**Lech Majewski**
Gen. broni pil. w stanie spoczynku
Wiceprezes SSLW RP,
Przewodniczący KSLiTK przy SITKRP

DOI: 10.35117/A_ENG_23_05_02

# Cybersecurity and the digital revolution (on the example of the civil and military domain)

**Abstract**: The emergence of new digital technologies creates new opportunities for development and building material capabilities, but also brings significant changes to social life, the legal dimension, and ethics. It can be confidently stated that whoever utilizes the possibilities offered by artificial intelligence, space, and cyberspace faster and better will shape the future of the world, create a new civilization, and change its fundamental operations. This process has already begun. The world's largest military powers prioritize digital technologies, autonomous and unmanned systems—their integration with manned aircraft or crewed vessels, artificial intelligence, and the utilization of space and cyberspace. It is important to emphasize that these actions enable real-time combat operations. A cognitively distorted world is emerging, making it difficult to objectively assess existing situations. For instance, the United States, Europe, China, and Russia evaluate situations differently. China's political system allows it to more easily and quickly dominate the cyber domain. China is progressively gaining technological superiority, mastering new technologies without facing civilizational or cultural objections.

**Keywords:** Cyberspace; Digital revolution; Outer space; Aircraft

We live in a period of revolutionary technological changes, during the fourth industrial revolution, which is progressing rapidly. The digital revolution influences our daily lives, determines the development of the state, and its place in the structure of the future world. It becomes the core of progress, and in the Armed Forces, it heralds a new type of warfare.

The driving force behind the fourth industrial revolution is a combination of modern computers with high computational power, robots, autonomous systems, advanced information technologies, and a better understanding and utilization of the human genome.

The mutual connection of various devices, access to the maximum amount of information, technological support, and decentralization of decisions can lead to autonomous decision-making, faster communication, and effective collaboration. At the same time, the new situation results in the need to quickly identify problems that we have not previously encountered.

Big Data analytics and artificial intelligence algorithms play a key role here. Intelligent systems possess comprehensive knowledge and cognitive abilities that allow them to perform tasks independently.

In addition to existing domains of warfare—land, sea, and air—the space domain and cyberspace (digital) are beginning to dominate.

In July 2016, during the NATO Summit in Warsaw, cyberspace was recognized as another domain (then the fourth) in which operational activities can be conducted. At the same time, NATO members emphasized that they would make every effort to defend the new operational domain in the same way the Alliance protects its operations in the land, sea, and air dimensions. To this end, seven commitments known as the Cyber Defence Pledge were adopted, which allies agreed to develop and strengthen. It was also agreed that the implemen-

tation status of the aforementioned commitments would be monitored and reviewed by NATO annually.

Cyberspace is already subjected to continuous attacks during peacetime. Critical infrastructure, communication systems, and the information space are systematically attacked.

Before our eyes, two digital worlds are taking shape: the Chinese and pro-American. A great revolution and rivalry are ongoing. Poland, along with other countries in our bloc, is often the target of cyberattacks from various nations, primarily from the Russian Federation. In such a situation, especially in the context of the war in Ukraine, we should not allow ourselves to fall behind in this area.

All indications point to the fact that the most important war of the 21st century will take place in the virtual world, in cyberspace. In this direction, the largest military powers are conducting intensive preparations and actions. New strategies for conducting wars are being developed. Certainly, Poland's security is more threatened now than, for example, ten years ago.

We increasingly talk about contactless warfare, autonomous means of conducting combat, combat robots, new electromagnetic, laser, plasma, and microwave weapon systems, combat exoskeletons, and implants that make soldiers resistant to stress.

The world's largest military powers prioritize digital technologies, autonomous and unmanned systems—their integration with manned aircraft or crewed vessels, artificial intelligence, and the utilization of space and cyberspace. It is important to emphasize that these actions enable real-time combat operations.

As a result, the significance of contactless operations increases, in which the warring parties are beyond the range of direct observation, there is no border of military contact, and an attack on a potential opponent can be carried out from all directions, from all domains of operational activities.

The Pentagon predicts that in the coming decade, autonomous systems will become one of the main means of warfare. Currently, work is underway on the so-called Future Combat Systems (FCS) program, valued at over $120 billion. This is the largest contract in U.S. history.

