DOI:10.59800/bn/170903

Brig. Gen. Dr Hab. Eng. Mariusz M. Fryc[1]
National Security Bureau, Warsaw, Poland

MODERN TECHNOLOGIES SHAPING THE DEVELOPMENT OF THE ARMED FORCES AND THEIR OPERATIONAL ENGAGEMENT UNTIL 2039

Abstract:
In the first quarter of 2023, in accordance with the "Methodology of planning and programming the development of the Polish Armed Forces", the "Main directions of development of the Polish Armed Forces and their preparation for state defense for the years 2025–2039" should be im-plemented. The key document for defense programming will direct the entire process of planning and programming the development of the Polish Armed Forces, including their technical modernization, for the next fifteen years. This analytical and planning project will be one of the key projects implemented this year in the field of state defense, not only for the Ministry of National Defense, including the General Staff of the Polish Armed Forces, but also for the National Security Bureau.
It can be assumed that, to a large extent, its content will be shaped by the experiences resulting from the involvement of the Polish Army so far, among others in counteracting the COVID-19 pandemic and operations to prevent hybrid attacks on the Polish-Belarusian border, as well as recommendations from the ongoing war in Ukraine. While indicating development priorities for the armed forces, planners must not forget that the long-term design horizon adopted by this document will force them to "cut away" from the present and look far into the future so that they can determine the key capabilities that the military forces should have in 2039. In this context, when talking about the main directions of development of the armed forces, it is impossible not to look at technological innovations, which today, though at an early stage of development, have

[1] https://orcid.org/0000-0002-8037-7435.

the potential to determine the functioning and operations of the armed forces in the future.

Keywords: armed forces, defence planning, modern military technologies

Introduction

Throughout history, the development of modern technologies has determined not only the ways in which goods are produced or services are provided, but also how armed operations are conducted and wars are fought. Today, such technologies as artificial intelligence, big data and wireless, broadband telecommunications networks, robotics, autonomous systems, the Internet of Things, immersive technologies and additive manufacturing, as well as energy, hypersonic, space and cyber technologies are significantly shaping social and economic life.

American visionary Alvin Toffler argued that societies struggle in the same way as they produce goods. We can therefore assume that each of the aforementioned emerging technologies today – whether applied to the defense and military dimensions individually or various hybrid combinations of them – will change the way armed forces function and operate. It is fair to assume that their application will be aimed at achieving the best results of operations with the least possible expenditures. In this case, this optimization may boil down to, among other things: reducing numbers and commitment, lowering costs, minimizing risks and providing a higher level of security, accelerating the pace and increasing the precision of operations, expanding situational (operational) awareness or improving decision-making.

Research methodology

The subject of the research in this study were the key technologies mentioned above, which are currently being developed and their potential impact on the armed forces. The main research problem was the question of how the identified technologies may determine the functioning and operational capabilities of the armed forces over the next fifteen years. For this reason, the aim of the research was to identify the areas, capabilities and features that the armed forces will acquire thanks to the implementation of new technologies which will contribute to optimizing their operation and performance. The indirect idea behind the research was to draw the attention of military analysts and planners to the particular importance the developing technologies may have in the area of military's operational capabilities, and to inspire them to conduct an in-depth analysis in this regard during their work on the document *Main directions of development of the Polish Armed Forces and their preparation for national defense for the years 2025–2039*. The research approach was based on review and analysis of the literature on the subject of the research. However, the synthesis of the analyzed material made visible certain characteristic features and regularities that may occur in the process of transformation of the armed forces under the influence of new technologies. Inductive and deductive reasoning allowed for cognitively interesting material to be collected, which was then systematized and generalized into specialized theses.

Artificial intelligence, large data sets and wireless broadband telecommunications networks

The deployment of artificial intelligence technologies – i.e., computer systems capable of performing tasks that normally require human intelligence – is there. Artificial intelligence – defined as the ability of machines to exhibit human skills such as reasoning, learning,

planning and creativity is increasingly applied[2]. Artificial intelligence tools are actually ubiquitous today, both in civilian as well as in security and defense applications. Virtual assistants, speech and facial recognition systems, image analysis software, search engines, etc. are tools which are practically used in our daily lives[3].

The ability of computers to evaluate data and information, make choices and take decisions has progressed significantly over the past decade. The European Parliament's Think Tank estimates that the productivity growth associated with the development of artificial intelligence will oscillate between 11 and 37 percent by 2035[4]. For this reason, artificial intelligence is broadly identified as one of the most important technologies that will contribute to the development of a new generation of products and services in the future. The authorities in Beijing, among others, have recognized it as such, describing it as a critically important resource for strategic development[5].

It seems that the artificial intelligence will most importantly offer a huge leap in the ability of computing to create knowledge from available data and information. The development of artificial intelligence, combined with machine learning, the Internet of Military Things (IoMT), the exploration of big datasets and the development of broadband networks, will open up opportunities for the armed forces to optimize the temporal processes of their operation and performance, including the development of a range of new and unique capabilities.

In principle, this will allow to raise the capabilities of combat potential and at the same time increase protection and resilience against negative impact. It will also foster the creation of full, automated

[2] *Artificial intelligence: what is it and what applications does it have?*, https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-sztuczna-inteligencja-co-to-jest-i--jakie-ma-zastosowania, (accessed February 28, 2023).

[3] J.J. Carafano, *Scenarios for artificial intelligence*, https://www.gisreportsonline.com/r/artificial-intelligence/ (accessed February 28, 2023).

[4] *Artificial intelligence: opportunities and threats*, https://www.europarl.europa.eu/news/pl/headlines/society/20200918STO87404/artificial-intelligence-opportunities-and-threats (accessed February 28,2023).

