INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 11, (2026) E-ISSN: 2222-6990

Artificial Intelligence in Modern Hybrid Warfare: from Operational Applications to Strategic Decision-Making

Ana-Maria Severin[1], Ivona Rapan[1], Anamaria - Catalina Radu[1*], Elena Denisa Mateevici[2], George-Aurelian Ghita[2]

[1]Institute of National Economy, Romanian Academy, Bucharest, Romania, [2]Romanian Academy, School of Advanced Studies of the Romanian Academy, Doctoral School of Economic Studies, National Institute for Economic Research ''Costin C. Kirițescu'', Institute of National Economy, Bucharest, Romania

*Corresponding Author Email: anamaria_radu15@yahoo.com

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i11/29332

Published Date: 04 November 2026

Abstract

Artificial intelligence is becoming exponentially crucial in the strategy and execution of modern-day military operations. Its function encompasses intelligence analysis, cyber operations, electronic warfare, surveillance, and decision support in addition to autonomous systems. In hybrid warfare, whilst military and non-military actions are frequently integrated, these applications become particularly relevant. The study explores the impact of artificial intelligence on operational and strategic decision-making in modern hybrid warfare. The study employs an exploratory methodology that is based on a specialty literature review and specific instances from current conflicts. Drones, cyber and electronic warfare, GEOINT and IMINT, misinformation and AI-supported decision systems receive special emphasis. The analysis also considers the manner in which artificial intelligence is able to process massive amounts of data and speed up the OODA cycle. The results imply that AI can facilitate the coordination of intricate activities, enhance situational awareness, and reduce decision-making time. Concerns regarding human oversight, accountability, data reliability, and the dangers of automated decision-making are also raised by its increasing use. The study emphasizes how, in hybrid warfare, the link between human judgment and technical capabilities is evolving.

Keywords: Artificial Intelligence, Hybrid Warfare, Military Operations, Decision-Making, Emerging Technologies

Introduction

There are significant financial, social, political, and environmental consequences associated with military conflicts. They have a significant impact on regional and global economies, resulting in the loss of labor, resources, and production capacities. Neighboring

nations and trading partners may also be affected. Glukh and Honcharenko (2024) define hybrid warfare as a combination of economic, political, cyber, military, and informational means of influence. This kind of warfare is characterized by the use of a variety of tactics, some of which may be non-military and unconventional.

Numerous industries and applications are being transformed by emerging and disruptive technologies, including situations where technology competencies may serve as a strategic advantage. The importance of evaluating services and user satisfaction has also been examined in other sectors, including healthcare education services financed through European funding programmes (Radu et al., 2017). Modern conflicts depend increasingly more on cutting-edge technology to outperform opponents. Drones played a rather minor role at the start of recent conflicts. Their significance grew over time, becoming vital to all parties and influencing changes in military tactics and strategy. Given their operational capabilities and capacity to carry out intelligence, surveillance, and reconnaissance (ISR) operations, drones have proven particularly helpful in hybrid warfare. One popular technology that has the potential to significantly change military conflicts is artificial intelligence. The ability of AI systems to process massive amounts of data quickly is one of their most crucial features. Another vital capability is represented by machine learning that allows existing AI algorithms to develop based on prior completed tasks, outcomes and identified errors. The use of automation technologies can also be observed in other fields, such as marketing, where digital platforms are used to improve customer experience during the buying journey (Dinu et al., 2020).

In modern armed conflicts, AI technology is employed both as software and as a component of hardware systems. It depends on algorithms that, when incorporated into hardware, can allow different devices to carry out tasks independently. AI can facilitate situational analysis and speed up decision-making when used as a software tool. It can facilitate faster target identification and more precise targeting when incorporated into hardware. Thus, AI-based systems can be either software-based or integrated into hardware. Image analysis and recognition systems, including facial and speech recognition are examples of software-based AI. Digital technologies are also used in education, where e-learning platforms have been analyzed in relation to students' satisfaction and their experience during the COVID-19 pandemic (Petrescu et al., 2025).

