurity. Most existing studies consider military security separately from other dimensions, leading to fragmented analysis and limited predictive value in shaping comprehensive security policies.

The present study aims to fill this gap by analyzing the dynamics of military security in global (in)security through a unified approach that includes both classic military aspects and contemporary risks and vulnerabilities.

In the contemporary global context, security occupies a key place, especially against the backdrop of conflicts such as those in Ukraine and the Middle East. Despite the wide academic attention on traditional military security, there is a clear gap in terms of its overall interaction with emerging and non-traditional threats – cyberattacks, climate crises, hybrid warfare, and information impact. Much of the existing literature focuses on individual aspects of security, thus ignoring the complex and interconnected nature of contemporary threats.

The present study aims to overcome this gap by offering a systematic analysis of the dynamics of military security in the context of global (in)security, through an interdisciplinary approach. The study examines the classical military aspects and their interrelation with geopolitical, technological, and environmental factors, which are increasingly becoming catalysts of uncertainty.

II.MATERIALS AND METHODS

The study uses combined methods to analyze military security in the contemporary global context. A literature review of theoretical and empirical sources is conducted, and documents and strategic reports of governmental and international organizations are examined. Case study analyses and comparative analyses of strategies of different countries and organizations provide examples of emerging threats. The Saati method (AHP) is also applied for hierarchical structuring and assessment of the importance of factors affecting the development of sound security strategies such as technological progress, geopolitical changes, and new threats.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8467

III.RESULTS AND DISCUSSION

In the modern world, military security is subject to continuous changes, determined by four interrelated factors depicted in Figure 1.

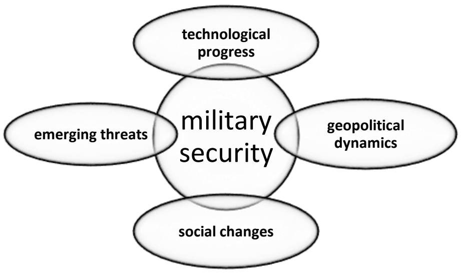

Fig. 1 Challenges to military security

Technologies such as artificial intelligence and autonomous systems are significantly changing the way we wage war and provide defense, expanding both offensive and defensive capabilities. Geopolitical changes are leading to new strategic alliances and shifts in the global balance of power, requiring new approaches to national and international security. The dynamically evolving security environment and the expansion of combat domains increase the degree of uncertainty in military operations [1]. At the same time, emerging threats such as cyberattacks, terrorism, and climate change require integrated strategies that encompass not only military but also economic and social aspects of security. Societal changes, including demographic and political transformations, influence national strategies, emphasizing the need for social stability and effective interaction between the state and citizens. All these factors emphasize the need for complex, global, and adaptive solutions to ensure security in an increasingly unpredictable world.

The first factor – *technological progress* is represented by the rapid development of areas such as artificial intelligence (AI), cyber capabilities, space technologies, and autonomous weapons systems. The modern security environment and dynamic changes on a global scale require the use of alternative and modern methods of conducting and ensuring combat operations in different environments [2]. These innovations are transforming the nature of military security, introducing new forms of warfare and operational approaches. On the one hand, technologies expand the range of potential threats – for example, through cyberattacks or the use of unmanned aerial systems that are programmed to perform tasks that are potentially dangerous to humans but can also be remotely controlled [3]. On the other hand, they provide tools for more effective protection, such as improved early warning systems, cyber defense, and adaptive military strategies. Technological developments also highlight the need for international regulation and ethical standards to avoid escalating conflicts and unmanageable risks.

The second factor – geopolitical dynamics involves the emergence of new centers of power and the formation of alliances that can lead to unforeseen changes in global security. Changes in the balance of power are manifested through the transformation of traditional alliances and the rise of new powers. These processes require a rethinking of strategic approaches to military security, taking into account both cooperation and potential conflicts between states. Successful management of geopolitical changes depends on the ability to anticipate and adapt to new realities on the international stage.