In the United States, the following pillars of Armed Forces modernization are increasingly being discussed and implemented:

1. A network-centric command and control system. The idea of connecting everything with everything and creating an augmented reality that allows designing additional information over the real-world view. The experimental proving ground is, of course, the Strategic Command (SP).
2. Autonomous systems collaborating with humans, being deployed on a large scale across all branches of the Armed Forces.
3. Artificial intelligence—the key to data, and data is today the battlefield.

There is no talk of tanks, aircraft, missiles, ships, or even satellites—instead, the focus is on networks, communications, data, and the potential of AI technology, which automates processes, predicts future events, assesses risks, and conducts preventive measures. Not megatons but megabits.

The global artificial intelligence market reached approximately $450 billion in 2022. By 2030, the AI sector's value will increase to $1.3 trillion and will add nearly $16 trillion to the global economy. By 2022, new technologies created 133 million jobs worldwide.

In 2019 alone, global AI expenditures reached nearly $40 billion—44% more than the previous year (two-thirds in the USA; 5.5% in Europe).

It is estimated that cyberattacks in 2021 cost as much as $11.4 million per minute! One zloty invested in the space industry returns fourfold.

In Poland, the demand for specialists in artificial intelligence will reach 200,000 people within the next five years.

Many countries, led by Russia, are conducting intensive cyber activities, breaking international law, and interfering in their internal politics. Using military force against neighbors: Georgia and Ukraine, and also engaging in aggressive actions against NATO countries. All these actions also affect the internal political processes of states.

In March 2021, President Biden stated that the President of Russia is a “killer” and that he would pay for interference in U.S. elections.

Poland is spending hundreds of billions on new armaments.

However, do decision-makers realize that the path to the future of the Armed Forces, to effective state defense, lies in artificial intelligence, autonomous systems, and network-centricity, that the potential is here, not in tanks or missiles, and that no matter how modern a weapon on the contemporary battlefield is, it has no significance if it is not connected to a resilient and high-bandwidth information network.

The rapid development of information technologies has led to their application in cyberspace activities, especially to damage critical infrastructure (banks, energy, industrial and military facilities, e.g., command and control systems).

In the short term, robotization in industry and on the battlefield will lead to their full autonomy in performing assigned tasks.

**Australia: The Army Focuses on Robots and a New Approach to Robotics**

Australians not only recognize increasing threats but are also taking concrete actions. They are beginning to conduct a broad program of testing and research concerning breakthrough technologies, including autonomous land robots. The program is based on extensive collaboration between the military, industry, and academia, and, of course, with the United States.

In Australia, it is not just about talking about robots; they are already being exploited, tested, or development programs are being advanced.

**Turkey: Plans to Create an Aircraft Carrier for 30-50 Combat Drones**

Previously planned for the F-35—the purchase of the S-400 has changed plans. Elon Musk's satellites are essential for the Ukrainian army and the civilian population—they help in determining Russian positions, enable contact with loved ones, and President Volodymyr Zelenskyy's speeches can be broadcast worldwide.

Thanks to SpaceX's system, the Kremlin failed to cut Ukraine off from the outside world, and the Kremlin's plans proved unrealistic.

**The War in Ukraine**

The war in Ukraine clearly demonstrates that increasing access to artificial intelligence, space, and the latest technologies makes truth the first casualty of the situation.

For example, in light of recent political events, media situations, and the internal situation in Ukraine, we increasingly speak of a "fog of war." Information is transmitted in a way that makes it difficult to determine the dynamics of events in the existing situation, such as the situation and losses on the Ukrainian front.

This new infosphere (not always appreciated) contributed, among other things, to NATO, the EU, and the United States being unable to assess the situation in the East and stop Russia's aggressive actions. The dominance of social media in democratic systems has become indisputable and difficult to control. Hundreds of thousands of non-productive intermediaries in state structures are becoming a major headache for the West, often shaping and slowing development.

**Digital Domination and Communication**

In the context of digital domination and the rapid development of new communication methods, including social media, legitimizing authority becomes a significant problem. Social media can significantly contribute to disrupting the situation in a state; they can become part of a business strategy. The role of authorities is clearly diminishing. Unrestricted and unsupervised use of the Internet can lead to addiction and cause psychological problems, especially among young people.

Therefore, an important aspect of operating in cyberspace is the ability to monitor information, particularly focusing on the dynamics of virtual community development. The Internet is an excellent tool for false leaders who present themselves as competent individuals, which in the age of post-truth is not verified in any way. Such social mechanisms are often used by terrorist and criminal organizations, as well as by political and state institutions.

