Tomasz Grabowski
Jesuit University Ignatianum in Krakow
https://orcid.org/0000-0003-1280-1609
https://doi.org/10.35765/slowniki.157en

Trends in global security

Summary

DEFINITION OF THE TERM: The article is devoted to contemporary technological development, which is considered a major megatrend in security.

HISTORICAL ANALYSIS OF THE TERM: Technological development has led to fundamental changes in military affairs. The Third Industrial Revolution brought computerisation and the networking of the armed forces. The Fourth Industrial Revolution will enable the implementation of new technologies that could have a disruptive impact on global politics.

DISCUSSION OF THE TERM: The development and use of artificial intelligence and unmanned systems, combined with advances in areas such as robotics, biotechnology, and brain research, will lead to another revolution in military affairs.

SYSTEMATIC REFLECTION WITH CONCLUSIONS AND RECOMMENDATIONS: The implementation of cutting-edge technologies could have enormous implications for the global balance of power. It is necessary to recognise the challenges involved and to strive to control technological development.

Keywords: revolution in military affairs (RMA), artificial intelligence (AI), unmanned systems, hypersonic weapons, biotechnology

Definition of the term

The article reviews, identifies, explains, and describes the latest trends in global security. The article focuses on the most fundamental long-term trends that are manifested at the level of large social structures. With reference to Fernand Braudel's (1982) work *Ecrits sur l'histoire* [*On History*], the analysed trends can be described as processes of a *longue durée*, i.e., processes that are independent of current political events ('event-based history'), that are located outside of the collective consciousness, and that escape the attention of researchers who confine their studies to within the boundaries of a narrow scientific discipline (Pawłuszko, 2018). Moreover, the processes described in this article are the most influential and are known as 'megatrends', which lead to fundamental and radical changes in contemporary societies. The last criterion used for selecting contemporary security trends for the purposes of this study was their origin: the trends described in this article are anthropogenic only; those resulting from natural forces (and from natural forces unleashed by man) are excluded.

Trends in global security that meet all the above-mentioned criteria (scope, persistence, depth, and anthropogenicity) primarily include the technological revolution and the resulting increase in the importance of cutting-edge disruptive technologies in the security sphere. However, technology is closely related to globalisation: it is through the achievements of technology that globalisation's characteristic 'shrinking' of time and space is possible.

Historical analysis of the term

The second half of the 20th century witnessed a technological revolution (called the Third Industrial Revolution'), a manifestation of which was the IT revolution – including computerisation and digitalisation. In security, the Revolution in Military Affairs (RMA), also called Information Technology RMA (IT-RMA), gained momentum at the same time. This was another radical change in the military sphere in history that resulted from the development of new technologies and included innovations in the way military operations were conducted (doctrinal

change) and transformations in the organisational structure of the armed forces. It occurred in the United States during the Cold War in an effort to avoid nuclear war and a conventional clash with Warsaw Pact forces, and to win global superiority by achieving a technological (qualitative) advantage. The US victory in the Cold War was a triumph of the 'Western Way of Warfare' and set the stage for military development at the turn of the 21st century. Western military capabilities were demonstrated in subsequent conflicts and crises, such as Operation Desert Storm (1991) and Operation Desert Fox (1998), the airborne Operation Allied Force against Yugoslavia (1999), the invasions of Afghanistan (2001–2002) and Iraq (2003), and the airborne intervention in Libya (2011). These demonstrated the capabilities of precision weapons and the network-centric organisation of operations (with hardly any political and strategic effects of the aforementioned military interventions).

It can be legitimately argued that another RMA is currently underway, this time with the use of Artificial Intelligence (AI). This is referred to by the acronym AI-RMA and is situated within the framework of the Fourth Industrial Revolution (4IR), along with 'smart factories', automation, and robotisation (Raska, 2021). Again, the principle put forward by Alvin Toffler that the mode of production determines the mode of destruction (i.e., warfare) is thus confirmed. The first war of the AI era was Israeli operations against Hamas and Palestinian Islamic Jihadists in 2021 (Operation Watchman on the Walls), when Israel's extremely modern military intelligence used AI in almost every phase of the intelligence cycle (planning and directing operations, data collection, data analysis, and the production of processed intelligence information and its dissemination). A huge amount of battlefield data was acquired through the implementation of the 'Every Soldier is a Sensor' (ES2) concept, as well as through signal intelligence and geospatial intelligence. The use of AI in the process of reconnaissance and targeting (including the prediction of target locations) has made it possible to increase the scale, speed, precision, and lethality of Israeli Air Force attacks.

