Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

Deep Learning in Military Applications: Threats and Opportunities

Jerzy SURMA
jerzy.surma@sgh.waw.pl
https://orcid.org/0000-0002-5544-2573
Warsaw School of Economics, Warsaw, Poland

Received: 20 November 2023 | Revised: 10 April 2024
Accepted: 10 April 2024 | Available online: 26 June 2024

Abstract

The latest advancements in Artificial Intelligence, especially in Deep Learning technology, accelerate innovation and development in different application domains. The development of Deep Learning technology has profoundly impacted military development trends, leading to major changes in the forms and models of war. In this paper, we overview Deep Learning's history and architecture. Then, we review related work and extensively describe Deep Learning in two primary military applications: intelligence operations and autonomous platforms. Finally, we discuss related threats, opportunities, technical and practical difficulties. The main findings are that Artificial Intelligence technology is not omnipotent and needs to be applied carefully, considering its limitations, cybersecurity threats and a strong need for human supervision in the OODA decision loop. Certain safeguard mechanisms are required at the strategic decision-making level. In this context, one of the most important aspects relates to the education, training and selection of military officer personnel.

Keywords: Artificial Intelligence, Deep Learning, Military Applications.

1. Introduction

Artificial Intelligence (AI) is a comprehensive technology involving psychology, cognitive, information, system, and biological science. Since the concept of AI was first proposed by John McCarthy at the Dartmouth Conference in the summer of 1956 (Hyman, 2012), AI technology has entered a new period of high-speed growth and is recognized as the most likely disruptive technology to change the world in the future.

The success of AI applications has inspired an active exploration by a vast number of military researchers. The world's military powers foresee the broad application prospects of AI technology in the military field and believe that a future arms race will take place in the context of intelligent competition. In the near future, AI will play the "Intelligent Decision Center" role in the Observation, Orientation, Decision, and Action (OODA) cycle because of its maturity and increasing reliability. This growing importance of AI is self-evident, and the contribution of an intelligent command system will surpass the classical approaches. Using AI and other related technologies can reduce the time consumed by the whole OODA loop, and the goal of command and control in multi-domain joint operations can be achieved.

In the following section, we begin with an analysis of the technological development of the most successful subfield of AI, i.e., Deep Learning (DL). Then, we review the DL military application and, finally, discuss its potential threats and opportunities.

2. Deep Learning

As it was already mentioned, a subset of Artificial Intelligence (AI), called Machine Learning (ML), has revolutionized several fields since the 1950s. The most important subfield of ML is Convolutional Neural Networks (CNN). The CNN approach is commonly

Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

known as Deep Learning (DL), and we will use this well-recognized term in this paper. Since its inception, DL has been showing outstanding success in a huge variety of application domains. Figure 1 shows the taxonomy of AI technologies, including DL.

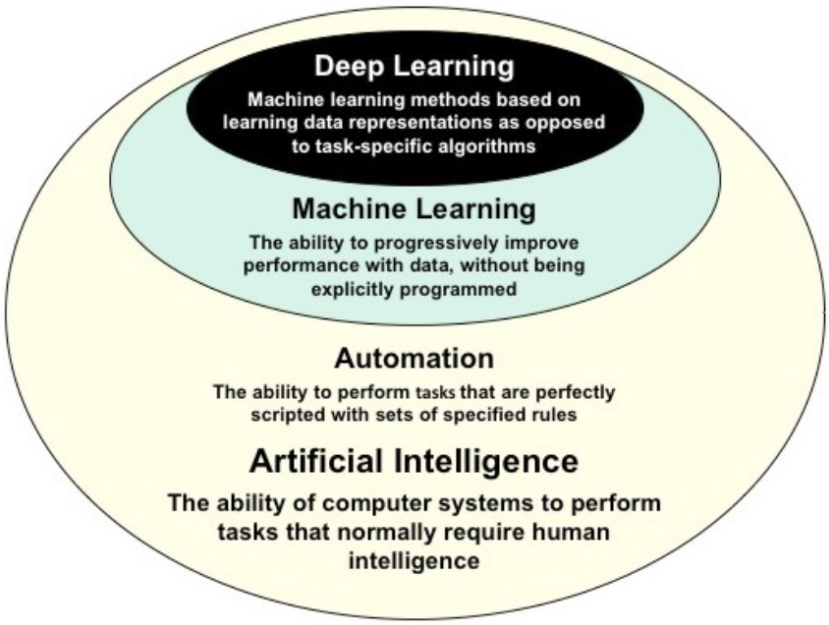

Figure 1. The taxonomy of Artificial Intelligence Technologies
Adopted from: "Military applications of artificial intelligence"
by F. Morgan. Copyright 2020 by the Publisher.

