CENTER FOR SECURITY AND MILITARY STRATEGIC STUDIES
UNIVERSITY OF DEFENSE IN BRNO

TECHNOLOGICAL DEVELOPMENT

IMPLICATIONS FOR THE CAPABILITIES OF THE CZECH ARMED FORCES 2019

JAKUB FUČÍK ET AL.

TECHNOLOGICAL DEVELOPMENT
IMPLICATIONS FOR CZECH ARMED FORCES CAPABILITIES 2019

JAKUB FUČÍK ET AL.

BRNO 2020

AUTHORS

Mgr. et Mgr. Jakub Fučík, Ph.D.

Ing. Fabian Baxa, Ph.D.

PhDr. Libor Frank, Ph.D.

doc. Ing. Josef Procházka, Ph.D.

This analytical study is a partial result of the *STRATAL project - Strategic Alternatives,* solved at the University of Defense in Brno.

Reviewers:
Gen. Ing. Miroslav Feix, M.S. – Commander, Army Cyber and Information Operations Command. Czech Armed Forces.

Col of Gen. Staff doc. Ing. Petr Františ, Ph.D. - Head of the Department of Informatics and Cyber Operations, Faculty of Military Technology, University of Defense in Brno

Lt Col of Gen. Staff Ing. Jan Farlík, Ph.D. - Deputy Head of the Department of Air Defense and Vice-Dean for External Relations and Development, Faculty of Military Technology, University of Defense in Brno

Centre for Security and Military Strategic Studies (CSMSS)

The Centre for Security and Military Strategic Studies (CBVSS) is a part of the University of Defence and is defined as another workplace for education and creative activity according to Act No. 111/1998 Coll., Section 22(1)(c).

It has the following mission:

- Scientific and research activities in the field of security studies, strategic leadership, military art, strategic management and defence planning, carried out for the purposes of strategic level of decision-making, state defence management and the construction of the Czech Armed Forces.
- Preparation of military and civilian experts of the Ministry of Defence and the Armed Forces in professional and career courses (KGŠ, KVD).
- Expert, publishing and popularization activities (among other things, it guarantees the publishing of the magazines *Vojenské rozhledy* and *Obrana a strategie*).

ISBN978-80-7582-345-8

INTRODUCTION

The aim of the analytical study is to evaluate the trends in technological development and their implications for the Czech Armed Forces in 2019. The ambition of the Centre for Security and Military Strategic Studies of the University of Defence (CBVSS) is to provide an alternative contribution to the discussion of technological consequences for the formulation and implementation of effective defence policy of the Czech Republic and the capability building and development of its armed forces (primarily the Army of the Czech Republic). The document should serve as a periodic evaluation of the issue and thus provide basic way-outs for further research. In this sense, the study is directly related to the evaluation of technological trends for 2017 and 2018.[1]

The study is based on the analysis and comparison of open sources, which relate to the nature of current trends in technological development and its relevant examples. The implications for the Armed Forces of the Czech Republic (ACR) are analysed using the so-called Main Capability Areas (MCA) defined through the NATO methodology.[2] For each trend, areas of capabilities are identified that are directly affected by its development and are of immediate importance to the entity concerned (for a summary, see the final table). At the same time, it is necessary to note that although the individual trends and their implications are analysed and described gradually, their nature cannot be perceived separately.

The reader should always consider the "overarching" theme of the impact of technological development on the armed forces, or society in general, and the interconnectedness of the trends concerned. The same comprehensive approach is relevant to the MCA analytical framework used and the specific capabilities identified. The study is time-framed to 2019 and focuses on trends that may directly affect the armed forces. The verification of the outputs was carried out within expert meetings and a workshop with the participation of members of the Ministry of Defence of the Czech Republic, the Czech Armed Forces and representatives of the security community of the Czech Republic.

[1] See FUČÍK et al. *Technologický vývoj: Implikace pro schopnosti ozbrojených sil ČR 2018* [online]. Brno, CBVSS UO, 2019. Available at: https://bit.ly/3c7WKvE

[2] MC 400/3, MC Guidance for Military Implementation of Alliance Strategy. 2012.

GROWING IMPORTANCE OF "NEW" STRATEGIC DOMAINS

In addition to the traditional dimensions of strategic thinking and leading armed conflicts (land, sea and air), space and cyberspace have become increasingly important, regardless of whether individual states/international organizations consider these domains to be separate or part of other dimensions (e.g. cyberspace as part of the information domain within the Russian approach).

OUTER SPACE

As in previous years, there is a growing interest from both state and non-state actors in this domain. At the national level, we can identify the strategic direction of development of space capabilities, which would ensure, or support, the ability to project (military) power on a global scale. Space assets provide global communication, navigation, intelligence or enable the use of advanced (weapons) systems such as precision-guided munitions or remotely controlled and autonomous systems. This approach reflects the nature of outer space and emphasizes, in particular, the fact that any place on the Earth's surface is directly accessible from its orbit, regardless of the terrain, altitude or remoteness (not only of the rest of "civilization", but also of the mainland itself). Similarly, it is not necessary to use, or disturb, state borders, airspace or territorial waters of other states.