Among the actors involved in the scientific, technological, and conceptual race for supremacy, in which the US has dominated in recent decades, China has emerged as a fully equal rival. Then there is Russia, as well as second-tier powers, including Israel, which is constantly proving that power can be built not only on quantitative but also on qualitative

potential. Countries of similar stature, namely Australia, France, Israel, Singapore, South Korea, and the UK, can use advanced technologies to strengthen their power and international position. After the post-Cold War 'strategic pause', the return of the global superpower competition is evident, albeit this time at a completely different level of technological development.

The increased role played by information systems and man's entire cognitive sphere should be emphasised. The goal in this domain is to keep one's information systems intact and to weaken or destroy the functionality of one's opponent's systems. It seems that the era of 'information warfare' or 'digital warfare' is being taken over by a broader perspective of automated warfare, where increasingly more decisions will be made by artificial intelligence. Russian 'hybrid warfare', particularly in the first phase of the Ukrainian conflict (the annexation of Crimea), has demonstrated the effectiveness of disinformation and psychological and cyber warfare (which can also be automated, e.g., through bots). In Russia's war with Ukraine, this has targeted the broad social 'audiences' of the conflict in order to manipulate and demoralise them and facilitate operations in other domains. The activities of the Ukrainian side are an example of very effective information warfare conducted in the new media during a conventional conflict.

The changes taking place now seem so significant that AI-RMA will most likely be treated in the future as a distinct phenomenon and the beginning of a new era in military history. IT-RMA consists in integrating digital technologies with existing weapons and conventional systems. Linked with AI-RMA, the extent and nature of human involvement in the wars of the future is analysed in the context of the diffusion of autonomous systems and artificial intelligence, the implementation of new operational concepts, and transformation of the structure of armed forces (Raska, 2021). Chinese theorists argue that only the character of war will change, while its nature will remain the same: war will still be an application of violence for political purposes, and people will remain at its centre. People will still plan, organise, and initiate wars, while the merger of man and machine will amplify the capabilities of human cognition and action (Dahm, 2020).

Discussion of the term

The development of new technologies will have the greatest impact on the creation of a new security environment. The invention and development of fundamentally disruptive technologies which can be utilised in the sphere of external and internal state security seems to be within reach. At the level of the international system, these technologies can affect the global balance of power; at the level of the state and its citizens, new technologies determine changes in internal security policy, where increasingly more space is given to systems of social control and surveillance.

This section discusses the latest emerging technologies that may have military and policing applications, such as artificial intelligence, autonomous systems, hypersonic weapons, directed energy weapons, and the military applications of biotechnology. It also describes new forms of conflict in which the boundary between the civilian and military spheres and between peace and war is blurred. Attention is also drawn to the utilisation of new technologies by states and corporations in order to acquire and aggregate data on citizens and users on a mass scale, which poses great challenges and threats to personal security.

Artificial Intelligence (*AI*), together with its military applications, is an area that requires particular attention. According to the European definition, "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous action" (European Commission. Directorate General for Communications Networks, Content and Technology, 2019).

Artificial intelligence is used, among other things, to acquire and process huge sets of data in intelligence, surveillance, and reconnaissance. Signals intelligence (SIGINT) or imagery intelligence (IMINT) data can be acquired by autonomous systems that monitor a specific territory

or type of activity and then analyse the data using AI. If hostile activity is spotted, the subsequent process (e.g., one that leads to a kinetic response) can also be automated and thus accelerated by reducing or completely bypassing the human factor, i.e., the analyst, who previously had to spend a lot of time, for example, examining images from reconnaissance drones.

In the case of open-source intelligence (OSINT), AI seems essential for the selection and analysis of huge data sets (Big Data). Some techniques within AI which are applicable here include speech recognition (in multiple languages and recorded in adverse conditions), translation, and recording; the geolocalisation of images (even when metadata is lacking); the use of 2D images to represent objects in 3D models; and the creation of predictive analytics.

Artificial intelligence is also revolutionising the Command and Control field. In the US, the concept of 'Joint All Domain Command and Control' (JADC2) is being developed to centralise the planning and execution of operations on land, in the air, in space, and in cyberspace. AI will be used to combine data from sensors located in all these domains and provide decision-makers with a single information (analytical) product, which in this context is called a 'common operating picture' (COP). Until now, data has come from multiple sources, has differed in format, and has included inconsistent content or redundant detail. AI can find applications in military logistics (e.g., the predictive maintenance of aircraft or vehicles), cyber operations (e.g., the detection of anomalies in a system at a stage when prevention is possible), and psychological operations (e.g., the creation of deep fakes, thanks to the possibility of fabricating highly realistic images and audio or video recordings).