DL's architecture was first proposed by Fukushima (1988). It was not widely used due to the limited computing hardware used to train the network. In the 1990s, Denker and LeCun (1990) applied a gradient-based learning algorithm to CNNs and obtained successful results for the handwritten digit classification problem. After that, researchers further improved CNNs and reported state-of-the-art results in many recognition tasks. CNNs are mainly trained with the use of a gradient-based learning algorithm and suffer less from the diminishing gradient problem. Given that the gradient-based algorithm trains the entire network to minimize an error criterion directly, CNNs can produce highly optimized weights.

Figure 2 shows the overall architecture of CNNs consisting of two main parts: feature extractors and a classifier. In the feature extraction layers, each layer of the network receives output from its immediate previous layer as its input and passes its output as input to the next layer. The CNN's architecture combines three types of layers: convolution, max-pooling, and classification. There are two types of layers in the low and middle levels of the network: convolutional layers and max-pooling layers. The even-numbered layers are for convolutions, and the odd-numbered layers are for max-pooling operations. The output nodes of the convolution and max pooling layers are grouped into a 2D plane called feature mapping. Each layer's plane is usually derived from the combination of one or more planes of the previous layers. The nodes of a plane are connected to a small region of each connected plane of the previous layer. Each node of the convolution layer extracts the features from the input images by convolution operations on the input nodes (Alom et al., 2018).

The entire DL story began to spread worldwide when Professor Geoffrey Hinton and his two PhD students decided to participate in the ImageNet Competition (Krizhevsky et al., 2012). ImageNet is a dataset of over 15 million labeled high-resolution images belonging to roughly 22,000 categories. The images were collected from the web and labeled by human labelers using Amazon's Mechanical Turk crowd-sourcing tool. Starting in 2010, an annual competition called the ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) has been held. ILSVRC uses a subset of ImageNet with roughly 1,000 images in each of 1,000 categories. In all, there are roughly 1.2 million training images, 50,000 validation images and 150,000 testing images (Krizhevsky et al., 2017).

Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

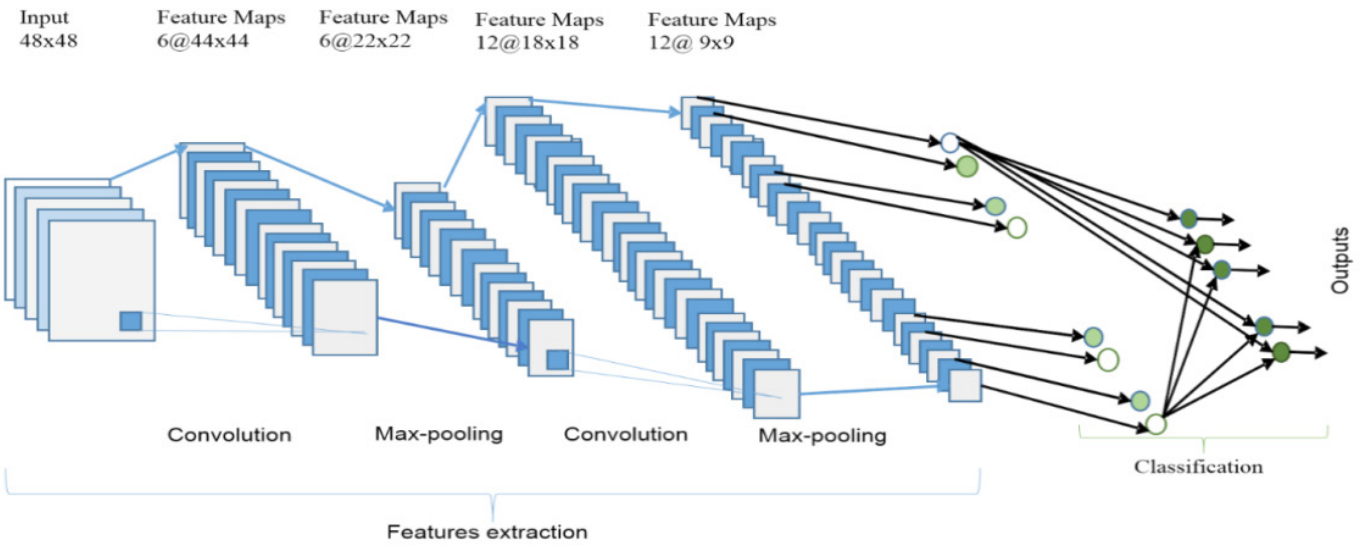

Figure 2. The taxonomy of Artificial Intelligence Technologies
Adopted from: "The history began from AlexNet: A comprehensive survey on deep learning approaches" by M. Alom. Copyright 2018 by the Publisher.

Russakovsky et al. (2015) explained the ImageNet dataset and the state-of-the-art accuracies achieved during the first years. AlexNet received a 16.4 error rate in 2012 (Krizhevsky et al., 2012), and only after three years, the ResNet-152 architecture showed a 3.57% error rate (Zhang et al., 2016), which is better than human error for this task at 5%. This was a crucial moment in the history of DL when image recognition based on an algorithm outperformed human beings. The critical history of ImageNet as an exemplar, utilizing critical discourse analysis of major texts around ImageNet's creation and impact is presented in Denton et al.'s paper (2021).

3. Related Work

In recent years, AI has been successively launched in a large number of machine learning technology research projects, exploring and developing related technologies for military applications. The main goal was to solve the problems of battle field attack, deterrence, and defense algorithmically to achieve the goals of gaining victory in war and serving political aims.

According to Wang et al. (2020), between 2015 and 2019, crucial projects and investments in AI military applications were carried. In 2015, the US military launched the "Commander's Virtual Staff'' program, which provides decision-making support for army commanders and their staff in the process of making operational plans (Seffers, 2016). In 2017, a project called Maven was proposed (Long, Zhou, 2017), which focused on tapping the enormous potential of AI algorithms for situational awareness, intelligence analysis, command, decision-making, and combat action. The US Department of Defense regards AI and autonomy as two technical pillars of the new offset strategy (Yi-Ming, Hai-Ming, 2016) and have kept up with the application of machine learning technologies in decision support (Merket et al., 2015). Starting in 2018, DARPA decided to invest two billion US dollars to reshape the application of AI technology in the military over the next years in a project called "AI Next" (Tadjdeh, 2019). In 2019, US Army invested 72 million dollars in AI and DL projects with many universities to study AI technology in the military to greatly improve combat effectiveness by enhancing soldiers' capabilities, optimizing operational guidance, improving agility and reducing casualties (Layton, 2021).

A comprehensive review of AI/DL military applications was done by Svenmarck et al. (2018) and Masuhr (2019). More recent investigations on military applications of AI were presented by Wang et al. (2020) and Szabadföldi (2021).

Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

4. Review of Military Applications

4.1. Military Intelligence

The origin application of DL is image classification tasks. Firstly, the state-of-the-art deep learning systems in real-life image recognition are described in Rawat and Wang's paper (2017). From a military perspective, one of the crucial applications is satellite imagery. These applications require manually identifying objects and facilities in the imagery (Pritt, Chern 2017). A representative example is a multi-spectral satellite imagery understanding by means of convolutional neural networks (Mohanty et al., 2020).

It is possible to perform image classification based on the images generated by side-scan sonar technology, which allows situational awareness under the water. Research on the automatic analysis of sonar images has focused on classical, i.e., non-deep learning based, approaches for a long time (Steiniger et al., 2022). In recent years, however, the application of Deep Learning in this research field has grown constantly. The broad overview of past and current research involving deep learning for feature extraction, classification, detection and segmentation of side-scan and synthetic aperture sonar imagery is presented by Neupane et al. (2020).

It is not well known that deep learning models might be applied directly to a passive sonar signal classification of military data. The noise radiated from ships can be used for their identification and classification using passive sonar systems**.** Several techniques have been proposed for military ship classification based on acoustic signatures, which can be acquired through controlled experiments performed in an acoustic lane. The cost for a such data acquisition is a significant issue since the ship and crew have to be dislocated from the fleet (Fernandes et al. 2022).