NATO responded to this aspect last year, recognizing space as another separate operational domain.[3] However, as a result of the temporary lack of follow-up, such as the creation of strategy documents focused solely on this domain, it is not yet possible to determine precisely how this decision will impact the Alliance as a whole, or its individual Member States. In the US, the Congress passed and approved the creation of the United States Space Forces as a separate component of the United States Armed Forces (founded on December 20, 2019).[4] At the same time, through the updated version of the *Missile Defense Review*[5] document, within the missile defence system (in addition to strengthening the space sensor component) the idea of developing and deploying weapons systems designed to intercept ballistic missiles in the ascending phase of the flight (*boost phase*) was revitalized. A similar trend is evident not only in the People's Republic of China (within the People's Liberation Army Strategic Support Force) and the Russian Federation (within the Russian Aerospace Forces), i.e. the main "challengers" of the United States, but also other regional powers. President Macron's authorization of the French Space Forces in July 2019[6] is an example.

Also, the role and increasing importance of non-state actors (especially represented by the private SpaceX-type companies), who in fact privatize space research and development of related capabilities, cannot be overlooked. In addition to space carriers, they are gradually moving towards human-crewed flights, which were originally reserved for states or state/international organizations. In 2019, both Boeing and SpaceX

[3] NATO. *Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain* [online]. 2019. Available at: https://bit.ly/3ernSHB
[4] MYERS, M. The Space Force is officially the sixth military branch. Here's what that means [online]. *Air Force Times*, 2019. Available at: https://bit.ly/3c3Wo95
[5] U.S. DoD. *Missile Defence Review* [online]. 2019. Available at: https://bit.ly/2TL1H7j
[6] ZIHNIOGLU, K. Macron announces creation of French space force [online]. *AFP*, 2019. Available at: https://bit.ly/36wp8q4

successfully tested their modules[7] and the first manned flights are scheduled for 2020. On one hand, this phenomenon brings better availability of the systems and capabilities concerned (e.g. by reducing the cost per kg transported to orbit) due to competition between individual private companies). On the other hand, there is a reduction of state control over the systems that will be placed in orbit. This situation further "obscures" the dual-use problem described below.

Generally, the potential of space and relevant technologies can be divided into two groups - civilian and military - with the dividing criterion being the nature of activities or real artificial bodies (satellites, stations, etc.) operated in space. The civilian group includes, for example, the building and consequent use of satellite networks designed to monitor the weather, to transmit television signals, etc. The military group includes, for example, spy satellite networks, satellite navigation of military units or weapon platforms designed to intercept ballistic missiles, etc.

In accordance with the definition below, the so-called anti-satellite weapons (*ASAT*) cannot be neglected, which may be located on the earth's surface or sea surface, but their use is directly meant for space. The group of states that have officially successfully tested such weapons systems (China, Russia, USA) includes India since last year[8] through the conversion of technologies used for the construction and development of its own anti-missile "umbrella".

At the same time, it is necessary to mention that the boundary between the two categories is very unclear or that the two groups often overlap in their elements and their differentiation in practice is relatively difficult. Thus, there is a persistent phenomenon of dual use of the relevant technologies or activities. For example, the satellite navigation network can be used not only to determine the position of civilian entities, but also to coordinate the operations of operational battle groups or guiding missiles or unmanned aerial vehicles (reference to the US GPS system or different types of services to be provided through the European Galileo system). Similarly, the usability of built satellite networks for global communication and 5G Internet coverage (currently OneWeb or LeoSat) can be evaluated.

The use of satellite systems is increasingly available to small states in terms of technological development (miniaturization), capacity sharing and the emerging role of private space companies. Last year, this phenomenon was also demonstrated by the Czech Republic through the completion of the SATCEN Satellite Center, which reached full operational readiness by January 1, 2020. The Centre is managed by Military Intelligence and enables the acquisition and analysis of electro-optical and radar image data from space reconnaissance.

The outer space is increasingly important for the ability to project (military) power of the state and plays a role in the field of providing national security. NATO responds to this development through recognizing space as another separate operational domain. At the same time, the role of private companies is growing, developing capabilities originally reserved to states or international organizations. Use of space is very closely

[7] NASA. NASA, Partners Update Commercial Crew Launch Dates [online]. 2019. Available at: https://go.nasa.gov/3c67yub; MALIK, T. Boeing's 1st Starliner Spacecraft Lands in New Mexico After Shortened Test Flight [online]. *Space.com*, 2019. Available at: https://bit.ly/3caCWYh

[8] CHAUDHURY, D. R. Explained: What's Mission Shakti and how was it executed? [online]. *The Economic Times,*2019. Available at: https://bit.ly/36y9oCV

connected with the phenomenon called dual-use, blurring the boundaries between civilian and military sectors.

Implications for the Armed Forces of the Czech Republic

The growing influence of the **outer space** (possibly also as a separate operational dimension) imposes new requirements on the armed forces MCA "*Prepare/Training*", which must take into account the specificities of this domain. Although at first glance the approach to this dimension may be "exotic" and distant from the goals and capabilities of the Czech Army in particular, the broader context of both the European Union and NATO cannot be overlooked. Membership in these institutions represents the potential for gaining access to different types of space systems (navigation, communication or monitoring) and using them to develop relevant capabilities. This aspect is further strengthened by the NATO's recognition of the universe as a separate operational domain, which for Czech Armed Forces creates conditions for further cooperation throughout the organization. Similarly, the increasing opportunities arising from the privatization/commercialization of this area can be assessed as an opportunity, albeit with the hidden threat of dependence on such an actor associated with potentially different interests or unclear control over its activities. In connection with the security interests and character of the Czech Republic, or its armed forces, the focus should be on projects and activities strengthening the main capability areas: *Project; Consult, Command and Control* (C3); *Protect; and Inform*. These prerequisites are met by the above-mentioned development of the Galileo navigation system or the provision of data for the needs of (strategic) IMINT through international cooperation with the European Union Satellite Centre (EU SatCen), or purchases from private providers. Similar involvement can be expected at the national level from the involvement and exploitation of the Satellite Centre. All these projects can be used not only for the development and strengthening of a comprehensive C4ISR system, but also for providing a robust information flow for the control of unmanned and autonomous systems.