[5] J.J. Carafano, paraphrase of the quote

situational awareness, including through early detection, identification and classification of threats in various domains in real time. It will also enable access to a wide range of data, information and identified patterns of adversary activity (operation). As a result, technology will be conducive to building information and decision-making superiority over the adversary. Moreover, it is fair to say that with access to data sets as well as information and identification of models (patterns) of action, the forecasting of future events, including threats, will also prove much more effective.

One can assume that, thanks to artificial intelligence, practically all functional areas of the armed forces, i.e.: command, reconnaissance, striking, protection and survival of troops, or logistical security of operations, will be subject to far-reaching optimization. Both offensive and defensive systems will develop as a result. AI is also likely to increase the degree of precision strike. One can also expect that artificial intelligence will increase the effectiveness of air defense systems, including air and missile ones, as well as various types of anti-access (counter-access) systems.

Artificial intelligence along with the Internet of Military Things will enable better management of resources and their flow, save energy, improve military logistics, and ensure optimization of procurement and service processes. It will also play an increasingly important role in the information space, especially in terms of conducting information warfare and countering its effects. One can assume, with a high degree of probability, that artificial intelligence will prove useful not only in military operations, but also in the area of broadly defined crisis management. It will allow to provide earlier warning against natural disasters, natural catastrophes and technical failures. This, in turn, will promote more effective preparation for such events, as well as mitigation of their consequences.

Artificial intelligence relies on sets of data and information, and its development depends on how they are managed. Large data sets, on their part, in order to be properly processed, require the application of new technologies, including artificial intelligence. So there is a clear interdependence in this respect. The emergence of large

datasets has enabled the development of machine learning[6] and deep learning[7]), which in turn has translated into their faster acquisition, processing, analysis and visualization[8].

Today, mankind is producing huge amounts of digital data. The European Commission predicts that by 2025, their total total amount worldwide will increase by 530 percent compared to 2018[9]. Digital data integration processes and use of digital data are becoming increasingly autonomous, thus limiting or even excluding human participation. As a result of the integration of mass-produced data by networks, whose participants are people, organizations, systems and devices, the phenomenon of so-called datafication is being created. It involves specific economic, social or political values[10].

Datafication will certainly affect the military as well. One can assume that the future operations of the armed forces will increasingly be determined by access to data and information, while their effectiveness will be determined by the ability to draw conclusions and create forecasts. Information and decision-making advantages will be gained only by those armed forces which will be able to select the most important data and distribute it quickly and securely[11]. These processes will increasingly be autonomous.

Fifth-generation (5G) mobile technology today allows for data transfers at speeds of up to 20 Gb/s and latency of 1 ms. It covers three categories of applications:

[6] Machine learning is a part (subset) of artificial intelligence. It focuses on learning from data and improving through experience.

[7] Deep learning is a type of machine learning. It is based on layers of neural networks, which are algorithms that are modeled roughly on the functioning of human brains.

[8] K. Śledziewska, R. Włoch, *Digital Economy. How new technologies are changing the world*, Warsaw University Publishing House, Warsaw 2020, p. 74.

[9] *Big data: definition, benefits, challenges (infographic)*, https://www.europarl.europa.eu/news/en/headlines/society/20210211STO97614/big-data-definition-benefits-challenges--infographics (accessed February 28, 2023).

[10] K. Sledziewska, R. Włoch, paraphrase of the quote p. 93.

[11] *Top 10 Military Technology Trends & Innovations for 2023*, https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/ (accessed February 28, 2023).

– mass connectivity between devices, also known as the Internet of Things (loT), allowing devices to connect without human interference on a large scale;
– ultra-reliable low-latency connectivity;
– improved wireless broadband – providing faster data transmission and greater capacity[12].

The June 2022 Ericsson Mobility Report estimated that about ¼ of the world's population currently has access to 5G, and by 2027 this share will increase to ¾. This growth is predicted on the basis of the increasing use of cell phones, the continued development of mobile broadband, and the ongoing digitization of society and the economy[13].

Work is already underway on the next wireless communication technology – the sixth-generation (6G). These efforts however are not very advanced at this point. Nevertheless, it is expected that the implementation of 6G technology will bring about revolutionary changes in communications. 6G technology will likely provide even higher transmission speeds and lower latency. The first trials are expected by the end of this decade[14].

The implementation of faster Internet has accelerated the development of so-called cloud computing. Thanks to the possibility of using computer resources – servers, databases, software, archiving – which were not stored on the local computer, the computing power of ICT systems has increased[15].

In 2022, the global value of the "cloud" market was estimated at about $549 billion. Analysts predict that in 2027 this value will increase to about $1.24 trillion[16]. In 2022 the U.S. Defense Department, in order to guarantee global access to cloud services (Joint

[12] *5G, fifth-generation mobile technology – the mobile network standard that is the successor to the 4G standard*, https://pl.wikipedia.org/wiki/5G (accessed February 28, 2023).

[13] *Ericsson Mobility Report: 5G to top one billion subscriptions in 2022 and 4.4 billion in 2027*, https://www.ericsson.com/en/press-releases/2022/6/ericsson-mobility-report-5g-to--top-one-billion-subscriptions-in-2022-and-4.4-billion-in-2027 (accessed February 28, 2023).

[14] *6G in Poland – is anything known yet?*, https://nafalinauki.pl/6g-w-polsce-czy-juz-cos-wiadomo/ (accessed February 28, 2023).

[15] K. Śledziewska, R. Włoch, paraphrase of the quote, p. 39.

[16] *Cloud Computing Market*, https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html (accessed February 28, 2023).