Among the hardware applications of artificial intelligence are drones and sophisticated robots. According to Stoica (Răpan) et al. (2022), artificial intelligence should be seen as both a general-purpose technology and a greater technological infrastructure that can enable more autonomous, cost-effective and efficient systems.

The Context of the Conflicts

Russia-Ukraine War

Russia's invasion of Ukraine sparked a war that had serious geopolitical and economic repercussions for the entire world, not just the countries directly involved. Additional shocks affected an already fragile global economy following the pandemic, especially in the agricultural and energy sectors. This war represents a hybrid form of state-on-state conflict involving the Ukrainian government and pro-Russian separatist groups. Large parts of the

population are increasingly affected by the conflict's social and economic costs, while the Russian government continues to portray the war as a vital defense of national interests.

The conflict between Russia and Ukraine was influenced by a number of causes that emerged over an extended period of time. Included among these are:

- Ukraine's independence (1991)
- Euromaidan movement (2013)
- Russia's annexation of Crimea and Donbass Region's independence (2014)
- Ukraine's move towards Europe and NATO
- Ukraine's refusal to grant Russia access to its territory
- Russia's invasion in Ukraine (2022)

The origins of the Russia-Ukraine war can be traced back to Ukraine's independence following the 1991 fall of the Soviet Union. In order to preserve the region's balance of power, Russia and the West nations began to compete for influence. The 2013 Euromaidan Movement which took place in the Maidan Nezalezhnosti represented as a public protest against the government's choice to seek deeper connections with Russia and the Eurasian Economic Union rather than negotiate an association agreement with the European Union (Magen & Stein, 2022). Russia's annexation of Crimea in 2014 and the emergence of pro-Russian separatist forces after a controversial referendum that proclaimed the Donbas region's independence from Ukraine marked the start of the two nations' conflict. Russia gained a significant naval advantage in the area after annexing Crimea (Robinson, 2022).

Ukraine's approach to Europe and the North Atlantic Treaty Organization (NATO) is another reason behind Russia's hostile actions toward the country. An attack on a NATO member state is deemed an attack on all NATO members, per Article 5 of the NATO treaty. Consequently, the Russian Federation perceived Ukraine's potential NATO membership as a security threat. Ukraine's refusal to grant Russia access to its territory, including access related to the strategically important Black Sea region and energy routes to European countries, is presented as another factor contributing to the conflict's escalation. The conflict dramatically intensified in 2022, when Russia launched a full-scale invasion of Ukraine on February 24. The invasion can be seen as part of a broader hybrid conflict with significant implications for international law, global politics, and security dynamics (Mankoff, 2022).

Apart from its economic effects, the war has also changed the geopolitical environment. While further isolating Russia from the global scene, the political reaction to the invasion in Europe improved relations between the European Union and the North Atlantic Treaty Organization (NATO). One of the clearest examples of how the conflict has reshaped European security priorities is the accession of Finland and Sweden to NATO (Forsberg, 2023). European countries have also increased their defense spending, demonstrating greater concern about regional security and potential future conflicts. Additionally, their stance on sanctions on Russia has remained properly unified.

The Iranian conflict and the Lebanon War

After a time of rising tensions in the region, the confrontation involving Iran, Israel, and the United States emerged. The 12-day conflict in June 2025 was a significant event. Iran's air defense and nuclear capabilities were impacted during this time. The strategic result was

still unknown, though. A long-term agreement was not reached during the ensuing negotiations. Additionally, Iran demonstrated a comparatively strong ability to withstand political and military pressure (Hokayem, 2026). These incidents set the stage for additional hostilities and military operations in the area.