CYBERSPACE

Strengthening the strategic importance of cyberspace is directly linked to the development of information technologies and their use in virtually all areas of human life. Information globalization enables any actor (state and non-state) to have almost instantaneous and unrestricted access to a vast amount of data and their subsequent processing and use for their own needs. In this sense, the information, or "raw" data, is gradually becoming a strategic commodity usable both for shaping the position in this dimension and for shaping the functioning of the real environment.

From the perspective of state and non-state actors, ensuring permanent and secure access to this domain is in fact a prerequisite for the effective fulfilment of their own interests. In this sense, the so-called cyber-attacks or malicious cyber activities - for example in the form of the ability to deny an opponent's access to this domain - represent important tools for achieving the set goals,[9] which are generally characterized not only by a very favourable utility ratio (investment/profits from the discussed activities), but also reduced ability to attribute such attacks and low probability to be punished by the injured entity.

[9] Cf., e.g., NATO. Strategic Foresight Analyses. 2017.

The development of the *Internet of Things* (IoT) is gradually evolving into the *Internet of Everything* (IoE), which not only facilitates more effective use of the comprehensive information links (e.g. to ensure monitoring and decision-making in real time), but also deepens the overall dependency on the stable and efficient operation of this space, resulting in user vulnerability. Building and development of 5G information networks takes the discussed issue to a qualitatively higher level, both in terms of opportunities and potential threats. At present, ensuring security, particularly of critical information infrastructure, must take this trend into account. Especially considering the potential abuse of many debated devices within the so-called botnets to conduct targeted attacks against the information systems of both relevant state and non-state actors (for example, attacks on the availability of Telegram services in Asia in 2019[10]).

Simultaneously with the intensification of the interconnection of humanity within this area, there is an increase in the number of networks, which are created and used on the distributive principle, i.e. without the existence of a central control or management "node". One such approach is the so-called "blockchain" technology, which is used by current cryptocurrencies and is gradually being introduced in other areas (e.g. banking[11] or data management and sharing[12]). The final form of this trend is an increase in the importance of the so-called "deep web", or in a narrower sense with the security connotations of "dark web" and "darknet".[13] Particularly, dark web/darknet is directly linked to illegal activities across all areas (from illegal information gathering to trafficking in arms, addictive substances or people). In addition to organized crime, similar means/possibilities are used, for example, by terrorist organizations and, in principle, by the states themselves. In fact, as a consequence there is a further weakening of state power in the form of the ability to control and regulate the activities and actors concerned and to intervene against them as needed. This is associated with a conflict between the protection of national interests (generally) on the one hand and the utility of such networks on the other hand.

The interdependence of all areas of human society with the cyberspace further develops interdependence in terms of the availability of information as such. The digitization of state administration and the transfer of links between the citizen and the state into this domain (e.g. in the form of electronic identity cards or elections) directly reflects this phenomenon, which, however, also brings new forms of vulnerability (e.g. the issue of manipulation with electoral systems). From this perspective, the Internet allows increased transparency in almost all activities in the real environment. Social media, such as Facebook, Instagram, Twitter, YouTube, or the latest TikTok, allow almost constant monitoring and keeping track of activities of individual entities. At the same time, it serves as an ideal tool and platform for conducting information operations by both state and non-state actors. Capacity to monitor these networks, or their providers, can

[10] SHIEBER. J. Telegram faces DDoS attack in China…again [online]. 2019. Available at: https://tcrn.ch/2ZJgfbc

[11] KELLY, Jemima. Top Banks and R3 Build Blockchain-Based Payments System [online]. *Reuters*, 2017. Available at: https://1url.cz/vM4zs

[12] KARL, Angela. *Blockchain Technology for Cloud Storage: This Looks Like Future* [online]. Tech Genix, 2018. Available at: https://1url.cz/yM4zC

[13] For detailed explanation, see e.g. SUI, Daniel – CAVERLEE, James – RUDESILL, Dakota. *The Deep Web and Darknet: A Look Inside the Internet's Massive Black Box* [online]. Wilson Center, 2015. Available at: https://goo.gl/AztPdM

therefore be seen as an important prerequisite for the ability to control and influence public opinion in general. On the other hand, this aspect helps in effective defence against the influential activities of a potential adversary. Building the independent Russian "Internet" RuNet, which was to be successfully tested in 2019,[14] or increasing the effectiveness[15] of the so-called "Great Chinese Firewall" in this respect, combine the two characteristics discussed above.

A fundamental importance (not only) for this domain will be the full implementation of quantum (computational) technologies, which by their very nature surpass the performance of individual computing systems. Consequently, new possibilities such as processing and storing large data (Big Data), calculating corresponding threats/opportunities for current encryption tools and procedures, i.e. protection of data and information itself, are associated with this. In January 2019, the first "commercial quantum" computer (IBM Q System One) was introduced.[16] On the other hand, these are still the imaginary first steps, and ensuring the widespread use of this technology is still a matter of long-term research and development.