Warfighting Cloud Capability), which provides the highest standard of security at all levels of command and control, i.e., from strategic to operational to tactical levels, signed contracts with Amazon, Google, Microsoft and Oracle worth $9 billion[17]. The use of the cloud offers global data-sharing capabilities, provides continuous access to data and information with real-time updates, reduces operating costs and contributes to the reduction of ICT infrastructure (hard drives, servers, etc.).

Artificial intelligence, large data sets, wireless, broadband telecommunications networks and cloud services are going to impact the development of military systems and the acquisition of new operational capabilities by the armed forces. The transmission of huge, updated amounts of data in real time will certainly significantly enhance situational awareness, support decision-making processes, relieve the burden on logistics, but also increase the combat and training capabilities of troops[18].

Robotics, autonomous systems, Military Internet of Things

The development of robotics, various types of autonomous systems and unmanned platforms will result in the increasing robotization of the battlefield and, cause a change in the tactics and operations of troops. Already today, unmanned systems have increasingly widespread applications and are having a greater impact on the way military operations are conducted. Robots are becoming more autonomous, more cognizant of their surroundings, more proficient at manipulating objects and cooperating with humans[19].

By 2030, the share of robotic platforms, both remotely controlled and autonomous ones, in the armed forces of the Russian Federation

[17] M. Farrell, *Pentagon Divides Big Cloud-Computing Deal Among 4 Firms*, https://www.nytimes.com/2022/12/07/business/pentagon-cloud-contracts-jwcc.html (accessed February 28, 2023).

[18] *Top 10 Military…*, paraphrase of the quote

[19] K. Śledziewska, R. Włoch, *Economy…*, paraphrase of the quote, p. 53.

is expected to reach 30%[20]. The US Army, in turn, has increased its budget allocated for robotics from $17 million in 2015 to $379 million in 2021. The robotics portfolio includes projects that range from small unmanned aerial systems and ground-based robots, to logistics and combat vehicles, to exoskeletons carried by soldiers. Development priorities in this respect entail improving situational awareness, reducing physical burdens and improving cognitive abilities in soldiers; enhancing the ability to sustain and protect troops, and improving movement capability as well as increasing vehicle maneuverability[21].

The size of the market for military robots is expected to grow from $14.5 billion in 2020 to $24.2 billion in 2025[22]. The development of robotization will be stimulated by commercial innovations implemented in advanced materials, nanotechnology, transportation or fuel cells[23]. Their further development will certainly translate into increased freedom of maneuver for troops, flexibility of their operations, preservation of the economy of forces or ensuring the safety of the military during ongoing missions. Robotics and unmanned (autonomous) systems will improve soldiers' mobility in difficult terrain, reduce their involvement and physical burden, provide better protection, but also allow for an increase in operational awareness. Robots will most likely take over a significant part of the entire spectrum of tasks, i.e. not only in the area of combat or reconnaissance, but also in the security of operations or logistical support[24].

Today, it is not only people who communicate with each other and with devices. In our environment, devices also communicate with each other – mainly to obtain additional information and expand their functionality. Currently, more than 20 billion devices work

[20] *Ibid*, p. 234.

[21] J. Harper, *Big Boost in Spending for Military Robots*, https://www.nationaldefense-magazine.org/articles/2021/1/4/big-boost-in-spending-for-military-robots (accessed February 28, 2023).

[22] *Military Robots Market*, https://www.marketsandmarkets.com/Market-Reports/military-robots-market-245516013.html (accessed February 28, 2023).

[23] J.J. Carafano, *Rapid advancements in military tech*, https://www.gisreportsonline.com/r/military-technology/ (accessed February 28, 2023).

[24] *Top 10 Military...*, paraphrase of the quote.

together in this way, making the industry one of the key branches of technological development[25].

The Internet of Things (IoT), understood as a network of objects (things) equipped with a variety of sensors, software and other technologies, connecting with each other and exchanging data via the Internet, is growing rapidly, and its practical use is likely to become increasingly widespread[26]. This kind of technology is a key factor in the development of smart cities with smart housing and transportation already today. The driving force behind the Internet of Things is the development of 5G connectivity, providing high-speed wireless data transmission, as well as artificial intelligence.

The Internet of Things is also applied in the armed forces. In the military and defense field, it involves linking weapons systems – ships, aircraft, tanks, drones, satellites, as well as military HQs and bases with soldiers – into a common network allowing for information exchange[27]. Sensors and computing devices, worn by soldiers and embedded in their equipment, collect a variety of static and dynamic biometric data[28]. As a result, the cooperating devices improve perception, increase situational awareness, shorten decision-making processes and maximize the speed of action[29]. It is fair to assume that this technology will lead to the development a new organizational feature in the armed forces called the smart army.

Immersive technologies and additive manufacturing

The rapidly developing new capabilities also include immersive technologies. They are used in both consumer and corporate solutions.

[25] W. Kulik, *Internet of Things – what is it? Examples of IoT devices*, https://www.komputronik.pl/informacje/internet-rzeczy-co-to-jest/?gclid=EAIaIQobChMI0a7Xy-im_QIV8RJ-7Ch3jxgZjEAAYASAAEgJK7vD_BwE&gclsrc=aw.ds (accessed February 28, 2023).

[26] M. Zerelik, *Internet of Things (IoT) – What is it? How does it work? Applications, examples*, https://cryps.pl/poradnik/internet-rzeczy-iot-co-to-jest-jak-dziala-zastosowanie-przykla-dy/ (accessed February 28, 2023).

[27] *Top 10 Military…*, paraphrase of the quote

[28] *ibid.*

[29] *ibid.*

They are present in the domain of computer games and the entertainment industry, as well as in the construction, automotive, aerospace, medical, marketing and customer service industries and many other fields. They are significantly changing both the labor market and its needs[30].