Advanced work is underway to implement AI into semiautonomous or autonomous drones, vehicles, and watercraft, where it is intended to record the environment, recognise conditions, combine data from different sensors, plan navigation, and maintain communication with other craft. Aerial experiments test the responses of unmanned systems to unprogrammed circumstances, such as changes in the weather. Based on artificial intelligence, swarming tactics for unmanned vehicles are being developed. Swarming can involve the use of a large number of low-cost unmanned vehicles to overwhelm an enemy's defence system, or small squadrons can be used for electronic warfare, fire support,

navigation support, or ground unit communications. Characteristics of this type of unmanned vehicles that operate in a swarm include:

- Autonomy (no centralised control);
- Ability to identify the local environment and that of other nearby swarm units;
- Ability to communicate with nearby swarm units;
- Ability to cooperate on a given task.

Work on the military use of artificial intelligence is being carried out by a number of countries. The momentousness of this race can be seen in the statement of Vladimir Putin, in his statement that "whoever becomes the leader in [AI] will become the ruler of the world" (Sayler, 2021).

Lethal Autonomous Weapon Systems (*LAWS*) are capable of both identifying a target as hostile and using the weaponry they possess to destroy it without any control from the human operator. In this scenario, the human is outside the decision-making loop, hence fully autonomous systems are called 'human out of the loop' systems. In addition, a distinction is made between combat systems where human monitors can stop an attack ('human on the loop' systems) and semi-autonomous systems where unmanned vehicles can attack only single targets or defined groups of targets set by an operator ('human in the loop' systems). There is rational justification for having such weaponry: on the battlefield, communications may break down, in which case an unmanned vehicle that is unable to operate fully autonomously is useless. Another argument is linked to operational precision and the possibility of reducing accidental civilian casualties and collateral damage to property. However, the US has announced that it does not have fully autonomous LAWS in the armament of its military forces. Many states and organisations are calling for their ban because they pose enormous legal and ethical problems and lead to potential political-military risks (Kopeć, 2016; Sayler, 2021).

Hypersonic weapons are weapons that reach speeds greater than Mach 5 (i.e., five times the speed of sound). A distinction is made between:

- Hypersonic Glide Vehicles (HGV), which are launched on missiles adapted from ballistic missiles; after the ascent phase, they proceed to 'glide' at a ceiling of 40–100 km and manoeuvre towards the target at speeds of up to 20–25 Ma. It is also possible to launch

hypersonic missiles from aircraft (Air-Launched Ballistic Missile, ALBM),
- Hypersonic Cruise Missiles (HCM), which can fly at low altitudes at 5–8 Ma thanks to a special type of jet engine. The same technology is used to build hypersonic aircraft and drones.

Unlike ballistic missiles, HGVs and HCMs do not follow a parabolic trajectory but can manoeuvre before reaching their target, making it much more difficult for the opponent to defend. Reaction time in such situations is very short and miscalculations and the triggering of unintentional escalations are possible. Perhaps defence against hypersonic weapons will also be possible thanks to systems using AI and automation. Work on such weapons is being carried out in the US, China, and Russia; it is expected that China could potentially use hypersonic weapons in the South China Sea (Piotrowski, 2019; Sayler, 2021).

Directed energy weapons (*DE*) use concentrated electromagnetic energy to incapacitate, damage, disable, or destroy enemy equipment, facilities and/or personnel. This is a modern, low-cost and mostly non-lethal type of weaponry that is mainly useful for suppressing demonstrations and violent crowd gatherings. One of its forms involves the generation of a permanent magnetic field with a strength of 1000–10000 times that of the Earth's magnetism. Such a field directed at a human being incapacitates the person and prevents him being able to move freely. This solution has been suggested as a form of military protection against divers attacking seaports. Microwave weapons that employ thermal radiation should also be mentioned here. 'Microwave throwers' can be mounted on vehicles or helicopters. When a human body is exposed to this radiation, the internal water content is heated. According to experts, "the radiation emitted by the weapon is able to penetrate clothing and cause a temperature rise of up to 54°C within 2 seconds, which is 9°C above the temperature-induced pain limit. Its purpose is to fight crowds and mass demonstrations; its range is up to 750 metres. Recent tests have shown that people 'hit' with the beam feel a burning pain after only two seconds. After less than five seconds, the pain is unbearable and the attacked person will do anything to escape from the field of fire. Then the pain disappears with no trace and no injury" (Wnuk, Matuszewski & Chudy, 2015, p. 93). The non-thermal radiation generated by microwave weapons causes "neurotic symptoms,