**Comparing Military and Economic Potential**

When comparing the military and economic potential of the EU, NATO, and the USA to Russia's potential, the differences are staggering, yet Russia attacked...

A cognitively distorted world is emerging, making it difficult to objectively assess existing situations. The United States, Europe, China, and Russia evaluate situations differently, not to mention Russia itself. The West, led by France or Germany, often fears the possibility of US dominance.

**China's Cyber Dominance**

China's political system allows it to more easily and quickly dominate the cyber domain. China is progressively gaining technological superiority, mastering new technologies without facing civilizational or cultural objections.

In the democratic world, the emergence of large global digital corporations without appropriate political responses leads to the destruction of small businesses and the middle class, generating social tensions. Silicon Valley businesses generate enormous money and gain an advantage over politics.

A Gordian knot is forming: if we divide powerful Western corporations, there will be no possibility of competition with powerful Chinese ones.

In China, digital capital does not have an advantage over politics or the government.

**Discussion and Conflict in Democracies**

Discussion and conflict—freedom of expression are normal in democratic societies. The Internet has tools that enable monitoring and managing such processes.

The greatest threat appears to be closed groups controlled by leaders whose potential and aspirations cannot be verified in the real world. Using a simple scheme, the triangle of oppressor - victim - savior can illustrate relationships both in radical organizations and in everyday life. The result is a process that causes the rapid brutalization of interpersonal relations.

Three main factors lead to this: lack of authorities, deterioration of basic living conditions (which often leads to stress and ultimately panic), and the functioning of strong pressure groups influencing the defenseless victim.

**Need for New Politicians**

In the current situation, considering the emerging threats, there is an urgent need to build a new category of politicians—well-educated and understanding reality, capable of making appropriate decisions and changing it.

**Impact of the COVID-19 Pandemic**

The COVID-19 pandemic accelerated the development of new technologies, artificial intelligence, changed the social communication system. It developed remote work and virtual learning through online courses, remote internet shopping, but also caused depressive tendencies among a broad group of society. According to experts, the pandemic accelerated the digital revolution by many years.

**Cyber Domain as a Weapon**

Before our eyes, the cyber domain used for disinformation has become a powerful weapon. A good example is Ukraine.

What if Russia had started attacking critical infrastructure in Ukraine from the beginning? The Russians created a false image of Ukraine. They did not treat Ukraine as a foreign state. They thought Ukrainians supported Russia. They had a distorted view of the situation in Ukraine. They overlooked, among others, Maidan, which changed everything.

Initially, they wanted to take over a state that was not destroyed; they felt a sense of superiority—but fortunately, it was false.

**Ukraine's Response**

In a difficult situation, Ukraine showed immense willpower, great creativity of the government and ordinary people, a strong desire to fight for freedom and democracy, and affiliation with the Western world.

The process of mitigating the damage caused by barbaric Russian attacks began already at the level of building IT infrastructure.

They well designed a computer network that functions even if individual terminals are infected. The distributed network proved very resistant to hacking attacks, provided that cybercriminals do not locate key devices responsible for redirecting most traffic.

It turned out that an important measure to enhance infrastructure security is the redundancy of network components—it allows duplication of communication channels and maintaining basic functions even if some are destroyed.

At the infrastructure level, they also ensured proper servicing, which always involves selecting trusted and verified subcontractors—something that was particularly not easy in Ukraine.

To date, only 77 countries have developed their own cyber strategies, only twenty have their special commands, and only 17 are capable of conducting cyberattacks.

**Examples of Major Cyber Operations**

Examples of major operations of this type include Israel's operations against Syrian air defenses, the Russian-Georgian war, and, of course, the Russian-Ukrainian war, as well as the American counteroffensive against ISIS.

Currently, it is difficult to define a register of virtual operations. Such actions have already gone beyond the scope of classical espionage or hacking activities. When the target becomes an entire state, we can talk about the proliferation of cyber weapons.

In the current battlefield, another highly specialized specialist is needed—field computer scientist, for example, similar to a JTAC aviation coordinator, sapper, or chemist.

Military networks are well protected against external interference, but penetration is still possible, similar to sterile computers in an Iranian nuclear power plant.

In the modern world, nothing can stop the development of new cyber technologies, especially at the level of critical infrastructure. Therefore, it is crucial to be able to identify potential attack points, assess their probability, and have procedures in place to minimize damage. A good example of possessing such skills is Ukraine.