As military actions grew, the situation became more complicated. The conflict involved the employment of drones, missiles, and airstrikes. The Middle East's broader security landscape was also impacted by these changes. The war was further complicated by tensions between Israel and Hezbollah. Consequently, the conflict was no longer confined to the activities of only two states. It became a component of a larger regional security issue involving many military capabilities and parties (Rupok, 2026). The widespread deployment of missile systems and drones further demonstrates the increasing significance of technology in modern warfare.

The conflict's repercussions extended beyond military actions. They also raised issues with energy and the economy. A large portion of the world's energy traffic goes through the Strait of Hormuz, making it extremely crucial. Oil and natural gas supplies may thus be impacted by military conflicts and attacks on energy infrastructure (Ishtiaq, 2026). This demonstrates how the effects of a military engagement can extend much beyond the battlefield. It could result in an impact on regional stability, energy security, and economic security. At the same time, military actors must analyze more information due to the increasing complexity of these battles. This increases the significance of technology that facilitates quick decision-making, analysis, and surveillance.

Artificial intelligence operational application

Artificial intelligence is becoming a vital tool in contemporary warfare. Increased accuracy and more effective reactions to opponent forces and activities are two examples of how AI is being used in combat. AI is used to monitor areas, assist with decision-making, evaluate vast volumes of data, and identify movements and changes that would be challenging to detect with human resources alone. Its primary objective is to give a thorough operational picture of the battlefield by processing information quickly and reacting to combat conditions that are always changing (Osimen et al., 2024). The primary applications of artificial intelligence in combat are shown in Table 1 below.

Table 1
The use of artificial intelligence in combat

Type	Utilization
Autonomous drones	• provide unprecedented surveillance, intelligence, and precision-strike capabilities • perform intelligence, surveillance, reconnaissance, and target acquisition (ISR) missions (Bahinskyi & Zaiets, 2023) • conduct electronic warfare by jamming and deceiving enemy radar, electronic systems, and air defenses (Kunertova, 2023)
Cyber warfare	• AI tools play an important role in reshaping offensive and defensive operations by introducing unprecedented speed, scale, and automation • algorithms can autonomously identify network vulnerabilities and adapt malware code in real time to bypass security systems

	• phishing campaigns and deepfakes can be created using generative AI tools, such as language models
Electronic warfare	• artificial intelligence is capable of enabling rapid signal processing, adaptive jamming, and autonomous decision-making • it plays an important role in protecting communication systems • machine learning can classify radar signatures, identify jamming techniques, and detect spoofing or intrusion attempts with greater precision
Disinformation	• artificial intelligence algorithms and machine learning proved particularly useful in the Russia-Ukraine war due to their ability to generate and intensify misinformation • algorithms embedded in social media platforms are used to determine the type of content displayed, as well as the most widely viewed posts, which can lead to a distorted perception of events
Imagery analysis	• artificial intelligence can analyze satellite imagery to detect military units, thus providing a significant advantage against enemy forces • examples of such applications include the Ukrainian Kropyva software and Reface
FPV drones	• the FPV drones used by Hezbollah are difficult to detect because they fly at low altitudes and use a wired connection that cannot be easily tracked or jammed by Israeli forces • their operation relies on a thin optical fiber cable that connects the drone to the operator and allows the operator to view and track ground targets. This tactic was previously used in the war in Ukraine
GEOINT and IMINT	• GEOINT (Geospatial Intelligence) and IMINT (Imagery Intelligence) are two highly complementary disciplines concerned with intelligence gathering based on visual data and Earth observation • GEOINT can be used in national security operations, reconnaissance, and disaster response • IMINT is a sub-discipline and a key component of GEOINT
Anti-missile networks	• AI serves as a core component of modern anti-missile systems • defense systems such as Iron Dome are able to rapidly detect and intercept threats • AI-enhanced systems such as Habsora and Lavender support target identification and strike planning