pulse disturbances, tingling in the arms and legs, rapid fatigue, insomnia, sweating, dizziness, and extreme nervousness [...]. With the use of microwaves, vital functions such as breathing or heartbeat can be affected" (Wnuk et al., 2015, p. 93).

Weapons that use light – visible, infrared, or ultraviolet – as a corrosive agent are also available. Visible light attacks the vegetative nervous system. As a result of its prolonged stimulation by luminous optical stimuli, the heart, blood circulation, and metabolism are disrupted. As experts write, "the result is constant sleepiness during the day and insomnia during the night" (Wnuk et al., 2015, p. 93). Similar effects of imbalances in the functioning of the human body are caused by infrared pulses. Like sonic and microwave weapons, light-based weapons can be effectively applied in the area of public security, e.g., to suppress illegal demonstrations and aggressive crowds (Wnuk et al., 2015).

Laser weapons that use the effect of light amplification through the forced emission of radiation are yet another type of weaponry. In recent years, lasers have usually been discussed in the context of the militarisation of space. The US aims to launch satellites armed with laser guns, and the possibility of using lasers as anti-satellite weapons is also considered.

In the context of conventional weaponry, it is entirely feasible to use powerful electromagnetic pulses (i.e., at the microwave level) such as an electromagnetic bomb or an 'E-bomb', which emits an extremely strong electromagnetic wave of billions of watts. According to experts on the subject, "the energy sent out propagates through the surrounding space and reaches all kinds of electronic devices. The alternating electric and magnetic fields that constitute this wave induce voltage changes in the circuits of the devices and destroy them or severely disrupt their work" (Wnuk et al., 2015, p. 94).

In the context of directed energy weapons, the US *High Frequency Active Auroral Research Program* (*HAARP*) must not be overlooked. This is a mysterious programme, surrounded by contradictory explanations from the US authorities and never fully confirmed hypotheses about its actual purpose. It is located in Alaska and consists of technical buildings and a 24-hectare area covered with specialised antennas. These antennas are capable of emitting radio signals that directly interact with the ionosphere. This is a scientific and research facility but it is obvious

that, at least in the past, it has played a military role, primarily as an anti-missile system. The pulses generated by the antennas could literally push a portion of the ionosphere into space and thus alter the trajectory of ballistic missiles. It is widely believed that HAARP can cause weather changes and lead to floods, droughts, etc.; thus, it can be classified as a meteorological weapon. This system can also control extremely low frequency (ELF) waves, which are used to affect brain and bodily functions. Thus, HAARP can also be classified as a psychotronic weapon used to lower the cognitive performance of the population, e.g., in times of war. ELF waves have an enormous range and can penetrate the soil and deep underground structures. They have been used to communicate with submarines and, with excellent efficiency, to detect underground deposits of natural resources. They can also have a colossal impact on nature and living organisms and can trigger natural disasters (e.g., earthquakes or tsunamis). Thus, HAARP is a major step forward in the development of geophysical weapons which involve the use of natural forces to exert a devastating effect on the environment (Kotasińska, 2012; Wrzosek, 2018).

Biotechnology offers such great possibilities for the military sphere that some even describe the changes taking place using the term 'biotechnological RMA'. Thanks to neuroimaging of the brain – specifically techniques such as functional magnetic resonance imaging (fMRI), computed tomography (CT), electroencephalography (EEG), magnetoencephalography, and positron emission tomography (PET) – it is possible to track the activity of ensembles of neurons and specific brain centres, which in turn makes it possible to discover the relationships between biological mechanisms occurring in the brain and human cognitive activity and behaviour. Consequently, neuroimaging of the brain may find application during recruitment processes in the armed forces, in which it could be utilised to profile candidates for suitability, predict their response to stressors, and to assign them to various functions and tasks.

The use of biosensors placed, for example, inside or on the body of soldiers makes it possible to monitor their psychophysical state on the battlefield. The US has conducted experiments with biosensors that measured glucose, lactic acid, cortisol, and histamine levels in soldiers' bodies. Chips placed in soldiers' bodies could replace traditional identification 'dog tags'; they might include biomedical data that could save

a soldier's health or life, allow a soldier's body to be tracked at a distance, and allow troops to be identified and located (and thus obtain better situational awareness of the location of soldiers, robots, and equipment).