The most developed countries in the world have appropriate structures in their Armed Forces that enable neutralizing threats at strategic and operational levels. The activities of individual cyber commands are comparable to classical special forces operations. They also need well-trained and equipped specialists performing specific tasks. To this end, many countries are creating new command structures. For example, in the United States, different branches of the Armed Forces have their cyber commands. More and more countries are establishing separate branches of the Armed Forces and commands to counter threats in the network.

In 2017, the United States' Cyber Command, established in 2009, was separated and became the tenth military command. In 2017, Germany established the Cyber and Information Space Command. In 2016, the UK increased its cybersecurity funding. Such actions are also undertaken by non-NATO countries. In 2016, Russia established information troops. Also in 2016, the Air Force of the Republic of Korea established a new cybersecurity center. Also in Poland, from November 2018, a new type of Armed Forces is being created—the Cyber Defense Forces.

Based on the Act on the Defense of the Fatherland, the Cyber Defense Military Component is being established, which will be subordinate to the Commander of the Cyber Defense Component (Dowódca Komponentu WOC).

The structure of the Cyber Defense Forces is based on the Cyber Operations Center—a unit already existing in the Polish Army. The number of positions there will triple.

Cyber soldiers are not the soldiers of the future; they are soldiers operating today. Changes are also taking place in the National Cryptology Center and the IT Inspectorate. Both institutions have been merged into the National Cybersecurity Center.

A Non-Commissioned Officer School of Communications and Informatics has been established in Zegrze (replacing the former Communications and Informatics Training Center) as well as an Informatics High School at the Military University of Technology. The cyber component is being created in the Armed Forces and is expected to eventually include 100 specialists. At the Military University of Technology (WAT), programs in cryptology have been established, with over 100 students studying each year. In 2017, Minister Macierewicz announced the intention to train 1,000 hackers (the same number as Germany, more than Russia). Poland currently lacks 50,000 IT specialists.

At WAT, postgraduate studies in cybersecurity have been launched, and the quotas for programs in cryptology and cybersecurity, computer science, electronics and telecommunications, and information systems in security have been increased. The Naval Academy in Gdynia also conducts military studies dedicated to cybersecurity. In 2019, the training module of the Academic Legion was expanded to include a cybersecurity component. It is there that soldiers are being trained whose main tasks will include combating computer viruses, fake news, and computer-based disinformation.

In Poland, despite the establishment of the Polish Space Agency, the development of the space sector and the utilization of its capabilities, as well as the construction of satellites, remain very serious problems. Unfortunately, these issues compound each year, and Poland is increasingly lagging behind Europe and the rest of the world.

Considering the decisions being made and the initiatives undertaken in the field of cybersecurity, it appears that a single strong entity should be established to ensure the coherence of Poland's cyber policy both domestically and internationally. This entity should achieve the state's strategic objectives by representing Poland's military, economic, and scientific interests on the international stage (EU, NATO, ESA, EUMETSAT, EDA), ensuring coordination between science, business, and state administration.

Unfortunately, as is often the case in Poland and worldwide, the initiators of new challenges frequently lack understanding and face serious difficulties.

**Proposals for Modernizing the Armed Forces**

Michale Flournoy, Joe Biden's presidential candidate for Secretary of Defense in the United States, presented the following proposals for modernizing the American Armed Forces during a speech in Congress: megabits instead of megatons, digital technologies, autonomous and unmanned systems—their integration with manned aircraft or crewed vessels and artificial intelligence should form the basis of the modernization of the Armed Forces.

Meanwhile, British Prime Minister Boris Johnson in March 2021 stated that "cyber power is revolutionizing the way we live and wage wars, much like the Air Force did a hundred years ago."

In the past, generals such as Gen. Douchet from Italy or Gen. Mitchell from the United States faced significant troubles with their revolutionary visions. The Polish example includes Gen. Zagórski and Gen. Rayski, and after the war, Gen. Frey Bielecki, the first Polish commander of the Military Institute of State Protection (WLiOP).

It can be confidently said that inconvenient "prophets" quickly did not end well. They were often only recognized and appreciated after their deaths. Time has shown and proven that all of them, like many others, were largely correct and spoke the truth.

**Current Challenges and Modernization Efforts**

Will it also be the same now? Are the current new challenges overwhelming the decision-makers? Is the current process of modernizing the Armed Forces, as well as the entire country, heading in the right direction?