The third factor – *emerging threats* such as cyberattacks, disinformation, terrorism, and climate change require more holistic strategies for military security. These threats not only go beyond traditional military approaches but also require integration between different spheres of security – economic, social, and environmental. Effectively dealing with them implies international cooperation, information exchange, and adaptability to new forms of risks. Protection against these threats includes both technologies and strategic policies that strengthen the resilience of states and societies.

The fourth factor – societal changes, demographic transitions, and political movements – also have a significant impact on priorities and approaches to national security. The increasing importance of social stability as a component of military security highlights the need for a balanced approach to economic and social policy. Demographic changes, such as an aging population or increasing numbers of migrants, can pose new challenges in resource allocation and maintaining public order. Political movements and changes in citizens' perceptions of security may require a readjustment of national strategies to respond to new realities and expectations. Efforts to strengthen social cohesion and build trust between the state and society are becoming increasingly crucial in ensuring the sustainability and effectiveness of military security.

The formula can be expressed as follows:

$$\boldsymbol{S = \sum_{i=1}^{n} wi \,.\, xi} \qquad (1)$$

Where:

- $\boldsymbol{S}$ is the overall assessment of the impact on military security.
- $\boldsymbol{n}$ is the number of key factors**.**

To analyze the impact of these key factors on military security, the formula according to the Saati method can be adapted, which uses the Analytic Hierarchy Process (AHP) for decision-making under multi-criteria situational factors.

$\boldsymbol{wi}$ is the weights, which must satisfy the condition to guarantee normalization, where:

$$\sum_{i=1}^{n} \boldsymbol{wi} = 1 \qquad (2)$$

xi is an estimate of the *i*-th factor (in the range of 1 to 9).

Example: If the factors and their weights are:

- technological progress ($w_1 = 0.3$, $F_1 = 8$),
- geopolitical dynamics ($w_2 = 0.25$, $F_2 = 7$),
- emerging threats ($w_3 = 0.3$, $F_3 = 9$),
- social changes ($w_4 = 0.15$, $F_4 = 6$),

then:

S=(0,3 x 8)+(0,25 x 7)+(0,3 x 9)+(0,15 x 6) = 7,55

This provides a generalized assessment of the impact of factors on military security.

Forecasting the evolving dynamics of military security

Forecasting the dynamics of military security is a complex process that requires the integration of multiple interrelated factors in the context of global and regional changes. In the modern world, marked by increasing uncertainty and constantly evolving threats, military security plays a key role in preserving the stability and sovereignty of states. The dynamics of this area are shaped by emerging factors such as technological advances, the expansion of hybrid conflicts, and the need for global coordination. This task is particularly challenging due to the high degree of uncertainty characteristic of the modern security environment and the possibility of unforeseen events that can significantly affect the global balance of power. The development of military strategies and capabilities is no longer limited to traditional dimensions of force but requires an integrated approach, encompassing innovation, sustainability, and multilateral cooperation.

Challenges defining the future dynamics of military security include: **adoption and deployment of new technologies, hybrid warfare, resilience and adaptability, multi-domain operations, and strategic alliances and partnerships.** These challenges require rethinking traditional approaches to military security and investing in innovation, coordination, and strategic cooperation. This analysis focuses on key aspects of these challenges and explores ways to address them through adaptability and strategic planning.

The Saati method is an effective tool for assessing the importance of different criteria and for determining the strategies that can lead to optimal results in conditions of global (in)security. By comparing each criterion against the others on a predefined scale (e.g. from 1 to 9), the weights of the criteria are calculated. This methodology provides a data-based and objective approach for the analysis and selection of strategies and policies, especially in the context of dynamic military security.

In this example, the method has been adapted to address multi-criteria challenges. The formula has been revised to provide a structured and integrated approach to evaluating different options based on multiple criteria. It can be represented as follows:

$$\boldsymbol{S = \sum_{i=1}^{n} wi\,.\;xi} \qquad (3)$$

where:

– ***S*** is the total score (the value of the alternative against the criteria),

– ***wi*** is the weight of the criterion ***i*** (determines the importance of the criterion in the overall assessment),

– ***xi*** is the evaluation of the alternative against the criterion ***i***,

– ***n*** is the number of criteria.