Neuromodulation involves invasive or non-invasive stimulation of the brain. Non-invasive methods include magnetic, electrical, and ultrasound stimulation. This type of treatment makes it possible to improve motor function, sleep quality and efficiency, pain tolerance, attention, concentration, willingness to take risks, visual memory, alertness, arousal, and concentration. Thus, the appropriate neuromodulation can enhance a soldier's performance during combat tasks ('combat mode') and support and accelerate the recovery process after mission accomplishment ('recovery mode').

Modern bionics applied in the military sphere primarily offers methods of treating disability in the form of bionic prostheses for veterans who suffer from paresis or paralysis. The idea is to create an interface (connection) between the human brain and a machine, in this case, e.g., a prosthesis which imitates a hand, which the human can control thanks to nerve signals. In the future, it will probably be possible to control advanced weapon systems using 'thoughts' (although this is unlikely to produce satisfactory results compared to fully autonomous systems). Even more advanced projects concern the construction of a brain-computer-brain interface, which would allow people to exchange information without additional devices, telephones, or physical links. Understandably, all these projects raise huge ethical concerns (Kamieński, 2014; Waszewski, 2021).

Brain science, artificial intelligence, and biotechnology are at the forefront of Chinese efforts gain the advantage in the war of the future. General Liu Guozhi, who is in charge of cutting-edge military technology, has stated that

> [t]he combination of artificial intelligence and human intelligence can achieve the optimum, and human-machine hybrid intelligence will be the highest form of future intelligence (as quoted in Kania, 2019, p. 84).

General He Fuchu, another Chinese military official active in this field, stated that "the sphere of operations will be expanded from the physical domain and the information domain to the domain of consciousness; the human brain will become a new combat space" (as quoted in Kania, 2019, p. 85). While Western countries are limiting this kind of

research due to costs and ethical considerations, China has launched the China Brain Project 2016–2030, which aims to create an effective brain-machine-brain interface and consequently enable the use of brain networks on the battlefield. Experiments with monkeys (macaques) have been documented: in one, researchers inserted the MCPH1 gene, presumably responsible for brain development, into an embryo to create a transgenic macaque, which indeed subsequently showed better performance in short-term memory tasks, although the brain took longer to develop; in another highly controversial experiment, human cells were added to macaque embryos, which consequently resulted in human-animal chimeras (Kania, 2019).

Another area which requires particular attention concerns the protection of the human genome, i.e., the complete set of genetic information of a given organism, which was first obtained in 2003. The stealing of huge sets of genetic data by actors who intend to exploit them aggressively is a particularly threatening possibility. Genome information could be an excellent tool for profiling victims of new precision-guided biological weapons or for building immunity in the population. In many countries, there are no effective genome protection laws. In this context, some even talk of 'genetic neo-colonialism', whereby powerful actors collect genetic data in third world countries. The largest collections of genetic data are currently located in China, at the China National GeneBank, which was established in 2016 and receives data from all over the world. The CRISPR system, which allows genomes to be edited, was used by China for the first time in 2016. In 2018, Chinese scientists, presumably with their government's approval, created the first 'gene-edited babies' (Sayler, 2021). A supercomputer with enormous computing power, called Tianhe-2, is used to analyse genomic data. According to Kania,

> this access to genomic information combined with continued advances in artificial intelligence could contribute to advances in understanding of the evolution of the human brain and genomic determinants of intelligence (Kania, 2019, p. 93).