Immersion stands for a sense of "immersion" in an artificially created digital reality. Thus, technology connects reality with the artificially created digital world. Generally speaking, it constitutes the next stage in the development of the Internet – its three-dimensional successor, which engages our senses to varying extents and degrees and allows us to feel the artificial world just like the real one[31]. Immersive technologies include virtual reality (VR), augmented reality (AR) or mixed reality (MR). Each of these varieties has different purposes and application potential and, as a result, allows immersion to be experienced to a different degree, scope and form[32].

The use of virtual reality is also spreading in the military environment. Simulations and training support the development of skills in both the individual soldier and entire military units. By creating synthetic training environments, troops exercise in real situations with real weapons and equipment. This, in turn, enables them to act and make decisions in circumstances that could, in many situations, prove too dangerous or too costly to be carried out[33].

Training processes with the use of virtual reality are significantly improving combat readiness of soldiers and units already today. It is highly probable that the influence of immersive technologies – such as virtual reality, augmented reality or mixed reality – will continue to advance and squeeze out classical training methods.

---

[30] M. Marszycki, *Industrial sector raises competence thanks to metaversum*, https://itwiz.pl/sektor-przemyslowy-podnos-kompetencje-dzieki-metaversum/ (accessed February 28, 2023).

[31] *ibid.*

[32] *Immersive technologies – how to use VR/AR in business*, https://gromar.eu/ blog/technologies-immersive/ (accessed February 28, 2023).

[33] S. Lasserre, *4 use cases for virtual reality in the military and defense industry*, https://blog.techviz.net/4-use-cases-for-virtual-reality-in-the-military-and-defense-industry (accessed February 28, 2023).

It should be mentioned at this point that virtual reality is also an excellent tool for designing and optimizing armaments, military equipment, as well as military installations. As a result, its use contributes to improving the overall quality of equipment, increasing its effectiveness and enhancing the ergonomics[34].

Additive manufacturing (AM/ 3D printing) has also been recognized as a breakthrough technology. It has enabled rapid prototyping by transforming 3D CAD data into physical models in just a few hours. As a result, it has become popular in almost all industrial sectors over the past few decades. Thanks to simplification of manufacturing processes, lowing costs and reducing the time necessary for marketing a finished product, additive manufacturing is used in the automotive, aerospace and medical industries, among others. What is more, the technology is increasingly seen as a "real" manufacturing technique, i.e. one that will enable mass production in the future.[35] This trend will certainly impact the operation of industrial defense capability enterprises, as well as the processes of manufacturing armaments and military equipment. It is also likely to create new opportunities for engineering design, significantly lower production costs and reduce logistical burdens. As a result, the production of components and parts will consume less material than traditional manufacturing. The new technology will also enable more efficient on-demand manufacturing, as well as facilitate the creation of novel material combinations[36].

Energy weapons, hypersonic and space technologies, cyberactivity

The sophistication of armaments and military equipment increasing depends on the electronic devices implemented in them and consequently makes them more vulnerable to electromagnetic shock.

[34] *ibid.*

[35] P. Groot, *Additive manufacturing: new challenges for validation*, https://www.plastech. en/wiado-mosci/additive-manufacturing-new-challenges-for-validation-17600 (accessed February 28, 2023).

[36] *Top 10 Military...*, paraphrase of the quote

This is accompanied by new developments in the field of high-power constant-current power sources and microwave generators. Due to these phenomena all major armies around the globe today are either developing energy weapons or working on relevant means to counter them[37].

The goal of energy weapons is to accumulate energy and then transmit it to a target in order to cause its destruction (incapacitation). Electromagnetic weapons include pulse weapons (electromagnetic pulse, EMP), microwave weapons, laser weapons and the railgun, or in other words an electromagnetic cannon.

Pulse weapons, which generate a strong electromagnetic pulse, are used to incapacitate enemy's electronic devices, including their weapons, reconnaissance or command systems. Microwave weapons affect the target with electromagnetic radiation with wavelengths between infrared and ultra-short. They are treated as a "non-lethal" weapon, used, for example, in preventive operations to deter crowds. Laser weapon systems, on the other hand, are capable of releasing concentrated energy in the form of a light beam in a very short time. An electromagnetic cannon (railgun), thanks to a strong magnetic field created thanks to electricity, is capable of launching projectiles at speeds of several Mach[38].

Currently, the market of directed energy weapons is valued at $4.3 billion and is projected to grow to $10.1 billion by 2026.[39] Today, energy weapons technology is implemented in the design of anti-aircraft, anti-ballistic, space or anti-drone systems[40]. It allows for the

[37] P. Bochniak-Koziołek, M. Dras, W. Tyranowicz, *Microwave electromagnetic weapons part 1.*, https://zbiam.pl/artykuly/mikrofalowa-bron-elektromagnetyczna-cz-1/ (accessed February 28, 2023).

[38] *Electromagnetic Weapons*, https://mlodytechnik.pl/news/23719-bron-elektromagnetyczna (accessed February 28, 2023).

[39] *Global Directed Energy Weapons Market by Technology (High energy lasers, High-power microwave, electromagnetic weapon technology, Sonic weapon technology), Platform (Land, Airborne, Naval, Space), Application, Range, Product and Region – Forecast to 2026*, https://www.researchandmarkets.com/reports/5367733/global-directed-energy-weapon-s-market-by (accessed February 28, 2023).

[40] Ł. Michalik, *Electricity instead of gunpowder, or why Europe is building a railgun*, https://tech.wp.pl/prad-zamiast-prochu-czyli-dlaczego-europa-buduje-railgun,6782886698445792a (accessed February 28, 2023).

establishment of counter-access zones, e.g. in the form of a "no-fly zone" around a defended installation. It can also act as an effective measure against low-cost numerous unmanned targets operating in a swarm. While energy weapons are currently quite costly to produce, they are expected to become relatively cheap to operate.