Example:

Let's consider four criteria for evaluating an alternative in the context of military security (for example, for evaluating a military strategy or system):

1. Technologies (w1) – weight: 0.4
2. Resources (w2) – weight: 0.3
3. Adaptability (w3) – weight: 0.2
4. Coordination (w4) – weight: 0.1

Now let's set the assessments *xi* for each alternative against these criteria (on a scale of 0 to 10, where 10 is the highest score):

1. Technologies (x1): 8
2. Resources (x2): 6
3. Adaptability (x3): 7
4. Coordination (x4): 5

Calculation steps:

1. Multiply each weight ***wi*** by the corresponding value ***xi***.
2. Sum the results to get the total value ***S***.

The calculations are as follows:

S = (0.4×8)+(0.3×6)+(0.2×7)+(0.1×5)
S = 3.2 + 1.8 + 1.4 + 0.5
S = 6.9

The result of the overall security assessment “S” for this alternative is 6.9.

This indicates the overall effectiveness of the strategy or system in relation to the various criteria, with a higher number implying better performance against the listed criteria.

The first challenge that will shape the future dynamics of military security is the adoption and implementation of new technologies. It is one of the most important factors. Innovations in areas such as artificial intelligence, quantum computing, autonomous systems, space technology, and biotechnology are transforming traditional concepts of security while creating new risks and challenges.

The development of autonomous weapons systems, such as drones and autonomous platforms, is changing the nature of warfare, increasing its precision and reducing human risk. The threat of the use of unmanned aerial systems (UAS) in potential combat operations against both friendly and enemy forces is significant. [4]. At the same time, advances in cyber technology are leading to new forms of conflict, including cyberattacks on critical infrastructure, electronic networks, and financial systems. Space technologies, such as surveillance and communication satellites, provide strategic advantages but expand the battlefield with new opportunities for conflict.

New technologies are also significantly improving defense capabilities. Artificial intelligence and machine learning algorithms are helping to analyze large volumes of data, allowing for more accurate threat prediction and real-time decision-making. Advanced early warning systems based on quantum sensors and advanced radars are increasing the accuracy and range of potential risk detection.

Despite these opportunities, the adoption of new technologies comes with several challenges. Ethical and legal issues, such as the use of autonomous weapons or biotechnology for military purposes, raise serious concerns about the accountability and control of lethal technologies. Furthermore, the uneven distribution of access to these innovations exacerbates global imbalances, creating the conditions for asymmetric conflicts, while dual-use technologies, such as drones and cryptography, can easily be used for terrorist purposes.

Predictions about the impact of technology on military security range from optimistic to pessimistic. In the best-case scenario, technology can strengthen international cooperation through information-sharing platforms and joint defense systems, supported by ethical frameworks and international treaties that minimize the risk of abuse. In the worst-case scenario, however, new technologies can provoke arms races in new areas such as space and cyberspace, escalating conflicts and eroding trust between states.

To effectively manage the impact of new technologies, strategies such as investment in research and development to prevent technological monopolies, and the creation of international partnerships and regulations to control autonomous weapons and cyber technologies are needed. Resilient infrastructure, including secure networks and advanced crisis management systems, is also essential.

The conclusion is that new technologies offer enormous potential for improving defense capabilities, but their misuse or lack of effective control can lead to serious global threats. Effective prediction and management of technological innovations will play a key role in maintaining international stability and security.

The analysis shows that the scenario achieves an overall score of 7.2, highlighting its effectiveness, with the technology criterion contributing the most (0.5458). High values for technology and infrastructure highlight the importance of innovation and a stable supporting environment, while coordination and risk management remain areas for improvement. A strategic focus on the deployment of new technologies, combined with resilient infrastructure and international coordination, is key to addressing global challenges, but managing risks and strengthening cooperation between allies require additional efforts to achieve long-term stability.