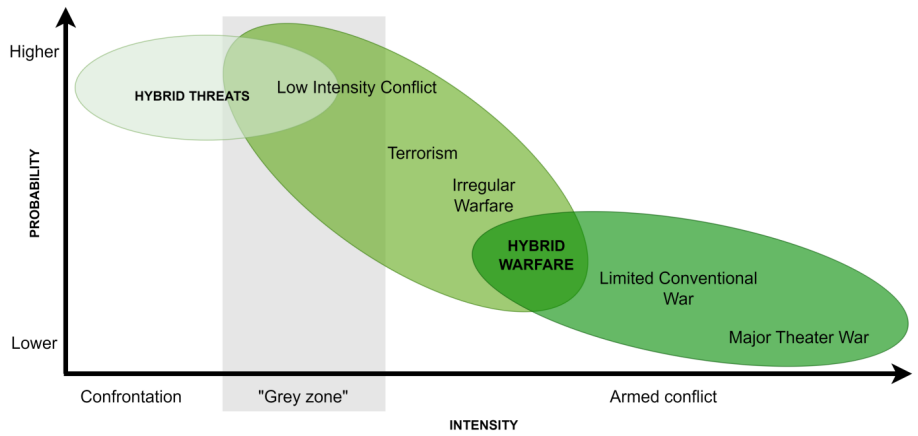
In the future, this is expected to open up the possibility of 'augmenting' the human mind and achieving a state of what in Chinese is called *zhinaoquan*, which can be translated as 'mind/mental dominance', 'mind/mental superiority', and 'cognitive superiority', and will allow China to claim victory over its rivals.

Other disruptive technologies that could have a revolutionary impact on the military sphere include quantum technologies, advanced materials, and space technologies that enable the progressive militarisation of space.

A pronounced post-Cold War trend is the blurring of the boundary between war and peace and between the civilian and military spheres. Technological developments, the popularisation of cyberspace, and the elevation of the role of cognitive operations have been strong catalysts in this area. Through an unusual combination of technology and tactics, illegal non-state actors are developing new capabilities and peculiar new niches to operate in. States, which are legitimate actors, use atypical forms of operation in order to exploit the resultant cognitive confusion in achieving their own goals without causing undue escalation.

It is rather difficult to define these types of threats or methods of warfare as they are designed to be fuzzy, surprising, and beyond the imagination of the victims of the attack. Contemporary conflicts should be seen as a kind of continuum in terms of intensity and probability (see Figure 1). Between non-violent confrontation and armed conflict, there lies an additional 'grey zone', where instances of isolated kinetic incidences in the form of kidnappings, assassinations (e.g., the assassination of Sergei Skripal), as well as cyber-attacks and hostile business activities are possible.

Figure 1. A continuum of contemporary conflict



Source: own elaboration based on (Monaghan, 2019).

It is a mistake to call every threat or crisis a 'war', which is often the case when the term 'hybrid war' is overused in the media. In the aforementioned continuum of contemporary conflict, Sean Monaghan (2019) distinguishes such phenomena as:

- Hybrid threats, which are a broad spectrum of combined measures of a non-violent nature that target weak and vulnerable points across the whole of society in order to disrupt its functioning, undermine its unity, weaken its determination to pursue its goals, and compromise and subvert the status quo. This strategy is used by revisionist actors to gradually achieve their goals without triggering decisive reactions, including armed responses. Hybrid threats mainly target the population and centres of power.
- Hybrid warfare, which is a challenge arising from the increasing complexity of contemporary armed conflicts and changes in the nature of war. It involves combining different types of military action with non-military means to neutralise an opponent's conventional military power. Hybrid warfare aims to reduce the effectiveness of the opponent's armed forces and increase the effectiveness of its own armed forces.

Modern warfare can thus be described as a mix-and-match type, where, in order to surprise the opponent, the participants select different forms and methods of action. Therefore, even in the same conflict, there are simultaneous manifestations of war from before the Third Industrial Revolution, from the IT-RMA period, and from the AI-RMA period that is beginning right now.

The blurring of the boundary between the civilian and military spheres means that entire populations are drawn into the interest of states and their security and defence agencies. Internet technologies offer excellent opportunities for bulk data collection on citizens or, to put it directly, mass and unlimited surveillance of citizens. This is justified on grounds such as the threat of terrorism, the fight against crime, sanitary considerations, etc. In practice, it means violating privacy, stifling freedom of expression (as a result of the chilling effect), and treating citizens as a priori suspects of criminal acts (during preventive surveillance) (Rojszczak, 2020).

Global actors which provide various internet services, such as Google, Apple, Facebook, Amazon, and Microsoft in particular, are in

a possession of an enormous amount of personal data, which allows them to control the social and political processes taking place. This is happening without any democratic mandate, control, or accountability. The deletion of the social network accounts of a sitting US president or a major political group in Poland demonstrates how digital giants threaten freedom of speech and expression. Consequently, they influence the outcome of elections, i.e., decide who holds political power. The aim is to stimulate socio-cultural change, co-create broad political processes, and generate commercial profit.