Information technologies are already interconnected with all areas of human life (inter alia for citizens - the state). Gradually, there is a shift from the "Internet of Things" to the "Internet of Everything". At the same time, there is a further weakening of state power through illegal activities within dark web/darknet. Great attention is also paid to the development of quantum technologies that have the potential to fundamentally influence current approaches, e.g. in the field of cryptography. In terms of information operations (information impact, including disinformation), social media/networks and actors capable of processing and using Big Data can play an important role.

Implications for the Armed Forces of the Czech Republic

From the perspective of the newest operational dimension, **cyberspace** also imposes increased demands on training and preparation, both to maximize the benefits and at least to suppress the vulnerabilities arising from the use of information technology. Importance of the discussed trends for the Czech Armed Forces can be further identified in the areas of *Project; Engage; C3; Protect; Sustain and Inform*. The development of capabilities in these areas will be, inter alia, linked to systems enabling the processing of large amounts of data, as well as to the systems supporting operational changes in the level of centralization and decentralization of command and control. The finalization of the complex interconnection of C4ISR in the ACR environment should not only prevent the lagging behind in this area vis-à-vis more developed states, but also provide an important competitive advantage in both "small" and "large" armed conflicts.

Support for this development can be provided by elements of cloud services adapted for military purposes. The "blockchain" technology and its implementation, data decentralization and its higher security (e.g. from unmanned reconnaissance vehicles), increased level of the resilience of systems against the electromagnetic pulse (EMP)

[14] WAKEFIELD, J. Russia 'successfully tests' its unplugged internet [online]. *BBC*, 2019. Available at: https://bbc.in/2X7vyst

[15] WYCIŚLIK-WILSON, M. It is getting harder than ever for VPNs to break through the Great Firewall of China [online]. *Beta News*, 2019. Available at: https://bit.ly/3gr4v32

[16] RUSSELL, John. IBM Quantum Update: Q System One Launch, New Collaborators, and QC Center Plans [online]. *HPC wire*, 2019. Available at: https://1url.cz/kM4K2

represent opportunities and ways ahead decreasing the danger of disrupting the information operations and communication systems. In all these MCAs, the importance of cyberspace and the trends described above for information activities cannot be overlooked. It is necessary to pay attention to the possible use of this platform, including the "Internet of Everything", social networks, elements of artificial intelligence (see the next chapter for more details) for action by the ACR against the enemy, and defence against such activities carried out by the enemy. The central role here is undoubtedly played by unified and continuous strategic communication (StratCom) with domestic and foreign audiences. In the *Engage* area there is an imminent combination with capabilities and elements of electronic warfare - e.g. in the form of bringing malware into adversary information networks via wireless connection, etc. At the same time, especially in the context of *Protect and Sustain*, increased emphasis should be placed on ensuring cyber defence and security. The importance of these aspects was supported last year by the Czech Republic's experience of attacks against the Benešov hospital facility and the OKD mining company. However, this recommendation must be applied not only to the traditional platforms, but also to the Internet of Things/Internet of Everything or opportunities and threats associated with the development of quantum computing. Based on experience, e.g. from the USA, it can be assumed that these devices will be used soon not only as targets of cyber-attacks, but also as a means of their realization. Even for a small country's armed forces, such as in the Czech Republic, it is therefore necessary to provide A2/AD capabilities in this domain that would allow for a stable use of this environment, while denying access to the enemy.

DEVELOPMENT AND EXPLOITATION OF REMOTE CONTROL AND AUTONOMOUS SYSTEMS

Unmanned Aerial Systems (UAS) are currently being used by the Armed Forces of more than 60 countries worldwide for reconnaissance, surveillance or monitoring purposes. Gradually, the range of states that have combat (strike) unmanned means is gradually expanding. It can be assumed that this general trend in the growing number of states that have individual categories of unmanned assets, will increase in intensity. Compared to manned aircraft, preference is given to lower acquisition and operating costs and the absence of a direct threat to the human "crew" (operators).

Through the development of especially additive manufacturing and nanotechnologies (for more details, see the chapter *Additive manufacturing*), new categories of UAS are gradually being introduced - micro and nano - which, with their proportions, can approach the size of insects. It is this aspect that, among other things, gives them an advantage over traditional sensors and gives them the ability to penetrate secured areas unnoticed.

Especially in the case of great powers, it is possible to identify both a significant increase in the number of individual types of unmanned aerial vehicles and an expansion of the range of tasks (e.g. supply or transport) for which they are used. This trend can be very well demonstrated by the example of the United States of America, when in 2000 their armed forces had only two types of UAS.[17] At present, at least eleven of them,[18] including

[17] Office of the Secretary of Defense. *Unmanned Aircraft Systems Roadmap: 2005-2030* [online], p. 3. Washington, D. C., 2005. Available from: https://goo.gl/RBfrij

[18] SICARD, Sarah. 11 Military Drone Names, Ranked [online]. *Task & Purpose*, 2017. Available from: https://goo.gl/Z3ExN7

UAS, are already equipped with weapons systems. Similarly, the Russian Federation is very intensively working on projects of combat drones, which are currently in the testing phase of individual prototypes. In August 2019, for example, the first flight of the jet UCAV S-70 Ochotnik-B took place.[19]