Energy weapons might have a significant impact on the manner and nature of future military operations. It is fair to assume that they will provide greater striking effectiveness compared to classic weapons systems, reduce the logistic burden, and result in lower battlefield lethality[41]. It is also forecast that directed energy weapons will develop in two directions. The first one will consist in the creation of systems that generate non-focused low-frequency pulses against civilian infrastructure targets; the second one in the creation of weapons that are used to generate targeted very high-frequency pulses aimed at military targets. On the other hand, efforts to miniaturize this kind of technology are aimed at developing a capability which will allow also tube and rocket artillery to deliver electric charges generating an electromagnetic pulse[42].

Another technology worth considering is the hypersonic one. Although it has been around for decades, it is widely regarded as a next-generation weapon. Advanced hypersonic military systems are currently being tested and gradually introduced into the armed forces.

Russia, China and the US are most advanced in developing this kind of technology. The already high level of investment in its development continues to grow. In 2022 the Pentagon allocated $3.8 billion for hypersonic systems research, and planned to increase this amount to $4.7 billion in 2023.

Hypersonic missiles do not follow a ballistic curve. Their flight trajectories are variable – they can maneuver, travel at low altitudes, and exceed the speed of sound (up to fifteen times). These properties

[41] *ibid.*

[42] A. Golanski, *EMP weapons – how do they work and what is the threat of the humanitarian terror of our time?*, https://www.dobreprogramy.pl/bron-emp-jak-dziala-i-czym-grozi-humanitarny-po-strach-naszychczasow,6628340455151233a (accessed February 28, 2023).

make hypersonic weapons almost impossible to track today by missile defense systems, let alone the possibility to intercept and destroy them[43]. They are currently being used in combat: e.g. in August 2022 Russians confirmed the three-time use of Kinzhal hypersonic missiles against targets in Ukraine[44]. Hypersonic weapons are designed to combat high-value targets, so their employment makes it possible to achieve completely new operational and strategic results, other than the classic ones. Along with the development of new missiles and hypersonic systems, work is being carried out on new air and missile defense systems[45].

The cyber-security environment is also evolving in a dynamic way. It is significantly influenced by the ongoing war in Ukraine. As a result, the nature of cyber threats is changing. We are seeing a significant increase in hacktivism and cyber activity. Operations in cyberspace are being conducted in coordination with kinetic military operations. We are witnessing mobilization of hacktivists, as well as an increase in cybercrimes. Hacking services – as a business model – continue to gain popularity, and states are increasingly sponsoring attacks carried out by cybercriminals. In addition, disinformation is becoming an important tool in cyber warfare. Cyberactors are also increasing their capabilities.

Advanced long-lasting cyberattacks are becoming more frequent, more destructive and increasingly destabilizing. The amount of data destroyed or stolen is also growing. Among cyber threats, ransomware[46] and denial of service[47] are dominant. These are general features of the contemporary cyber security environment.

---

[43] M. Dabrowski, *What to fight hypersonic missiles with? [ANALYSIS]*, https://space24.en/bezpieczenstwo/technologie-wojskowe/czym-zwalczac-pociski-hipersoniczne-analiza (accessed February 28, 2023).

[44] Ł. Pacholski, *Kinzhal missiles used militarily in Ukraine*, https://zbiam.pl/kinzal-naukrainie/ (accessed February 28, 2023).

[45] M. Dabrowski, paraphrase of the quote

[46] A type of attack aimed at taking control of a target's assets and demanding a ransom in exchange for restoring the assets' availability or keeping them undisclosed.

[47] Denial of Service – an attack on the availability of data, services or other resources. The goal of the attack can be achieved by depleting the service and its resources or overloading network infrastructure elements.

It is forecast that not merely the development of technology, but also geopolitics will continue to have a significant impact on the ongoing cyber operations and cyber security environment. The use of disruptive software is likely to increase significantly in the coming years. Cyber criminals, including state-sponsored actors, will broaden the scope of their operations[48]. Cyber attacks on critical infrastructure of states, such as power grids or communications systems, are likely to increase. In the same vein, more attacks on supply chains (on the relationship between organizations and their suppliers) and IT infrastructure management services can be expected.

The development of artificial intelligence combined with cyber threats will likely result in the creation of new comprehensive (hybrid) security threats. Targeted cyber-attacks, bolstered by the availability of data and information drawn from smart devices (Internet of Things), will become commonplace. Already today, disinformation and so-called "fake news" are powerful means of manipulating public opinions. It is fair to assume that in the future, disinformation, further aided by artificial intelligence, will produce new, more complex and sophisticated forms of the phenomenon. We can also expect to see a continued increase in the number of threats to data subject to destruction or theft.

Furthermore, the armed forces must adapt to the new cybersecurity environment. Among the development priorities included in the National Security Strategy of the Republic of Poland are: achieving the ability to conduct the full spectrum of military operations in cyberspace, increasing the level of resilience of information systems, as well as competence, knowledge and awareness of threats[49].

The space technology market is also developing at a great speed. Satellite navigation and communications systems, as well as satellite imaging are being applied in a great number of areas of social and economic life, including defense and security. The ongoing military operations in Ukraine confirm the importance and significance of

[48] *Cyber Warfare Inspired by the Actions of States*, https://techno-senior. com/2023/02/16/cyber-warfare-inspired-by-the-actions-of-states/ (accessed 28 February 2023).