Source: authors

Artificial intelligence is a broad branch of computer science that deals with the creation of machines able to replicate human behaviors such as learning and decision-making (Tableau, 2024). The effectiveness of autonomous drones is supported by their ability to avoid detection and destruction by conventional air defense systems. AI is a crucial technology for UAV autonomy and allows them to navigate without human intervention. UAVs can detect objects captured by their onboard cameras and autonomously assess sensor data and dynamic situations by using machine learning algorithms (Chávez & Swed, 2023). The kill chain in cyberattacks is a series of steps necessary for an attacker to successfully enter a network and acquire data from it (Muller, 2025). AI was extensively incorporated into the kill chain during the joint US-Israeli military attack against Iran, making it the first major conflict to use AI as a fundamental operational element (Ruiz, 2025). AI-driven technologies are crucial for safeguarding the country's cyber infrastructure, but they can also make cyberattacks more sophisticated and rapid. This paradox illustrates the dual nature of AI, in which a technological

instrument can be used both to support national security and to undermine it by enabling autonomous cyber weapons and disruptive operations (Olakunle et al., 2024). Artificial intelligence is seen as a crucial part of mobile electronic warfare (EW) systems deployed with military formations given to its intrinsic computing and decision-making capabilities. AI can also be used in areas including danger recognition, jammer identification, emitter categorization, emission and signal regulation, and signal recognition (Gannon, 2023). The ability of artificial intelligence to recognize and categorize targets using radar signatures is another significant use of AI in EW. By comparing radar signatures from a target with prior samples kept in a database, AI algorithms are able to detect and categorize the relevant target. The possibility of generating counterfeit materials makes disinformation particularly useful for cognitive warfare and operational purposes, as fake images, audio, and text materials can be extremely difficult, or even impossible, to distinguish from authentic content.

Strategic propaganda and disinformation campaigns have shifted towards social media as the main distribution channel for reaching large audiences. In this context, trust and privacy represent important aspects of social media use, particularly considering the growing role of these platforms in the online environment (Radu et al., 2016). Thus, the digital ecosystem became increasingly flooded with disinformation as the war progressed (Virtosu & Goian, 2024). Reface is a Ukrainian AI-based company that adapted critical tools such as computer vision and neural networks to process and recognize objects in satellite imagery. Therefore, it plays a vital role in geospatial intelligence and in identifying Russian troop movements. Kropyva is a widely used tactical-level C2 and intelligent mapping software among the Ukrainian Armed Forces. Its primary function consists of integrating a wide range of systems into one cohesive operation. Additionally, by utilizing a network of satellites and radio frequencies, it can assist in the management of Ukraine's airspace. It became a game-changer due to its ability to streamline communication, improve targeting, and enhance coordination across different units (Pardo de Santayana, 2024). First Person View (FPV) technology originated in military and surveillance applications for unmanned devices and intelligence gathering using drones. This technology allows users to receive real-time visual information remotely through devices or video feeds.

Within the Lebanon war, Hezbollah uses FPV drones to conduct attacks against Israel Defense Forces (IDF) targets in northern Israel and Lebanon. The group claimed, with video evidence, that this type of drone successfully hit an Iron Dome battery in May 2026. The authenticity of the video was not contested by military sources (Jerusalem Post, 2026). GEOINT is utilized in security-related activities through imagery and geospatial information. It integrates imagery, imagery intelligence, and geospatial information (Yusfan et al., 2021). GEOINT can incorporate AI into data processing and analysis, leading to the emergence of a new term, Geospatial Artificial Intelligence (GeoAI). It integrates AI to solve problems of a geographic nature (Wang et al., 2024). Imagery Intelligence, or IMINT, comprises representations of objects obtained from sources such as photographs, radar sensors, and electro-optical systems (Kovarik, 2011). Today, Imagery Intelligence involves different types of technology, such as military aircraft, missile defense systems, infrared cameras, satellites, and drones (Sadulski, 2025). Israel has extensively deployed artificial intelligence technologies in its defense and offensive systems, thus minimizing the need for human intervention and speeding up operations.