In comparison with UAS, Unmanned Ground Systems (UGS) are still represented in the national armed forces in a smaller number and variability. Their role is often directed towards the disposal of booby traps and unexploded ordnance, hazardous substances management or short-range exploration (e.g. in urbanized areas). The Israeli army also uses these means (the Guardium project) to guard border areas and protect military facilities. Vehicles have, in addition to sensors designed to detect the intruder, weapons systems of lethal and/or non-lethal character.[20] Similarly, a remotely controlled modification of the latest Russian armoured vehicle on the Armata platform or individual U.S. projects under the auspices of DARPA should be in the development phase - directly linked to the needs/assumptions embedded in the so-called third offset strategy.[21]

In connection with the control of individual means, great attention is paid to the development of capacities that would allow simultaneous deployment of a large number of individual types of the discussed (weapons) systems. Especially for unmanned systems, this approach is associated with the ability to control swarms, i.e. a high number of (small) means to overwhelm the enemy (air) defence. Intensive testing of these technologies is taking place, for example, in China, which is currently recognized as at least one of the leading countries.[22] Their use is assumed for the execution of separate tasks (such as the destruction of targets), other units support, especially aircraft with a human crew. In fact, there is also a visible development in strengthening of functional links between individual means in order to obtain a synergistic effect. The initial potential of such capability was demonstrated last year in attacks on oil facilities in Saudi Arabia.[23]

Similarly, projects of joint operation of piloted/controlled systems and remotely controlled or autonomous systems are being developed. A device with a human crew in such a combination usually plays the role of a leading element, which is supported by robotic systems. The result is a synergistic increase in the capabilities of such a set in virtually all aspects. For example, in connection with the *Skyborg program*, the USA is preparing an autonomous aircraft that would accompany the F-15 and F-35 aircraft.[24] Similar projects can be found, in principle, in all remaining domains (including cyberspace).

---

[19] ESHEL, T. Russian Okhotnik-B Combat Drone (UCAV) Makes its First Flight [online]. *Defense Update,* 2019. Available from: https://bit.ly/2TLJ6rw

[20] ARMY-TECHNOLOGY.COM. *AvantGuard Unmanned Groud Combat Vehicle, Israel* [online]. 2016. Available from: https://goo.gl/knZqWb

[21] LOUTH, John – MOELLING, Christian. *Technological Innovation: The US Third Offset Strategy and the Future Transatlantic Defense* [online]. Armament Industry European Research Group, 2016. Available from: https://goo.gl/pvEHAc

[22] BLEEK, P.C. – KALLENBORN, Z. Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons [online]. *War On The Rocks,* 2019. Available from: https://bit.ly/2TZLgEn

[23] SAFI, M. – WEARDEN, G. Everything you need to know about the Saudi Arabia oil attacks [online]. *The Guardian,* 2019. Available from: https://bit.ly/3dctx3W

[24] INSINNA, Valerie. Under Skyborg program, F-35 and F-15EX jets could control drone sidekicks. *Defense News*, 2019. Available from: https://bit.ly/2zq2y6t

Contrary to the remotely controlled devices, autonomous systems assume either no or minimal "interference" by the human operator. Individual systems should be able not only to obtain information about the environment, but also to process them (evaluate) and make appropriate decisions. The motivation to field these systems as soon as possible directly results from the increased demand for higher combat efficiency. As in the case of remote-controlled devices, the idea of minimizing casualties of own or friendly armed forces and non-combatants is represented.[25] Systems based on AI/machine learning elements more effectively suppress and eliminate the human beings physical and psychological limitations (including the need for sleep and the effects of fatigue or stress).

On the other hand, there are serious unanswered questions, e.g. the degree of autonomy that should be given to these systems, and whether, at least from an ethical point of view, a decision to kill a human being can be taken purely by these means. This aspect is increasingly being discussed throughout the professional community and is becoming a motivation for efforts to establish and enforce the supervisory regime at the international level (e.g. under the auspices of the UN).[26] On the other hand, it is necessary to point out that, following historical examples (e.g. cluster munitions, anti-personnel mines, etc.), the probability of achieving an overall ban across all states and enforcing it is rather unrealistic.

Certain elements of these technologies can be identified at present, when Guardium vehicles are able to operate in a fully automated (autonomous) mode.[27] Similarly, these elements are used in long-range missions of unmanned drones, where the human operator takes control of the UAV in the target area or surpass air defence systems (e.g. the Phalanx point defence system).[28]

Furthermore, in systems based on AI/machine learning elements, considerable potential can be identified in relation to cyberspace, or to the collection, evaluation and processing of data and information in general. Their development and performance bring new possibilities, for example, for the detailed analysis of a large number of documents, visuals or audio records. Consequently, related to this is the ability to imitate such data accurately, make copies or even give them brand new features (such as a virtual person) almost indistinguishable from reality/originals (so called deep-fakes).

Great attention is generally paid to the development of both unmanned and autonomous systems. In the arsenal of individual states, so far, reconnaissance UAS are the most represented, but based on individual projects, combat UAS or UGS can gradually expand this arsenal. Gradually, new categories (micro- and nano-) are being introduced. Research and development focus on the capability to simultaneously deploy and control large quantities (swarms) of special UAS. Attention is also paid to the joint operation of piloted/controlled systems and remotely controlled or autonomous systems. The development of autonomous systems is directly determined by the level of development of AI elements and affects resources and activities in all domains.