[49] *National Security Strategy of the Republic of Poland*, Warsaw 2020, p. 20.

the space domain on the modern battlefield. Satellite technologies provide valuable data in the form of imagery, they facilitate communication and navigation, make military operations more precise and effective. Satellite reconnaissance data provide basis for operational planning and securing operations. They allow us to expand situational awareness and improve decision-making processes. As a result, they contribute to better management of resources, time and, indirectly, human lives[50].

Nowadays, competition in space is clearly intensifying, and satellite systems are increasingly becoming the target of adversary actions. In April 2022, SpaceX, which provides the Ukrainian military and civilians with Internet through its Starlink satellite broadband service, reported that its satellites had been attacked by Russians[51].

In the contemporary geopolitical situation, it is necessary to develop national space capabilities and possess electromagnetic reconnaissance systems, secure communications as well as radar, optical, hyperspectral, infrared imaging to ensure full situational awareness at the strategic level, both for peacetime and in the event of war. Indeed, such a priority in the context of space technology development is also part of the National Security Strategy of the Republic of Poland. It stresses the need to build a national, integrated system of situational awareness, based on various means of reconnaissance, command and communications, including national satellite and unmanned systems while maintaining full cryptographic security[52].

[50] M. Mitkov, *The Year of Russia's Invasion of Ukraine. Space Domain in the Era of War [COMMENT]*, https://space24.pl/bezpieczenstwo/technologie-wojskowe/rok-inwazji-rosji-na-ukrainie-domain-space-domain-in-the-era-of-war-commentary (accessed February 28, 2023).

[51] *ibid.*

[52] *Strategy…*, paraphrase of the quote p. 19.

The impact of new technologies on the development of the operational capabilities of the armed forces

Modern technologies which are creating a new quality while gradually remodeling all aspects of our lives – political, economic and social ones – are also transforming the security, defense and military domains. They transform the markets, production, labor, consumption, and cause changes in the functioning and operation of the armed forces. This if the reason why this very context must not be marginalized in the course of work on *the Main Directions of Development of the Armed Forces for the years 2025–2039*.

Formation of a culture of openness to the implementation and dissemination of developing technologies

New technologies open up opportunities for the armed forces to optimize their operation and performance, including the development of a number of new, unique features and capabilities in the areas of reconnaissance, striking targets, command, operations support and logistical security. Therefore, in order to take advantage of this developmental opportunity, they must shape a culture of openness and readiness to make changes, develop innovative solutions, implement new technologies. Only such an approach can make the armed forces an organization that learns quickly and adapts efficiently to the changes that occur in its environment.

New technologies as support for armed forces interoperability

Interoperability, referred to as the key to effectiveness, has been one of the development priorities of most armed forces around the world for decades. The Defense Concept of the Republic of Poland, which outlines the vision of the Polish Armed Forces in 2032, also argues that the future effectiveness of the Armed Forces will be fundamentally determined by the ability of individual units of their branches to work together in a joint operation[53].

[53] *Defense Concept of the Republic of Poland, Ministry of Defense*, Warsaw 2017, p. 45.

Interoperability enables co-operation as well as implementation of the concept of multi-domain operations, which is a contemporary model for conducting current and future armed operations. New technologies in turn, such as artificial intelligence, the developed military Internet of Things, access to large data sets and the ability to transfer them over secure, wireless broadband telecommunications networks, can take interoperability to a new, higher level in terms of co-operation procedures, understanding of reality or integration of multiple functions and new domains. Digital technologies will support the construction of an intelligent military ecosystem, capable of effective networking of the devices and systems that make it up. They will enable the creation of so-called system of systems, linking devices, sensors, effectors in different domains: on land, in the air, at sea, in cyberspace or in space, which will allow to achieve the effect of synergy in terms of resources and activities. Therefore, military planners must develop a vision, and based on that vision plan a strategy for a multidimensional battlespace that takes into account the maximum use of today's evolving digital technologies.

Impact of new technologies on creating full situational awareness and obtaining decision-making superiority

Certainly, further advances in modern ICT technologies will result in the development of integrated situational awareness systems based on reconnaissance, communications, automated command systems, including manned and unmanned systems or satellite assets. They will be able to detect, identify and classify threats in various domains in real time thanks to access to numerous networks and sources of data, information and patterns. Furthermore, the technological leap will make it possible to extract knowledge from available data and information and forecast future events and processes. These capabilities will dramatically increase the armed forces' ability to obtain information and decision-making superiority. For this reason, when developing the Main Directions of Development of the Armed Forces,

military planners must anticipate the possible progress of new technologies, their implications, as well as create a picture of integrated, multi-domain decision-making systems, operating at each and every level of national defense leadership (strategic, operational, tactical) and command of the armed forces.

New technologies on the way to robotizing the future battlefield

Aiming to improve the efficiency of their operations, modern armed forces, next to using modern technologies, will probably try to maximize the robotization of the future battlefield. In the area of robotics, the development priorities today consist in improving soldiers' situational awareness, reducing their physical involvement, machines taking over more risks and relieving the military of certain activities and tasks. With this in mind, military planners need to find an answer to the following question: which functions, activities and domains among those hitherto performed by soldiers in such areas as combat, reconnaissance, operations security or logistical support, will be taken over by robots and autonomous systems? In what way will the use of robots, either on their own or along with conventional forces, in the form of so-called clouds or swarms, determine the shape of the organizational structures of the armed forces, as well as their size? It is also necessary to consider what changes robotization will bring about in the tactics of conducting operations and how the military training system will function in consequence. Based on the answers, the militaries must devise new doctrines in order to take advantage of the unique attributes of the evolving robotics and digital technologies.