The second challenge is hybrid warfare. It is a modern form of conflict that combines traditional military actions with unconventional means to achieve strategic goals. It combines elements such as cyberattacks, information operations, economic pressure, the use of mercenaries and terrorist networks, and the manipulation of political processes in opposing states. Hybrid warfare is difficult to predict and extremely effective in achieving asymmetric dominance. It is characterized by multidimensionality, including actions in land, sea, air, space, and cyber domains, as well as the use of economic sanctions, cultural and political pressures, and the manipulation of public opinion. Hybrid tactics are often used by weaker actors against stronger states or alliances, minimizing direct confrontation and relying on indirect methods. Moreover, these conflicts unfold without an official declaration of war, creating a *"gray zone"* in which it is difficult to identify the initiator of the attacks.

Key components of hybrid warfare are cyber operations targeting critical infrastructures such as energy networks, financial systems and communication channels, and cyber espionage to obtain strategic information. Information operations include the dissemination of disinformation, fake news and propaganda that destabilize the political environment and influence public attitudes through social media and controlled media channels. Political manipulation is expressed in support for movements or parties that can divide society or weaken state stability, as well as in undermining trust in democratic institutions through attacks on electoral processes. Economic pressure is applied through sanctions, trade blockades or control over energy resources, and illicit financial flows are used to destabilize the economic environment.

The impact of hybrid warfare on military security is significant. Difficulties in identifying threats and responsible actors make it difficult to formulate an adequate response, while at the same time strengthening the role of non-military means. Effective defense against hybrid attacks requires an integrated approach that includes diplomacy, economic strategies, and cyber defense. Traditional military forces must be complemented by new capabilities for information warfare, cyber defense, and societal resilience.

Countering hybrid threats requires strategies such as strengthening intelligence systems to identify early signs of hybrid attacks and establishing centers for analysis of disinformation and cyber threats. International cooperation is key to sharing information and resources, as well as developing regulations in the field of cyberspace and information security. The resilience of societies can be improved through educational campaigns that raise awareness of disinformation and through enhanced cybersecurity of critical infrastructure. Adaptive military strategies that integrate cyber capabilities and information operations are also crucial.

Hybrid warfare is one of the most complex aspects of modern military security, requiring innovative and adaptive approaches that combine traditional and non-traditional methods of defense. Success in managing hybrid threats depends on an integrated approach by states, effective international cooperation, and the resilience of societies against manipulation and pressure.

The overall score of 7.1 indicates that the strategy for addressing hybrid threats is effective, but with potential for improvement, especially in the areas of international cooperation and economic stability. To increase effectiveness, it is necessary to strengthen international cooperation through better coordination and resource sharing, increase information resilience by strengthening public awareness and improving educational campaigns, and improve economic stability through regulations against illicit financial flows and building backup economic systems.

Next in line are **resilience and adaptabil**ity. They are key concepts for ensuring effective national and international security in a dynamic environment characterized by rapid change and emerging threats. They not only support protection against traditional and hybrid attacks, but also enhance the ability of states and organizations to respond adequately to unforeseen circumstances. Resilience is the ability of a system – whether military, economic or social – to maintain its functionality despite the impact of external shocks. It includes the protection of critical infrastructures such as energy networks, communication and transport systems by implementing backup mechanisms that ensure continuity of operations even in the event of disruptions caused by cyberattacks or physical destruction. Societal resilience is also essential, as it strengthens the preparedness and awareness of the population, increases trust in institutions and promotes social cohesion. In the digital era, cyber resilience is a fundamental component, including the protection of digital infrastructures, rapid recovery from cyberattacks and training of personnel to respond to critical situations.

The importance of resilience is expressed in its ability to minimize damage and ensure rapid recovery from crises, creating a basis for long-term security and stability. This problem did not arise suddenly, and leaders of European and world countries began discussing it several decades ago [5]. On the other hand, adaptability allows for effective coping with new and changing conditions, especially in the context of threats that do not follow traditional models. It includes flexibility of strategies, such as developing scenarios for action in different crises and using *"red teams"* to analyze vulnerabilities and propose innovative solutions. Training and development of military and civilian personnel, as well as the integration of technological innovations such as artificial intelligence and autonomous systems, are important aspects of adaptability. This ability promotes the efficient use of resources and provides a competitive advantage in a complex geopolitical environment.