Several IDF officials have acknowledged the use of artificial intelligence tools for intelligence analysis and streamlined C2 (Mimran et al., 2024). Iron Dome is a weapon system that is able to detect, analyze, and intercept a variety of short-range threats, such as missiles, artillery, and mortars. It features a multi-purpose launcher designed to fire a variety of interceptor missiles (Patil et al., 2025). Habsora and Lavender are AI-based decision-support systems used in target identification and attack planning. They analyze data from UAVs, satellite images, and other intelligence sources. AI is also used in loitering munition systems. Israel's Harop system, which uses artificial intelligence to strike a target on its own, is one example. Its primary goal is to avoid inaccurate targeting (Duz & Kocakoglu, 2025).

Strategic implications of AI utilization

Among the capabilities of artificial intelligence are the ability to process large amounts of data, effective decision support, situational awareness, and predictive analysis of future scenarios (De Spiegeleire et al., 2017). Artificial intelligence can significantly reduce the time between the stages of the OODA (Observe → Orient → Decide → Act) loop, as shown in the table below.

Table 2
The role of AI in speeding the OODA Loop

Stage	Role
Observe	• automated analysis of satellite and video images • target identification via computer vision • real-time monitoring of drones and sensors • detection of anomalies in communications and radar
Orient	• intelligence fusion • predictive analysis • rapid threat assessment
Decide	• tactical recommendations • target prioritization • rapid scenario simulations • estimation of an operation’s probability of success
Act	• coordination of autonomous drones • intelligent munitions guidance • automated threat response • synchronization of combat systems

Source: authors

Traditionally, in the first stage of the OODA loop, Observe, information gathering was performed by humans through visual recognition and manual analysis. An example of implementing AI at this stage is an AI algorithm that can identify an armored vehicle from thousands of images collected by drones in seconds, compared with the minutes or even hours required by a human analyst. In the Orient or Analyze stage, the gathered information is interpreted and correlated. An example of AI use at this stage is that commanders can receive a near real-time operational picture without the delays generated by manual analysis.

An example in the Decide stage is that AI systems can suggest the most efficient allocation of artillery or drones based on battlefield data. Therefore, decision-making time can be reduced from tens of minutes to a few seconds or minutes. An AI-assisted anti-drone

system can identify, categorize, and eliminate a danger nearly quickly during the Act stage. At this level, the primary strategic implication is that the actor that completes the OODA cycle more quickly can attain operational dominance by responding ahead of the adversary, interfering with their decision-making process, and keeping the initiative on the battlefield.

AI converts information speed into military strength in modern-day wars. Furthermore, human involvement in the OODA loop is not eliminated by artificial intelligence; rather, it is shifted from direct analysis to strategic oversight and validation. Additionally, AI increases the amount of information processed and decreases the time between steps. Artificial intelligence has a lot of potential, but it also has limitations, like its need for large training datasets and vulnerability to manipulation by adversaries. For instance, AI algorithms become vulnerable to mistakes that could result in unintentional escalation in denied environments where adversaries can purposefully produce false signals. Furthermore, human oversight and legal accountability may be complicated by the black-box aspect of many AI models, especially deep neural networks.

AI-based systems can effortlessly handle and analyze the massive amount of data that can be found on the modern battlefield. Artificial intelligence will be incorporated into future decision-support systems to improve ISR capabilities. The potential of artificial intelligence to assist commanders in making operational decisions is one of its promises. On a battlefield that is becoming more complex and fast-paced, they must continuously monitor, orient, make decisions, and take action. Sophisticated instruments that can aid in military planning and assist in anticipating enemy movements have consistently been necessary.

In the end, this has resulted in the development of numerous applications, including early warning systems. Artificial intelligence can significantly improve military decision-making, but it should not be taken for granted because machines are still unable to fully comprehend the intricacies of warfare. DSS can speed up decision-making and cut down on the number of individuals needed to do specific activities, but it can also put pressure on military leaders to accomplish more with fewer resources. Artificial intelligence and autonomous systems may speed up some decisions, but its application should be calibrated based on contextual hazards and the caliber of the tools and procedures being used.