The possibility of implementing an effective logistics security system

New technologies are likely to take military logistics to a completely different level of functioning and securing processes in the armed forces. Artificial intelligence along with the Internet of Military

Things (IoMT) will allow to better manage resources and their flow, save energy, improve planning and movement, maintenance of troops, and ameliorate the procurement and service processes. Therefore, military analysts should rethink logistics and ensure it becomes a multi-domain field, tailored to new circumstances, organizational structures and robotized military units. In transforming logistics, they need to take into account their own experience, but also draw on models from the civilian business. The implementation of modern technologies offers an opportunity to improve logistics efficiency. It allows for enhancing its potential, boosting flexibility, responding more quickly to the needs of the military and managing resources more efficiently.

Increasing striking capability and creating a resilience system as well as anti-access areas

New technologies will enhance the striking capabilities of the armed forces. They will be supported by traditional capabilities in both lethal and non-lethal dimensions. The striking precision and the strategic effects will be amplified by directed energy systems, radio-electronic warfare and the properties of unmanned platforms combined with artificial intelligence and access to data networks, support of satellite technologies, as well as offensive and defensive capabilities in cyberspace. For this reason, military planners need to think how to properly deploy modern technologies in building a resilient state, how to utilize their features in the civilian and military spheres in order to ensure the continuity of state administration and the functioning of critical processes (e.g., ensuring civil protection, energy, water and food supplies). They also need to reflect on how modern technologies can be applied to create "anti-access" (Anti-Access/Area Denial, A2/AD) systems and how they can help to restrict access to multiple domains (land, sea, air, cyber, space, radio-electronic, information) to a potential adversary.

"Immersion" of military training into digital reality

Already now, we are seeing a fairly strong inclination to create synthetic, digital training environments. Immersive technologies will make the sense of "immersion" in an artificially created reality even more intense, merging the perfectly real world with the digital one. Military planners should take this trend into account when creating a vision of a modern training system and planning both the development of the skills of the individual soldier, HQs and Staffs, as well as subunits with autonomous platforms operating in a swarm.

New opportunities for the development of industrial defense capabilities

New technologies are going to change the processes of manufacturing weapons and military equipment. The development of additive technology might turn it into a "real" manufacturing technique, enabling mass production. New technologies will certainly simplify manufacturing processes, lower the costs and reduce the time. This will be followed by improvements in the overall quality of the military equipment and armaments, increasing the effectiveness and improving the ergonomics. However, in an era of the dominance of digital technologies, the military must remember, first of all, to open up to cooperation not only with large industrial corporations, but also with small companies, which frequently are start-ups. Since they are the ones who see opportunities for development in the process of digital transformation and will therefore increasingly offer high-quality, unique digital capabilities, services and products needed by the armed forces to function and operate.

New technologies as the axis of scientific research

On the other hand, national scientific research plans, including military domain, must aim at developing artificial intelligence, big data, broadband telecommunication networks, robotics and autonomous systems, the Internet of Things, immersive technologies and additive

manufacturing, as well as hypersonic, space, cyber or directed energy technology. These activities should include the establishment of new scientific research centers, the launch and funding of basic and applied research, as well as setting-up infrastructure to collect data and accumulate knowledge.

Conclusion

Main Directions of Development of the Armed Forces form the basis and provide the starting point for planning the development of the forces throughout the entire defense programming process. By adopting the perspective of 15 years, the document forces planners to "detach" themselves from current circumstances, events and processes and outline a long-term vision of the development of troops. For this reason, in addition to applying lessons learned from fighting the COVID-19 pandemic, conducting the counter-hybrid operation on the Polish-Belarusian border and the war in Ukraine, the military must review modern technologies and assess their potential impact on the armed forces.

When listing development priorities for the armed forces, special attention should be given to the analysis of development capabilities of artificial intelligence, big data, wireless broadband telecommunications networks, robotics, the Internet of Things, immersive technologies and additive manufacturing, as well as to energy, hypersonic, space and cyber technologies. The military should then assess their impact on the functioning and operation of the armed forces, including the way in which they will determine command, reconnaissance, striking, protection and survival of troops, or logistical security of operations.

The review of modern technologies included in this study was intended primarily to flag out this aspect to the military planners who are currently working on the *Main Directions of Development of the Polish Armed Forces and their preparation for national defense for the years 2025–2039*. Its aim was also to inspire analysts to make modern

technologies an important determinant in their thinking about the development of the armed forces when planning their future capabilities.

At the same time, the conducted research allows to conclude that modern technologies stand a good chance of enhancing the interoperability of the armed forces; enabling them to achieve full situational awareness and gaining decision-making superiority. They enhance striking capabilities, enable the implementation of a more efficient logistics security system, the creation of a more effective resilience system of the State and the development of counter-access areas. They are also likely to significantly robotize the future battlefield and further "immerse" the process of training troops, HQs and Staffs, as well as individual soldiers into a cyber reality. The new digital ecosystem is already penetrating the armed forces. Therefore, in order to ensure that the military takes full advantage of the opportunity and makes conscious use of modern technologies to become a "smart army," it must be open to their implementation and development.

Bibliografia
References List

5G, technologia mobilna piątej generacji – standard sieci komórkowej będący następcą standardu 4G, https://pl.wikipedia.org/wiki/5G (dostęp: 28 lutego 2023 r.).

6G w Polsce – czy już coś wiadomo?, https://nafalinauki.pl/6g-w-polsce-czy-juz-cos-wiadomo/ (dostęp: 28 lutego 2023 r.).

Big data: definicja, korzyści, wyzwania (infografika), https://www.europarl.europa.eu/news/pl/headlines/society/20210211STO97614/big-data-definicja-korzysci-wyzwania-infografika (dostęp: 28 lutego 2023 r.).