Such advancements give the opportunity for extensive multimodal and multiple intelligence, where structured sensor and unstructured audio, video and textual ISR (Intelligence, Surveillance, and Reconnaissance) data are generated by numerous air, ground, and space-borne sensors along with human intelligence. Of course, data fusion at all levels remains a challenging task. While algorithmic stove-piped systems work well on individual modalities, work is still in progress on seamlessly integrating and correlating multi-intelligence data that includes textual, hyperspectral, and video content (Das et al. 2018).

4.2. Autonomous Platforms

Autonomous vehicles are becoming a reality for civilian applications. In the form of intelligent driving assistance, the vehicle autonomy of the third level (smart cruise control, pedestrian recognition, automatic braking, blind zone sensors, rare cross-traffic alerts, collision avoidance, etc.) has been available for commercial and private vehicles for a number of years. The autonomy of the fourth and fifth levels (supervised autonomy and full unsupervised autonomy) is currently under development. The Kisačanin (2017) paper is one of the first descriptions of developments in the art and science of autonomous driving. The Deep Learning approach s become indispensable in designing and implementing such systems.

Military applications of machine learning and autonomous systems are presented first by Hagström (2019). According to his paper, designing a controller for autonomous vehicles capable of providing adequate performance in all driving scenarios is challenging due to the highly complex environment and inability to test the system in the wide variety of scenarios that it may encounter after deployment. However, deep learning methods have shown great promise in not only providing excellent performance for complex and non-linear control problems, but also in generalizing previously learned rules to new scenarios. For these reasons, the use of deep learning for vehicle control is becoming increasingly popular. Kuutti et al. (2020) paper surveys a wide range of research works reported in the literature, which aim to control a vehicle through deep learning methods.

As it was pointed out by Vecherin et al. (2020), there are significant challenges for autonomous military vehicles. Specifically, the tasks of advanced and current terrain awareness, off-road operation, unknown terrain for operation, the possibility of complete re-routing in open space, determination of possible alternative routes and optimal vehicle control for a given terrain condition and vehicle need to be solved. The main distinctions of military autonomous vehicles are: off-road operation, unknown terrain for operation and the possibility of complete re-routing in the open space. This environment requires different algorithms and environmental awareness for intelligent autonomy controls than those used for civilian applications in the industry. The latest research results indicate that some of the challenges can be successfully solved by ML-based algorithms, thus providing a substantial aid in the manual driving of military vehicles.

The DL approach might apply to unmanned underwater vehicles as well. One of the first research is an automatic target recognition approach for sonar onboard unmanned underwater vehicles. In this approach, target features are extracted by a convolutional neural network operating on sonar images and then classified by a support vector machine that is trained based on manually labeled data (Zhu et al., 2017). Actually, side-scan sonar imagery is of significant interest in both military and commercial applications. The results of applying the method to available data support the approach as simple yet robust in detecting objects/anomalies along the seabed is presented in Einsidler et al.'s (2018) paper.

It is worth mentioning that one of the first official military applications of autonomous weapons is the Kargu drone. This is a small portable suicide drone which is produced in Turkey by Savunma Teknolojileri Mühendislik ve Ticaret. It can be carried by

Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

an individual in both autonomous and manual modes. Kargu can be effectively used against static or moving targets through its real-time image processing capabilities and Deep Learning algorithms embedded on the platform. The autonomous weapons are rapidly proliferating: in accessibility, their degrees of autonomy, the range of international developers, intelligence, reconnaissance and lethal strikes (Longpre et al., 2022). There are a lot of challengers, such as autonomous systems, that remain highly prone to error, demonstrating poor robustness, interpretability, and adversarial vulnerability. Additionally, it should be emphasized that international policy remains ambiguous, and there is a lack of realistic accountability and enforcement mechanisms (Hayir, 2022).

5. Challenges and threats

The DL military application brings a lot of positive opportunities, but at the same, time generates significant level of risks and problems. This trade-off perspective is show in Table 1.