Although AI-DSS is a potential future path, there are concerns associated with it. Reducing technological risks is essential, and there are numerous ongoing initiatives to enhance AI systems from a technical standpoint. But when it comes to making sure AI systems are used properly and in accordance with the law, human actions continue to be the final line of defense.

Conclusions

By reducing processes that would often take hours or days to minutes or, in certain situations, seconds, artificial intelligence can shorten the military's decision-making cycle. As discussed earlier in the paper, AI is capable of conducting electronic warfare, protecting and attacking cybersecurity networks, precisely identifying and classifying targets, creating and intensifying disinformation, providing advanced capabilities like surveillance, intelligence, and precision strikes, and acting as a key part of contemporary anti-missile systems. Furthermore, artificial intelligence is frequently employed to quickly produce, spread, and magnify fake

propaganda and misinformation, thereby influencing public opinion and eroding confidence in democratic institutions. The goal of artificial intelligence applications is to establish an efficiently networked battlefield where deployed forces and platforms are connected by data that moves very quickly. In conclusion, because of its many uses, artificial intelligence has emerged as a crucial tool in contemporary combat.

The integration of artificial intelligence into current military operations has led to a series of changes in terms of analysis, planning, and decision-making. Currently, AI is not only used to automate various activities. It is also used to enable decision-makers to make use of the information it provides. In hybrid warfare, artificial intelligence plays a very important role, as it helps process information quickly and provides solutions that can be implemented more rapidly. However, it is important to distinguish between the existing capabilities of AI and its potential future benefits. While AI is already used for image analysis, surveillance, and decision support, its ability to provide long-term strategic advantages remains dependent on several factors, including data quality, system reliability, and human involvement in decision-making. Regarding the main limitations of the research, it should be noted that one limitation is related to the exploratory nature of the study. The study analyzed the specialized literature and briefly presented a series of examples from current military conflicts. Thus, the absence of empirical research does not allow for a precise measurement of the impact of artificial intelligence on the effectiveness of military decisions. Furthermore, the study does not allow for the establishment of direct causal relationships between the use of this technology and operational success. Moreover, this research only analyzes current military conflicts without making a comparison with those that took place in previous periods.

Considering these limitations, it should be noted that future studies should analyze in greater detail how AI can influence strategic decision-making processes in hybrid warfare. Thus, one of the first aspects that should be analyzed is how AI-based decision support systems influence the duration of the OODA cycle. Furthermore, a series of comparative studies should be conducted in the future to examine how these technologies are used in different conflicts. Their purpose would be to illustrate how operational advantages can be transformed into demonstrable strategic benefits. Future research in this field should also examine the main risks arising from the interaction between autonomous systems, cyber operations, and disinformation campaigns. Moreover, these studies should also examine possible ways to prevent unintended escalation. Another important aspect is related to human oversight and accountability in AI-assisted military decision-making. Although AI systems can process information and provide recommendations quickly, human involvement remains essential, especially when decisions may have serious consequences. Errors in data analysis or excessive reliance on automated systems may lead to incorrect decisions and increase the risk of conflict escalation.

Considering the aspects analyzed in this paper, it should be noted that the integration of AI into military strategies should not be examined only from the perspective of technological efficiency, but also in terms of the ethical and international security implications associated with its use.