The synergy between resilience and adaptability is crucial for predicting and managing military security. Resilience provides stability, while adaptability adds flexibility to deal with unforeseen situations. This combination allows for proactively addressing emerging threats, integrating lessons from past crises into future strategies, and strengthening cooperation between institutions, communities, and international partners.

However, several challenges make it difficult to implement resilience and adaptability. These include resource constraints that require significant investments in technology, training, and infrastructure, as well as the lack of effective coordination between different institutions and countries. The complexity of modern threats, such as cyberattacks and disinformation, also places new demands on the development of adequate solutions. Despite these challenges, resilience and adaptability remain fundamental pillars of modern military security, providing both stability in times of crisis and flexibility to respond to complex and rapidly changing threats. Their successful implementation requires coordinated efforts, innovation, and a deep understanding of global dynamics.

The overall score of 7.0 indicates that the resilience and adaptability system is well developed but with potential for improvement in the aspects of cyber resilience, strategy adaptability, and societal resilience. To increase effectiveness, additional investments are needed in protecting digital infrastructures and training personnel, improving strategic adaptability by developing scenarios for different threats and strengthening innovation, as well as measures to increase societal resilience through information campaigns and strengthening trust in institutions. This score highlights the importance of coordinated efforts and an integrated approach to addressing dynamic threats in the modern security environment.

Next in line is Multi-Domain Operations (MDO). They are an innovative and strategic approach to modern military security that responds to the complexity of the modern combat environment. They are based on integration and coordination between different domains – land, air, sea, space, cyberspace, and the information environment – to achieve operational superiority and effective management of resources and actions.

Multi-domain operations reflect the new reality of the global security environment, which includes non-traditional threats such as cyberattacks, disinformation, and hybrid warfare. At the same time, technological advances provide new tools for coordination, and geopolitical dynamics require adaptability and synchronization of efforts.

Cross-domain integration is at the heart of MDO, encompassing the synchronization of actions across domains to achieve operational objectives. The use of advanced technologies such as artificial intelligence, autonomous systems, and extended communication networks contributes to increased efficiency. Network-centric operations create globally connected networks to provide real-time information, facilitating decision-making through integrated data exchange. Flexible strategies allow for adaptation to changing conditions [6] and include a combination of offensive and defensive actions aimed at dominating key domains.

Multi-domain operations provide an operational advantage by accelerating decision-making processes through integrated command and control. They provide a better understanding of the operational environment through synergy between domains. Increased system resilience is achieved through the distribution of resources between domains and backup systems that ensure continuity in the event of failures. MDOs also introduce innovative tactics that include hybrid approaches such as disinformation and cyberattacks, as well as new technologies for dominating space and cyberspace.

Despite the many advantages, multi-domain operations face a number of challenges. Technological complexity requires significant investments in artificial intelligence, autonomous systems, and network connectivity, while vulnerability to cyberattacks and sabotage remains a serious threat. Coordination and integration across different units and domains can be hampered by the lack of unified protocols among allies. Legal and ethical issues are also significant factors, as the use of autonomous weapons and operations in space raises serious moral dilemmas, and the unpredictability of cyber operations can lead to the escalation of conflicts.

The future of MDO includes the integration of artificial intelligence, which will play a key role in data analysis and autonomous systems management. The development of space operations will be critical, including control of satellites and navigation systems and the introduction of new technologies for defense and attack in space. International cooperation will become even more important [7], requiring increased partnership between allies, sharing of resources, and common strategies to address global challenges.

Multi-domain operations offer a new approach to military security management in the context of rapidly changing threats and technologies. They require integration of resources, innovation, and global cooperation while offering the resilience and adaptability needed to cope with the complexity of the modern combat environment. Successful implementation of MDO will determine the ability of states and organizations to ensure their security in the future.

The overall score of 7.0 indicates that Multi-Domain Operations (MDO) is well-developed and effective, but there are areas for improvement, particularly in the use of technology and coordination between allies. To improve effectiveness, it is necessary to invest additional resources in technologies such as artificial intelligence and autonomous systems to increase operational effectiveness, improve coordination and management by developing unified protocols and data exchange between allies, and strengthen international cooperation by building joint strategies and sharing resources. These actions will support the sustainable development of MDO, ensuring the ability to address rapidly changing threats and technological challenges.