[25] E.g. STOJAR, Richard. Bezpilotní prostředky a problematika jejich nasazení v soudobých konfliktech. *Obrana a strategie*. 2016, 16(2). Available from: https://goo.gl/dYJsZ2
[26] E.g. Autonomous Weapons: An Open Letter from AI & Robotics Researchers [online]. *Future of Life Institute*, 2017. Available from: https://goo.gl/X2N6CA
[27] ARMY-TECHNOLOGY.COM, ref. 21.
[28] RAYTHEON. *Phalanx Close-in Weapon System: Last Line of Defense for Air, Land and Sea* [online]. Available from: https://goo.gl/Ky3RD1

At the same time, there is an intense debate over the moral/ethical aspects of using (not only) this type of technology for military purposes.

Implications for the Armed Forces of the Czech Republic

The development of remote control and autonomous systems will primarily affect the *Prepare/Training* and *Protect* areas not only in terms of their use, but also their ability to respond to their engagement by the adversary (regardless of their nature). However, the development of these means must not neglect the newly emerging categories of micro- and nano-UAS (see the chapter on *Additive manufacturing*). Interesting opportunities in the counter-UAS area are based on the combined use of radar and directional jammer or high-power laser, which, however, are not widespread within the Czech Armed Forces. Similarly, it is necessary to ensure the implementation of systemic measures against the abuse of our UAS by the adversary (whether it is to obtain intelligence or take control of the affected system). From this perspective, the technological dimension of protection and security, as well as their overall procedural and legislative settings, should not be overlooked. In relation to the character of the Czech Armed Forces, it is necessary to emphasize the potential of "swarms" of remotely controlled means and the interaction of piloted/controlled systems and remotely controlled or autonomous systems. Both elements allow in the areas of *Project; Engage; Sustain; and Inform* for the compensation of the size of the Armed Forces (possibly adverse demographic development or lack of staff) and covering a wide range of tasks (from survey to direct encounter with the adversary). Similarly, the use of autonomous systems (AI/machine learning elements) creates opportunities for the development of capabilities not only in "physical" domains, but also in the cyberspace, as already discussed. On the other hand, especially the effective use of UAS and UGS swarms depends on the necessity to have sensors, communication systems and systems processing a vast amount of data from the environment around these devices (see the Cyberspace chapter). At the same time, it is necessary to answer the above-mentioned legal and ethical questions related to the use of autonomous systems, ideally before their potential acquisition.

DEVELOPMENT OF THE HUMAN-MACHINE INTERFACE

In addition to the above-mentioned "battlefield robotization" trend, projects that make it possible to achieve a more effective human-machine interface are being developed. Generally, this should facilitate improvement in the performance and multiplication of the human potential, e.g. as an improved capacity to control other systems or the individual's physical and mental abilities, to reduce human vulnerability and also to eliminate the consequences of injuries or illnesses.

When elaborating more on the first topic of man-made connection (control of systems), it is possible to identify the effort to provide all information from the sensors to the human operator in real time, eliminating the delay between the response of the human operators and the controlled system, while ensuring that all commands are executed as if the humans themselves were the concerned systems. It is the direction of the development and testing of sensor and control elements of the American Fighter F-35, which should, for example, transmit a comprehensive image from six infrared cameras

directly into the pilot's helmet and provide information about the surrounding environment including the position of the opponent.[29]

The area under discussion is very closely linked to technologies enabling exploitation of the so-called augmented or directly virtual reality and, if possible, the full involvement of man in its interactions. In this sense, the importance of information technologies and cyberspace, which can be used not only in the above described (combat) activities, but also in the planning of combat operations and training and preparation of combat units, is again emphasized. The development of augmented and virtual reality allows very realistic simulation - in our case the combat situation and environment in which the units will operate, the possible behaviour of the adversary included. A similar application can be identified also for "non-combat" activities (e.g. health care or logistics).

Within the second topic (increasing the performance of human abilities/activities), projects aimed at creating robotic combat suits (so-called exoskeletons) should be emphasized. The benefit can be seen not only in increasing the strength, endurance or mobility of the person (soldier) equipped with this hardware, but also another shift in protection, for example, from enemy fire. Hydraulic systems increase the load capacity and significantly simplify the handling of "armour" (if we use the analogy of medieval warfare), which otherwise one would not be able to carry, not mentioning fast movement on the battlefield. Lockheed Martin or Raytheon companies have demonstrated prototypes of exoskeletons, which are able to handle the weight of the carried armament and equipment, thus allowing to possibly carry/manipulate a larger load, but also to increase the speed of movement and distance, which is far above physical abilities of even a well-trained fighter.[30] Last year, the United States Special Operations Command signed a contract with Sarcos Robotics company to supply Guardian XO robotic exoskeletons.[31] In contrast, a functional model of "armour" has not yet been introduced, although this situation can be expected to change over the coming years.

In addition to the exoskeleton projects, however, it is also important to mention technologies that directly connect with the human organism and thus become its (integral) part. Robotic limb replacements may be considered, which should/could make it possible to compensate for such types of (combat) injuries, or even sight and hearing replacement. The potential of these technologies should not be limited only to these situations and it can be assumed that with further advancement in cybernetics, neurobiology, genetical engineering, etc., we will witness enhancement of human abilities through various muscular sensors and implants. Currently, however, ethical and legal aspects related to the retention or removal of these implants from soldiers' bodies after leaving active service are not solved.