Bochniak-Koziołek P., Dras M., Tyranowicz W., *Mikrofalowa broń elektromagnetyczna cz. 1.*, https://zbiam.pl/artykuly/mikrofalowa-bron-elektro-magnetyczna-cz-1/ (dostęp: 28 lutego 2023 r.).

Broń elektromagnetyczna, https://mlodytechnik.pl/news/23719-bron-elektro-magnetyczna (dostęp: 28 lutego 223 r.).

Carafano J. J., *Rapid advancements in military tech,* https://www.gisreportsonline.com/r/military-technology/ (dostęp: 28 lutego 2023 r.).

Carafano J. J., *Scenarios for artificial intelligence*, https://www.gisreportsonline.com/r/artificial-intelligence/ (dostęp: 28 lutego 2023 r.).

Cloud Computing Market, https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html (dostęp: 28 lutego 2023 r.).

Dąbrowski M., *Czym zwalczać pociski hipersoniczne? [ANALIZA]*, https://space24.pl/bezpieczenstwo/technologie-wojskowe/czym-zwalczac-pociski-hipersoniczne-analiza (dostęp: 28 lutego 2023 r.).

Ericsson Mobility Report: 5G to top one billion subscriptions in 2022 and 4.4 billion in 2027, https://www.ericsson.com/en/press-releases/2022/6/ericsson-mobility-report-5g-to-top-one-billion-subscriptions-in-2022-and-4.4-billion-in-2027 (dostęp: 28 lutego 2023 r.).

Farrell M., *Pentagon Divides Big Cloud-Computing Deal Among 4 Firms*, https://www.nytimes.com/2022/12/07/business/pentagon-cloud-contracts -jwcc.html (dostęp: 28 lutego 2023 r.).

Global Directed Energy Weapons Market by Technology (High energy lasers, High-power microwave, electromagnetic weapon technology, Sonic weapon technology), Platform (Land, Airborne, naval, Space), Application, Range, Product and Region – Forecast to 2026, https://www.researchandmarkets.com/reports/5367733/global-directed-energy-weapons-market-by (dostęp: 28 lutego 2023 r.).

Golański A., *Broń EMP – jak działa i czym grozi humanitarny postrach naszych-czasów?*, https://www.dobreprogramy.pl/bron-emp-jak-dziala-i-czym-grozi-humanitarny-postrach-naszych-czasow,6628340455151233a (dostęp: 28 lutego 2023 r.).

Groot P., *Produkcja addytywna: nowe wyzwania dla walidacji*, https://www.plastech.pl/wiadomosci/Produkcja-addytywna-nowe-wyzwania-dla-walidacji-17600 (dostęp: 28 lutego 2023 r.).

Harper J., *Big Boost in Spending for Military Robots*, https://www.nationaldefensemagazine.org/articles/2021/1/4/big-boost-in-spending-for-military-robots (dostęp: 28 lutego 2023 r.).

Koncepcja Obronna Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej, Warszawa 2017.

Kulik W., *Internet Rzeczy – co to jest? Przykłady urządzeń IoT*, https://www.komputronik.pl/informacje/internet-rzeczy-co-tojest/?gclid=EAIaIQobChMI0a7Xyim_QIV8RJ7Ch3jxgZjEAAYASAAEgJK7vD_BwE&gclsrc=aw.ds (dostęp: 28 lutego 2023 r.).

Lasserre S., *4 use cases for virtual reality in the military and defense industry*, https://blog.techviz.net/4-use-cases-for-virtual-reality-in-the-military-and-defense-industry (dostęp: 28 lutego 2023 r.).

Marszycki M., *Sektor przemysłowy podnosi kompetencje dzięki metaversum*, https://itwiz.pl/sektor-przemyslowy-podnosi-kompetencje-dzieki-metaversum/ (dostęp: 28 lutego 2023 r.).

Michalik Ł., *Prąd zamiast prochu, czyli dlaczego Europa buduje railguna?*, https://tech.wp.pl/prad-zamiast-prochu-czyli-dlaczego-europa-buduje-railguna,6782886698445792a (dostęp: 28 lutego 2023 r.).

Military Robots Market, https://www.marketsandmarkets.com/Market-Reports/military-robots-market-245516013.html (dostęp: 28 lutego 2023 r.).

Mitkow M., *Rok inwazji Rosji na Ukrainie. Domena kosmiczna w dobie wojny [KOMENTARZ]*, https://space24.pl/bezpieczenstwo/technologie-wojskowe/rok-inwazji-rosji-na-ukrainie-domena-kosmiczna-w-dobie-wojny-komentarz (dostęp: 28 lutego 2023 r.).

Pacholski Ł., *Pociski Kinżał użyte bojowo na Ukrainie*, https://zbiam.pl/kinzal-naukrainie/ (dostęp: 28 lutego 2023 r.).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Sztuczna inteligencja: co to jest i jakie ma zastosowania?, https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania (dostęp: 28 lutego2023 r.).

Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2020.

Technologie immersyjne – jak wykorzystać VR/AR w biznesie?, https://gromar.eu/blog/technologie-immersyjne/ (dostęp: 28 lutego 2023 r.).

Top 10 Military Technology Trends & Innovations for 2023, https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/(dostęp: 28 lutego 2023 r.).

Wojna cybernetyczna inspirowana działaniami państw, https://techno-senior.com/2023/02/16/wojna-cybernetyczna-inspirowana-dzialaniami-panstw/ (dostęp: 28 lutego 2023 r.).

Zerelik M., *Internet Rzeczy (IoT) – Co to jest? Jak działa? Zastosowanie, przykłady*, https://cryps.pl/poradnik/internet-rzeczy-iot-co-to-jest-jak-dziala-zastosowanie-przyklady/ (dostęp: 28 lutego 2023 r.).