In fifth place are strategic alliances and partnerships. They are a fundamental element of the modern concept of military security in the global environment, which is characterized by geopolitical upheavals, technological innovations, and hybrid threats. Effective interaction between states, international organizations, and the private sector plays a key role in maintaining stability and building adaptive security systems.

The role of strategic alliances and partnerships includes stabilizing global and regional security by coordinating military efforts to ensure collective defense and response to threats. Allies create common prevention and response strategies aimed at traditional and non-traditional threats. In addition, resource sharing is achieved by sharing technology, infrastructure, and information, which reduces the individual burden on each country through coordinated financial and human resources. Strengthening interoperability is essential and includes the introduction of common standards and procedures that allow seamless interaction between different military forces, as well as the development of integrated command and control systems based on modern technologies.

Key forms of partnership include intergovernmental alliances such as NATO, which provides collective defense and adapts to new threats through programs such as NATO 2030 [8]. Bilateral and multilateral agreements also play a role in strengthening regional stability. Partnerships with international organizations such as the United Nations and the European Union are implemented to provide peacekeeping missions and conflict management, and participation in global initiatives such as the United Nations Sustainable Development Agenda is linked to addressing climate change as a factor for military security. Private-public partnerships include interaction with technology companies to develop innovations in defense and cybersecurity, creating common platforms for sharing information and raising awareness of threats.

The benefits of strategic alliances include increased readiness through faster response to crises and joint training programs and exercises that improve operational capabilities. The technological advantage provided through joint development and sharing of innovations contributes to strengthening cyber defense through globally coordinated efforts. The geopolitical influence of allies is also enhanced by countering the influence of hostile states through collective action.

Challenges facing strategic alliances include divergence of interests, as differences in national priorities and strategies can lead to internal tensions. Technological and operational differences also exist, as differences in the level of military technology development between allies and difficulties in integrating different platforms and systems can hinder effectiveness. Political instability in member states resulting from changes in political leadership can affect the stability of the alliance and increase the risks of termination of cooperation due to geopolitical pressures.

The future of strategic alliances is predicted to be digitalized and automated through the introduction of real-time data exchange platforms that improve joint planning and response. The use of artificial intelligence for threat analysis and coordination between partners will also play an important role. Expanding partnerships by integrating new members into existing alliances, especially in regions with increased risk of conflict, as well as strengthening cooperation with non-governmental organizations and civil society will be key to stability. Addressing global threats such as climate change, migration crises and hybrid threats will also require the creation of common strategies for cyber defense and the fight against disinformation.

Strategic alliances and partnerships are fundamental to anticipating and managing military security dynamics, providing a platform for collectively addressing the challenges of the modern security environment and strengthening the resilience and adaptive capacity of all participants. The success of these alliances depends on their flexibility, coordination, and ability to adapt to the ever-changing global context.

The overall score of 7.1 indicates that strategic alliances and partnerships have significant potential, but there are challenges related to geopolitical stability and coordination between partners. To increase their effectiveness, it is necessary to reduce the differences in interests and strategies between partners, in order to improve internal coordination and reduce internal tensions. It is also necessary to strengthen the integration of new technologies, such as artificial intelligence and automation, to modernize military systems and improve cyber defense. Strengthening global stability through better geopolitical coordination and active participation in international initiatives to address emerging global threats is of key importance. These actions will increase the effectiveness and adaptability of alliances, ensuring stability and preparedness for future challenges.

Based on the calculations and analysis using Saati's method, **the adoption and implementation of new technologies** in the biggest challenge that determines the future dynamics of military security. The reasons behind this are:

1. **Technological complexity and speed of innovation:** Rapid advances in technologies such as artificial intelligence, quantum computing, and autonomous systems require significant investment, expertise, and time for integration. Military organizations often lag behind the private sector in developing and implementing innovations.