References

Bahinskyi, A., & Zaiets, O. (2023). Strategies of the sides in the Russia-Ukraine war. *Defence and Strategy, 23*(2). https://www.ceeol.com/search/articledetail?id=1203645

Chávez, K., & Swed, O. (2023). Emulating underdogs: Tactical drones in the Russia-Ukraine war. *Contemporary Security Policy, 44*(4), 592–605. https://doi.org/10.1080/13523260.2023.2257964

De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial intelligence and the future of defense*. https://www.researchgate.net/publication/316983844_Artificial_Intelligence_and_the_FuturF_of_Defense

Dinu, D. M., Radu, A.-C., & Văduva (Ene), L. (2020). Using marketing automation platforms to enhance customer experience during the buying journey. In Proceedings of the 32nd EBES Conference (Vol. 2, pp. 1106–1116). Istanbul, Turkey.

Duz, S., & Kocakoglu, M. S. (2025). *Deadly algorithms: Destructive role of artificial intelligence in Gaza war*. https://media.setav.org/en/file/2025/02/deadly-algorithms-destructive-role-of-artificial-intelligence-in-gaza-war.pdf

Forsberg, T. (2023). Finland and Sweden's road to NATO. *Current History, 122*(842), 89–94. https://doi.org/10.1525/curh.2023.122.842.89

Gannon, B. P. (2023). Implement AI in electromagnetic spectrum operations. *Proceedings*. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2023/august/implement-ai-electromagneticspectrum-operations

Glukh, M., & Honcharenko, M. (2024). The essential understanding and nature of the concept of "hybrid warfare" in the modern doctrine of international law. *Irpin Law Journal: Scientific Journal, 1*(14), 197–205. https://doi.org/10.33244/2617-4154-1(14)-2024-197-205

Hokayem, E. (2026). The war against Iran. *Survival, 68*(2), 41–48. https://doi.org/10.1080/00396338.2026.2647633

Ishtiaq, A. (2026). From oil shock to health crisis: Pakistan's mediation in the US-Israel-Iran war—An international relations analysis. *The Health Sciences AUS, 13*(1). https://healthsciencesaus.com/journal/index.php/HSA/article/view/65

Jerusalem Post. (2026). IDF chief Zamir says military has 'solutions ready' to Hezbollah's FPV drone threat. *The Jerusalem Post*. https://www.jpost.com/israel-news/defense-news/article-897758

Kovarik, V. (2011). *Imagery intelligence (IMINT)*. University of Defence. https://www.researchgate.net/profile/Vladimir-Kovarik/publication/270686775_Imagery_intelligence_IMINT/links/59c6b1620f7e9bd2c00f4722/Imagery-intelligence-IMINT.pdf

Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy, 44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

Magen, Z., & Stein, S. (2022). *The Ukraine crisis: An interim analysis*. Institute for National Security Studies. https://www.jstor.org/stable/resrep39807

Mankoff, J. (2022). *Russia's war in Ukraine: Identity, history, and conflict*. Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep40567

Mimran, T., Pacholska, M., Dahan, G., & Trabucco, L. (2024). Israel–Hamas 2024 symposium—Beyond the headlines: Combat deployment of military AI-based systems by the IDF.

Lieber Institute for Law & Warfare. https://lieber.westpoint.edu/beyond-headlines-combat-deployment-military-ai-based-systems-idf/

Muller, L. P. (2025). Cybersecurity in practice: The vigilant logic of kill chains and threat construction. *European Journal of International Security, 10*(2), 231–251. https://doi.org/10.1017/eis.2024.27

Olakunle, A. A., Chinwe, C. O., Onyeka, C. O., Chuka, A. A., & Obinna, D. D. (2024). Review of AI and machine learning applications to predict and thwart cyber-attacks in real-time. *Magna Scientia Advanced Research and Reviews, 10*(1), 312–320. https://doi.org/10.30574/msarr.2024.10.1.0037

Osimen, G. U., Newo, O., & Fulani, O. M. (2024). Artificial intelligence and arms control in modern warfare. *Cogent Social Sciences, 10*(1). https://doi.org/10.1080/23311886.2024.2407514