These corporations can afford to be so aggressive as a result of the passivity of the majority of internet users, who are addicted to digital stimuli, technological innovations, and the conveniences offered by applications; they also lack the will to subjugate the increasingly diverse and overwhelming technological environment. At present, social media is the most important data set for profiling users. With the implementation of the Internet of Things and smart city projects, there will come ubiquitous sensorisation, i.e., the deployment of sensors which collect vast amounts of data about people's activities.

In countries where attempts are made to limit the field of action of giant digital corporations, their negative role is usually taken over by the state. An example is China, which is implementing a data-driven government project. Heated discussions held around the world have been stirred up by the points-based Social Credit System in China, which is supposed to allow people to be assessed for their usefulness to society. A low score results in a number of inconveniences, such as not being allowed to use air transport or high-speed rail (which de facto means social segregation). The system is still being developed and its implementation is uneven across the country; so far, mainly enterprises have been covered by this system, and only 0.15–0.3% of Chinese citizens per year have been blacklisted (Drinhausen & Brussee, 2021). However, this is only a part of China's entire surveillance apparatus.

The surveillance systems described above are part of global trends in security. The term 'dual-use technologies' does not simply mean that certain technologies proven in the military sphere find civilian application after some time (or vice versa). A more appropriate term would be 'simultaneous-use technologies'. These two spheres have converged, and measures used in the civilian sphere have simultaneous applications

in the security sphere. For example, a smartphone with a geolocalisation function simultaneously facilitates users' navigation and, if necessary, provides security authorities with information about their location.

Systematic reflection with conclusions and recommendations

Technological advancements have always influenced the military and security spheres, but the scale and depth of contemporary changes are unprecedented. The progressive proliferation of the technological environment and the extent of its impact on the social and natural environments creates enormous threats and challenges. As Błażej Sajduk (2020) observes, the impact of the technological factor on the social sphere can be assessed from positions that range from optimism to pessimism and from determinism to constructivism. Optimists believe that successive phases of technological development represent a simple and beneficial progression from earlier stages, whereas pessimists argue that technology is not a neutral tool but an instrument for the exercise of power by certain actors over other actors. Proponents of technological determinism assume that technological development is an independent variable that exerts a direct and causal impact on the social, political, and economic spheres (thus, the development of societies is determined by the technology of the means of production: 'machines make history'). Finally, social constructivists see the proliferation of technology as "a process that interacts with other social forces, which is co-constructed by them, and through which it is influenced by, e.g., politics, culture, and economics" (Sajduk, 2020, p. 95).

In the context of technologies used in security, it is obvious that they serve to exercise power, control, and surveillance. Their vast proliferation begs questions about their purpose and effectiveness: at the international level and in the geostrategic dimension, a resurgence of superpower rivalry has been noticed; in the military arena, another technology and arms race has begun; in the civilian and private sphere, new and increasingly extraordinary security measures are applied; at the level of social life and individual security, new social pathologies have emerged, linked to, e.g., cyberspace or cyber disorders which adversely affect the

psychological and somatic spheres. One has to agree with researchers (K. Zybertowicz & A. Zybertowicz, 2017) who see technological development that is too fast and takes place simultaneously in too many fields of social life as the source of the general crisis of the Western world. It also leads to people experiencing a lack of a sense of security, agency, and control over their lives. In the future, "it will not be possible to preserve the Western world of freedom, pluralism, and concern for the weak, nor the legal procedures that offer protection against abuses of power wielded by political and oligarchic actors, without a significant global slowdown in technological development" (K. Zybertowicz & A. Zybertowicz, 2017). Of course, it can be predicted that new categories of personal and civil liberties will be adopted, although they will most likely be significantly different from the previous liberal notions.

Analysing globalisation processes that are closely linked to technological development helps to assess whether the future of the social sphere will proceed deterministically or whether the course of events can be controlled. On the one hand, some point out the objectivity of globalisation changes, their independence from political decisions, and their general irreversibility (Pietras, 2015). On the other hand, it is clear that, from its inception, globalisation has been a phenomenon full of internal contradictions and paradoxes. For example, in the context of the military technologies described above, it is not surprising that globalisation and openness in knowledge and technology is contrasted by an opposite tendency, namely fierce competition and clandestine efforts in the field of disruptive technologies. Globalisation, centralisation, and integration are accompanied by their internal opposites in the form of localisation, decentralisation, and fragmentation. As experience shows, globalisation processes can also be halted by unpredictable events, as was the case with the COVID-19 pandemic, when there was a breakdown of global market linkages and a relapse into protectionist practices. This offers hope that, to some extent, demands to limit the proliferation and deployment of some of the disruptive technologies that emerge within the Fourth Industrial revolution are feasible. A historical example of such self-restraint is nuclear weapons and the successful attempts of international regimes and disarmament agreements to prevent their use during the Cold War. Today, however, it is difficult to count on the ability of some states and economic actors to make concessions in so many spheres.