Table 1. Advantages and Disadvantages of applying machine learning in military applications

	Benefits/Advantages	Risks/Disadvantages
OODA decision making and Intelligence Analysis	High quality and more precise decision Decision time reduction Cost effectiveness Reducing emotions and prejudices Rational behavior in crisis situation Possibility to generate potential scenarios based on the predictive analytics Possibility to deal with a huge amount intelligence data	High vulnerability to cyber attacks Analytical errors: bias, false positive and false negative errors, risk governance Cost of false positive and/or false negative errors Lack of explanation capability Unknow reaction for “black swan” cases High skills required for development and maintenance of machine learning models The acceleration and lack of human intervention in the decision-making loop may contribute to an escalation rather than de-escalation of a crisis.
Military Operations and Autonomous Platforms	Reduced risk of harm and number of wounded soldiers through remote operations Precise targeting Time readiness reduction Cost effectiveness Rational behavior in crisis situation	High vulnerability to cyber attacks Risk of taken control by adversaries Significant cost of false positive and false negative errors Unclear whether autonomous platforms may be used in complex situation due to a lack of adequate training data. Unexpected behavior based on “blind” execution of the loss function which my imply escalation of the conflict.

Own elaboration based on: “AI in military enabling applications” by N. Masuhr. Copyright 2019 by the Publisher.

According to Wang et al. (2020), the main challenges in designing and operational use of military AI applications are:

1. Complex system modeling: the overload of battlefield information, including combat units and weapon equipment, in warfare. The complexity of the real-life situation is extremely significant including unexpected cases (like “black swans”), which might not be included in the training data.
2. Inaccurate information: in a confrontation situation, the information obtained is always limited and the authenticity of the information is not guaranteed. Making decisions with such inaccurate information and ensuring the maximum benefit requires comprehensive trade-offs**.**
3. Volume and quality of training data: an acceptable level of DL systems performance depends mainly on high quality, low bias, and extensive volume of data. At present, there are great difficulties in the sources of sample learning, from tactics to action plan generation. Actual combat experience is still facing the problem of an insufficient volume of training data.

Additionally, one of the crucial problems is the cybersecurity of military systems. This issue in mentioned in Table 3 for both Intelligence Analysis and Autonomous Platform as well. This challenge is extensively described in Surma’s (2020) paper.

Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

6. Final Conclusions

AI technology is not omnipotent. It needs to be combined with traditional technologies, such as a human in the OODA loop, in which the role of domain knowledge and common sense are indispensable. Certain safeguard mechanisms are required at the strategic decision-making level. In this context, one of the most important aspects of machine learning relates to the education, training and selection of military enlisted and officer personnel (Masuhr, 2019).

Two significant technological advancements will strongly impact AI military applications soon. Firstly, the development of Generative AI which gives an outstanding opportunity to deal rationally with unstructured data like text (Jo 2023). Secondly, the development of Metaverse technology (Surma, 2023) that might completely redefine the battlefield of the future. Those two technological directions required deep and meaningful analysis from a military perspective.

Declaration of interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., ... & Asari, V. K. (2018). The history began from alexnet: A comprehensive survey on deep learning approaches. *arXiv preprint arXiv:1803.01164*.
2. Das, S., Jain, L., & Das, A. (2018). Deep learning for military image captioning. In *2018 21st International Conference on Information Fusion (FUSION,* IEEE, 2165-2171.
3. Denker, J., & LeCun, Y. (1990). Transforming neural-net output levels to probability distributions. *Advances in neural information processing systems*, *3*.
4. Denton, E., Hanna, A., Amironesei, R., Smart, A., & Nicole, H. (2021). On the genealogy of machine learning datasets: A critical history of ImageNet. *Big Data & Society*, *8*(2), 20539517211035955.
5. Einsidler, D., Dhanak, M., & Beaujean, P. P. (2018). A deep learning approach to target recognition in side-scan sonar imagery. In *Oceans 2018 Mts/Ieee Charleston,* IEEE, 1-4.
6. Fernandes, J. D. C. V., de Moura Junior, N. N., & de Seixas, J. M. (2022). Deep learning models for passive sonar signal classification of military data. *Remote Sensing*, *14*(11), 2648.
7. Fukushima, K. (1988). Neocognitron: A hierarchical neural network capable of visual pattern recognition. *Neural networks*, *1*(2), 119-130.
8. Hagström, M. (2019). Military applications of machine learning and autonomous systems. *The impact of artificial intelligence on strategic stability and nuclear risk*, *1*, 33-38.
9. Hayir, N. (2022). Defining Weapon Systems with Autonomy: The Critical Functions in Theory and Practice. *Groningen Journal of International Law*, *9*(2).
10. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 770-778.
11. Hyman, P. (2012). John McCarthy, 1927--2011. *Communications of the ACM*, *55*(1), 28-29.
12. Jo, A. (2023). The promise and peril of generative AI. *Nature*, *614*(1), 214-216.
13. Kisačanin, B. (2017). Deep learning for autonomous vehicles. In *2017 IEEE 47th International Symposium on Multiple-Valued Logic (ISMVL)*, IEEE, 142-142.
14. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, *25*.
15. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, *60*(6), 84-90.
16. Kuutti, S., Bowden, R., Jin, Y., Barber, P., & Fallah, S. (2020). A survey of deep learning applications to autonomous vehicle control. *IEEE Transactions on Intelligent Transportation Systems*, *22*(2), 712-733.
17. Layton, P. (2021). Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars. *Network*, *4*(20), 1-100.
18. Long, K., & Zhu, Q. (2017). Algorithmic warfare: concept, characteristics and implications. *National Defense Science & Technology*, (6), 8.
19. Longpre, S., Storm, M., & Shah, R. (2022). Lethal autonomous weapons systems & artificial intelligence: Trends, challenges, and policies. *Edited by Kevin McDermott. MIT Science Policy Review*, *3*, 47-56.
20. Masuhr, N. (2019). Ai in military enabling applications. *CSS Analyses in Security Policy*, *251*.