2. **Cybersecurity and vulnerabilities:** New technologies bring with them an increased risk of cyberattacks. Devices and systems based on artificial intelligence or connected via IoT are particularly vulnerable to sabotage, espionage, and manipulation.

3. **Financial constraints:** Implementing advanced technologies requires huge financial resources for research, testing, maintenance, and staff training. For many countries, these costs are difficult to justify, especially with limited budgets.

4. **Operational integration:** Incorporating new technologies requires adapting existing platforms, procedures, and organizational structures. The lack of standards and interoperability among allies further complicates the process.

Conclusions

The diagram visualizes the challenges to military security, with the weights of the factors presented in percentages for clarity. The highest weight is given to the adoption and implementation of new technologies (30%), which highlights their key role. Strategic alliances and partnerships (25%) also occupy a significant place, highlighting their impact on stability and effectiveness. Resilience and adaptability (20%) complement the basic requirements for dealing with the dynamic environment. Multi-domain operations (15%) and hybrid warfare (10%) have lower, but still important, weights. The main conclusion is that the strategic focus should be on new technologies and alliances, as they combine innovation and coordinated efforts to address modern challenges.

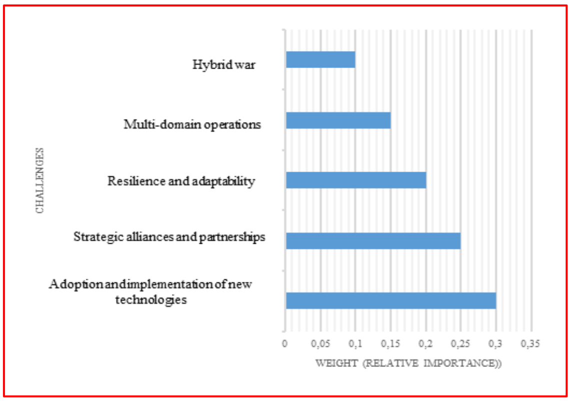

Fig. 2. Comparison of military security challenges.

The conclusion from examining the dynamics of military security in the context of global (in)security is that the future state of military security will be shaped by the ability of states to adapt to the constantly changing environment. Despite growing global threats, such as hybrid conflicts, cyberattacks, and emerging technological risks, there are significant opportunities to strengthen military security through innovation and strategic cooperation. Key factors that will shape the future of military security include the integration of new technologies, a proactive approach to hybrid threats, the development of adaptive and multi-domain systems, as well as strengthening of international cooperation and alliances. The successful integration of these elements will require not only technical and operational readiness but also ethical and legal awareness of new challenges, which will allow for the sustainable formation of stable strategic approaches in the context of global uncertainty.

Acknowledgments

This report is supported by the National Science Program Security and Defense, approved by decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

References

[1] V. Statev, Does combat deployment experience affect the commander’s decision-making process?. Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference. Volume IV. Rezekne, Latvia, 2024. pp. 251-254.

[2] N.Nichev, K. Koynakov, Use of unmanned aircraft in the logistics support of military formations. The Eurasia Proceedings of

Science, Technology, Engineering & Mathematics (EPSTEM), 2024, pp. 92-99.

[3] K. Koynakov, Logistical reconnaissance using unmanned aerial vehicles. Proceedings of the scientific conference "Logistics and social systems". 2021, pp.76-84.

[4] N.Tsvyatkov, System for countering unmanned aerial systems – threat analysis and force protection planning, NMU Annual University Scientific Conference, 2024, pp. 433-443.

[5] N. Dolchinkov, N. Nichev, Gamma-background radiation control systems as a factor of Bulgaria's national security, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume IV, pp 83-88.

[6] N. Dolchinkov, Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, pp. 1-9.

[7] S. Stoykov, Risk management as a strategic management element in the security system, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, March 2019, Article number 8840098, Category number CFP19U17-ART; Code 152084, pp. 156-160.

[8] S.Stoykov, The system of education, training and research in the field of security - managing change through experience and knowledge, ETR, vol. 4, 2024, pp. 269-274.

[9] Nato, [Online]. Available: https://www.nato.int/nato2030/ [Accessed: Feb. 18, 2025].