Current technological developments are characterised by a rapid pace and a profound and multi-faceted impact on the entire social sphere. The intensity of change means that, over time, politics or culture have diminishing possibilities to limit the spread of technology, as this would also be economically disadvantageous for the major players. Nor is this spread hampered by crises and problems directly linked to globalisation. The COVID-19 pandemic slowed down economic globalisation but intensified the use of technological tools used for population control. From this perspective, it is to be predicted that the future looks pessimistic and that technological development will be increasingly deterministic.

References

Braudel, F. (1982). *On History*, trans. S. Matthews, Chicago: Chicago University Press

Dahm, M. (2020). *Chinese Debates on the Military Utility of Artificial Intelligence. War on the Rocks*. https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/. Accessed 05.08.2022.

Drinhausen, K., & Brussee, V. (2021). *China's Social Credit System in 2021. From fragmentation towards integration* [*Mercator Institute for China Studies (MERICS)*]. https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration. Accessed 05.08.2022.

European Commission. Directorate General for Communications Networks, Content and Technology. (2019). *Publications Office*. file:///C:/Users/48606/Downloads/ai_hleg_ai_definition_final_DF06F793-EA01-3573-16D2ACD625E2BDB0_56341.pdf. Accessed 05.08.2022.

Kamieński, Ł. (2014). *Nowy wspaniały żołnierz. Rewolucja biotechnologiczna i wojna w XXI wieku*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Kania, E.B. (2019). Minds at War. China's Pursuit of Military Advantage through Cognitive Science and Biotechnology. *PRISM*, *8*, 82–101.

Kopeć, R. (2016). Autonomia systemów bojowych. *Przegląd Geopolityczny*, *17*, 133–147.

Kotasińska, A. (2012). HAARP – "puszka Pandory" XXI wieku. *Zeszyty Naukowe Ruchu Studenckiego*, *1*, 60–73.

Monaghan, S. (2019). Countering Hybrid Warfare: So What for the Future Joint Force?. *PRISM*, *8*, 82–99.

Pawłuszko, T. (2018). Analiza gospodarki-świata według Fernanda Braudela. *TEKA of Political Science and International Relations*, *12*, 125–146.

Pietraś, M. (2015). Przestrzeń badawcza nauki o stosunkach międzynarodowych. *Politeja*, *12*, 65–97.

Piotrowski, M.A. (2019). Perspektywy wyścigu zbrojeń hipersonicznych między USA, Chinami i Rosją. *Biuletyn PISM*, *32*.

Raska, M. (2021). The Sixth RMA Wave. Disruption in Military Affairs?. *Journal of Strategic Studies*, *44*, 456–479.

Rojszczak, M. (2020). Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego. *Studia nad Autorytaryzmem i Totalitaryzmem*, *42*, 207–243.

Sajduk, B. (2020). Konceptualizacja wpływu czynnika technologicznego na międzynarodowy wymiar bezpieczeństwa. Determinizm technologiczny i proliferacja broni. In: P. Bajor (ed.), *Bezpieczeństwo międzynarodowe. Aspekty metodologiczne i systemowe*. (pp. 87–104). Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Sayler, K.M. (2021). *Emerging Military Technologies. Background and Issues for Congress (No R46458; CRS Report). Congressional Research Service*. http://crsreports.congress.gov/product/pdf/R/R46458/8. Accessed 08.05.2022.

Waszewski, J. (2021). *"Nie ukryjesz się". Konsekwencje synergii big data, mediów społecznościowych i neuronauki*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Wnuk, M., Matuszewski, J., & Chudy, Z. (2015). Nowe technologie i urządzenia rażenia elektromagnetycznego w dziedzinie walki elektronicznej. *Przegląd Elektrotechniczny*, *91*, 92–95.

Wrzosek, M. (2018). *Wojny przyszłości. Doktryna, technika, operacje militarne*. Warszawa: Wydawnictwo Fronda.

Zybertowicz, K., & Zybertowicz, A. (2017). Okiełznać zmianę. Bezpieczeństwo ontologiczne, rozwój technologiczny a kryzys Zachodu. *Filo-Sofija*, *17*, 521–538.