The development of the human-machine interface is very closely related to information technology aspects. Firstly, it allows more efficient control of other systems - such as UAS - and development of augmented and virtual reality elements. Secondly, it is about the potential elimination of human body limitations through its "strengthening". In

[29] LOCKHEED MARTIN CORPORATION. *The F-35 Helmet: Unprecedented Situational Awareness* [online]. 2016. Available at: https://goo.gl/MD6gDK

[30] E.g. HUSSEINI, T. US Army trials exoskeletons for military use [online]. *Army Technology,* 2019. Available at: https://bit.ly/2XCXZ0n

[31] Sarcos wins USSOCOM contract to supply XO robotic exoskeleton [online]. *Navy Technology,* 2019. Available at: https://bit.ly/2X4kcFM

addition to the development of exoskeletons, there is also possibility of intentional replacement of certain parts of human body, not necessarily only in the case of need to compensate for the consequences of (devastating) injuries.

Implications for the Armed Forces of the Czech Republic

In the area of *Prepare/Training*, through the augmented and virtual reality the development of the human-machine interface enables achieving higher effectiveness of training programs and creation of conditions, which are very close to real combat deployment. Currently, inter alia, we can emphasize the positive experience from the pilots' training and aircraft daily maintenance, incl. the possibility to hand over some special maintenance tasks directly to the manufacturer. There is possibility (in training applications) to consider interfacing with machine learning systems, which could allow better adaptation of the training load to the individual. Similar implications arise for the areas *C3 and Inform*, inter alia, through the creation of a comprehensive picture of the battlefield and its conveyance to relevant subjects. Streamlining the control of other systems - such as the UAS - and improving human traits through both exoskeletons and human limb and organ replacement represent significant potential for *Project; Engage; and Protect* areas. Particularly, the first topic (control of other systems) further supports the development of the previous trend.

BIOTECHNOLOGY

Trends in biotechnology represent an effort to strengthen and develop control over living organisms and their biological processes. In relation to human society, this is expressed, in particular, through agriculture, medicine and genetics and their routing towards the formation and strengthening of a human individual, their descendants and possibly human civilization as a whole. The application of these trends in the military basically acts as a stimulating element of the human factor of the armed forces and its importance in military operations.

Although the nature of the area in question does not represent a new trend in the history of human society (e.g. in reference to the use of microorganisms in the form of biological weapons), on the other hand, it is the development in the fields of genetics or the above-mentioned nanotechnologies that brings new possibilities for the realization of the respective ambitions. These overlaps are, among other things, visible in the projects of comprehensive soldiers' nutrition, which limit the consequences of sleep deprivation or stimulate muscle growth.[32] The use of small animals and microorganisms as components of a sensor network can be interpreted similarly.[33]

Probably the most discussed topic is the issue of the so-called genetic manipulation. This can directly influence the properties and abilities of living organisms, or specifically the human individual (up to the form of a certain ideal of "super-human"). As with robotic technologies (human-machine connection), there is clearly the possibility of compensating for damage caused by, for example, "combat injuries". However, compensation does not take place through prosthetic replacement, but, for example, through stimulation of a new limb growth. Similarly, the broad issue of the so-called

[32] E.g. SCHARRE, Paul – FISH, Lauren. *Human Performance Enhancement* [online]. Centre for a New American Security, 2018. Available at: https://1url.cz/gM4z8

[33] SOUTH, Todd. From Shellfish to Plankton [online]. *Navy Times,* 2018. Available at: https://1url.cz/LM4zA

biological weapons, as one of the categories of weapons of mass destruction, cannot be neglected. Through this area, they can, among other things, obtain the "necessary" attributes of targetability or control over their effects. It is precisely these implications that reflect, in comparison with other discussed areas of technological development trends, probably the greatest degree of controversy and ethical/moral challenges for the entire human society.

Biotechnology represents the ability to shape and influence the nature and essence of living organisms, incl. human individuals. From the military point of view, it is basically connected with the emphasis on the human factor. In general, it covers a wide range of aspects ranging from nutritional adjustments to the so-called genetic manipulation. At the same time, this area is probably characterized by the greatest degree of controversy and the emergence of moral/ethical challenges.

Implications for the Armed Forces of the Czech Republic

The implications of **biotechnology** for the Armed Forces of the Czech Republic primarily arise for the areas of *Prepare/Training; Engage; Sustain*. Here, possible uses can be identified through the inclusion of nutritional supplements in the nutritional and nourishment plan of personnel, either during training/preparation or during deployment in military operations. Similarly, permanent evaluation and monitoring of the effectiveness of training and physical processes, and their impact on the development of the human body, come into consideration. The *Protect* area then includes the issue of protection against biological weapons and gradually emerging genetically modified microorganisms by the adversary (state and non-state actors), not only against the armed forces but also civilians.

DEVELOPMENT OF ENERGY TECHNOLOGIES

The development of energy technologies is also becoming a major trend. In general, there are two interrelated directions: 1) obtaining a stable and efficient energy source as an alternative, especially for fossil fuels; 2) use in dedicated weapons systems.