Pardo de Santayana, J. (2024). *Artificial intelligence and the war in Ukraine*. In *Artificial intelligence in geopolitics and conflicts* (IEEE 81/2024). Spanish Institute for Strategic Studies. https://www.defensa.gob.es/documents/2073105/2278118/la_inteligencia_artificial_y_la_guerra_de_ucrania_2024_dieeea81_eng.pdf

Patil, A. V., Naik, O. Y., & Patil, P. S. (2025). Advanced integrated missile defense system "IRON DOME". *International Journal of Research Publication and Reviews, 6*(5), 416–423. https://ijrpr.com/uploads/V6ISSUE5/IJRPR44565.pdf

Petrescu, G. D., Preda, A. L., Radu, A.-C., Ulmet, L.-A., & Radu, A. V. (2025). Evaluating medical students' satisfaction with e-learning platforms during the COVID-19 pandemic: A structural equation modeling analysis within a multimodal educational framework. Social Sciences, 14(3), 160. https://doi.org/10.3390/socsci14030160

Radu, A.-C., Orzan, M. C., Dobrescu, A.-I., & Arsene, O. (2016). The importance of trust and privacy in social media. International Journal of Academic Research in Economics and Management Sciences, 5(2), 57–66.

Radu, A.-C., Orzan, M. C., Ceptureanu, S., & Stoica, I. (2017). User satisfaction regarding healthcare education services financed through the European Social Fund. Journal of Economic Computation and Economic Cybernetics Studies and Research, 51(1), 89–102.

Robinson, P. (2022). The Russia-Ukraine conflict and the (un)changing character of war. *Journal of Military and Strategic Studies, 22*(2). https://jmss.org/article/view/76588

Ruiz, A. (2025). The future of war: Kill-chain supremacy and Ukraine's lessons. *Journal of Strategic Security, 18*(4), 53–63. https://doi.org/10.5038/1944-0472.18.4.2592

Rupok, R. (2026). *The 2026 US-Israel-Iran war: Divergent strategies, information warfare, and a fractured West Asia*. SSRN. https://ssrn.com/abstract=6447919

Sadulski, J. (2025). What is IMINT? How it works and why it's useful for security. *American Public University*. https://www.apu.apus.edu/area-of-study/intelligence/resources/what-is-imint/

Stoica (Răpan), I., Zaman, G., Suciu, M. C., Purcărea, V. L., Jude, C.-R., Radu, A. V., Catana, A., & Radu, A.-C. (2022). A better integration of industrial robots on Romanian enterprises and labour market. *Applied Sciences, 12*(12), 6014. https://doi.org/10.3390/app12126014

Tableau. (2024). *The ultimate guide to artificial intelligence (AI): Definition, how it works, examples, history, & more*. https://www.tableau.com/data-insights/ai/what-is

Virtosu, I., & Goian, M. (2024). Disinformation using artificial intelligence technologies—A key component of Russian hybrid warfare. *Smart Cities International Conference (SCIC) Proceedings, 11*, 197–222. https://scrd.eu/index.php/scic/article/view/493/455

Wang, S., Huang, X., Liu, P., Zhang, M., Biljecki, F., Hu, T., Fu, X., Liu, L., Liu, X., Wang, R., Huang, Y., Yan, J., Jiang, J., Chukwu, M., Naghedi, R. S., Hemmati, M., Shao, Y., Jia, N., Xiao, Z., & Bao, S. (2024). Mapping the landscape and roadmap of geospatial artificial intelligence (GeoAI) in quantitative human geography: An extensive systematic review. *International Journal of Applied Earth Observation and Geoinformation, 128*, 103734. https://doi.org/10.1016/j.jag.2024.103734

Yusfan, M. A., Supriyadi, A. A., Martha, S., Gultom, R. A. G., & Sakti, S. K. (2021). Geospatial intelligence (GEOINT) as a national defense strategy for information overload in Indonesia. *International Journal of Engineering Technology and Natural Sciences, 3*(2), 56–62. https://doi.org/10.46923/ijets.v3i2.129