Safety & Defense 10(1) (2024)
DOI: https://doi.org/10.37105/sd.214

21. Merkert, J., Mueller, M., & Hubl, M. (2015). A survey of the application of machine learning in decision support systems. *Clin. Cancer Res.*, 5(2), 267-274.
22. Mohanty, S. P., Czakon, J., Kaczmarek, K. A., Pyskir, A., Tarasiewicz, P., Kunwar, S., & Schilling, M. (2020). Deep learning for understanding satellite imagery: An experimental survey. *Frontiers in Artificial Intelligence*, *3*, 534696.
23. Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military applications of artificial intelligence. *Santa Monica: RAND Corporation*.
24. Neupane, D., & Seok, J. (2020). A review on deep learning-based approaches for automatic sonar target recognition. *Electronics*, *9*(11), 1972.
25. Pritt, M., & Chern, G. (2017). Satellite image classification with deep learning. In *2017 IEEE applied imagery pattern recognition workshop (AIPR)*, IEEE, 1-7.
26. Rawat, W., & Wang, Z. (2017). Deep convolutional neural networks for image classification: A comprehensive review. *Neural computation*, *29*(9), 2352-2449.
27. Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., & Fei-Fei, L. (2015). Imagenet large scale visual recognition challenge. *International journal of computer vision*, *115*, 211-252.
28. Seffers, G. I. (2016). Commanding the future mission. *Signal*, *70*(9), 16-19.
29. Steiniger, Y., Kraus, D., & Meisen, T. (2022). Survey on deep learning based computer vision for sonar imagery. *Engineering Applications of Artificial Intelligence*, *114*, 105157.
30. Surma, J. (2020). Hacking machine learning: towards the comprehensive taxonomy of attacks against machine learning systems. In *Proceedings of the 2020 the 4th international conference on innovation in artificial intelligence* , 1-4.
31. Surma, J. (2023). The Business dimension of Metaverse. *Scientific Papers of Silesian University of Technology. Organization & Management* (170).
32. Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018). Possibilities and challenges for artificial intelligence in military applications. In *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, 1-16.
33. Szabadföldi, I. (2021). Artificial intelligence in military application–opportunities and challenges. *Land Forces Academy Review*, *26*(2), 157-165.
34. Tadjdeh, Y. (2019). DARPA's 'AI next'program bearing fruit. *National Defense*, *104*(788), 8-8.
35. Vecherin, S. N., Desmond, J. R., Hodgdon, T. S., Bates, J. T., Parker, M. W., Lever, J. H., & Shoop, S. A. (2020). Artificial intelligence and machine learning for autonomous military vehicles.
36. Wang, W., Liu, H., Lin, W., Chen, Y., & Yang, J. A. (2020). Investigation on works and military applications of artificial intelligence. *IEEE Access*, *8*, 131614-131625.
37. Yi-Ming, L., & Hai-Ming, S. (2016). Technology subduing: Analysis of the US third 'Offset Strategy. *J. Command Control*, *2*(2), 167-171.
38. Zhu, P., Isaacs, J., Fu, B., & Ferrari, S. (2017). Deep learning feature extraction for target recognition and classification in underwater sonar images. In *2017 IEEE 56th annual conference on decision and control (CDC)*, IEEE, 2724-2731.