The first direction is directly linked to the energy requirements of, for example, the earlier-mentioned robotic exoskeletons, where use in the field is currently significantly limited (in terms of performance or operating time) by their high energy consumption. The effort to find an effective substitute for fossil fuels is motivated (apart from the general approach to the issue of climate change) by the need to have mobile or easily transportable energy sources and the decentralization of energy production.[34] At the same time, there is a logical need for reduced dependence on external actors, local resources and increasing self-sufficiency.

The second direction can be divided into three main categories of weapons systems. The division reflects the form of the use of energy technologies, both to achieve lethal and non-lethal effects. These categories are: Directed Energy Weapons (DEW), weapons using energy pulses (electromagnetic radiation, EMP), and electromagnetic weapons. In general, development is focused on all of these categories. But especially the first and the third group identify the potential to replace "traditional" firearms. In contrast, the second category - EMP - has a more specific focus. It is particularly intended for the use against enemy electronic systems to achieve their elimination or destruction. Central

[34] Cf. FUTURE ASSESSMENT DIVISION. *Notes from the Edge: Insights into Evolving Future*, pp. 1–2. 2017.

attention is paid to the development of non-nuclear assets that could be deployed without escalation of the conflict or the necessity to possess a nuclear weapon (and master nuclear technology). Gradually, the possible use of microwave radiation against enemy personnel is also being developed.

In the case of DEW and electromagnetic weapons, projects are currently aimed at using these resources in air and naval combat, or as alternatives to missile defence elements. Examples are the deployment of the Israeli *Iron Beam* anti-missile system[35] or the resumption of ground tests of the electromagnetic cannon by the USA,[36] although the testing on a dedicated vessel has been delayed for the time being.[37] On the other hand, according to available resources,[38] the PRC's navy has already moved into this phase and conducted naval fire tests last year. Possibilities for broader deployment are downsized by the factual limits related to obtaining an efficient source of energy and its sufficiency to accomplish the required tasks (e.g. temporary or permanent blinding of sensors, destruction of the vessel or incoming missiles). For this reason, the usability in the field of small arms is significantly limited, while energy requirements do not yet allow higher efficiency compared to "traditional" weapons (due to weight, mobility or destructive effect in the target area).

At the same time, the usability of these technologies in the form of non-lethal weapons cannot be neglected, i.e. as a means to "only" temporarily paralyze or neutralize the enemy. The advantage is minimization of losses among non-combatants, which becomes relevant especially in urban area fighting or in the performance of tasks that are not directly related to combat activities (e.g. in the case of securing the public order).[39]

The energy technologies focus both on the research/acquisition of an alternative energy source and on their use in weapon systems. Three basic categories of weapons systems can be identified - weapons using directed energy, weapons using energy pulses (especially the issue of electromagnetic radiation) and electromagnetic weapons. For DEW and electromagnetic weapons, projects are currently being developed, especially in the framework of air and naval combat, or missile defence. The fundamental limit is to obtain a stable and efficient source of energy which simultaneously meets the requirements for performance or mobility.

Implications for the Armed Forces of the Czech Republic

The development of (new) alternative energy sources can currently be considered relevant for the Armed Forces of the Czech Republic. In the *Project, Engage, Sustain and Protect* areas, there are efforts to ensure self-sufficiency and independence of the armed forces, not only during their deployment. At the same time, the so-called footprint on the battlefield is being reduced, because of lean logistics and utilization of (financial,

[35] RAFAEL. *Iron Beam* [online]. Available at: https://goo.gl/NGYa6N

[36] TREVITHICK, J. Navy's Railgun Now Undergoing Tests In New Mexico, Could Deploy On Ship In Northwest [online]. *The Drive*, 2019. Available at: https://bit.ly/3glXccS

[37] Cf. e.g. ECKSTEIN, M. Navy Making Room For Railguns In Next Warship, But No Extra Investments [online]. *USNI News*, 2018. Available at: https://1url.cz/mM4z7

[38] VAVASSEUR, X. Chinese Navy Railgun: What We Know Thus Far [online]. *Naval News*, 2019. Available at: https://bit.ly/2AZVEFc

[39] In detail, e.g. ARTICLE36. *Directed Energy Weapons* [online]. Discussion paper for the Convention on Certain Conventional Weapons, 2017. Available at: https://goo.gl/fiV7AW

material, human) resources. Within the *Protect* area, it is also necessary to point out the threat of the use of an electromagnetic pulse by the opponent. In this sense, it is necessary to ensure the resilience of all electronic systems and, similarly to cyber-attacks, to prepare alternatives (backups) in the event of their elimination.

ADDITIVE MANUFACTURING

Additive manufacturing (especially "3D printing") is a very rapidly developing industry. In the United States, for example, approximately two thirds of manufacturers use 3D printing at some stage in development and production.[40] Similarly, this technology is increasingly used for the "construction" of buildings/facilities,[41] which represents from the point of view of the armed forces a potential reduction of time and cost of base or check point construction, especially in remote places with difficult access.

Expansion among the whole society and wide use of this method of production are not expected until the next ten years. But even today, in comparison with the traditional method of production, it is already possible to create, for example, spare parts for weapons systems and reduce very flexibly the demands on storage and transport capacity. Although this example points to the importance for logistics, the usability itself extends to a much wider field of projection of the armed forces or the production of the required (weapons) systems.[42] Similarly, there is a rapid development of this area in health care. Here, additive production (3D printing) represents an opportunity for the creation (printing) of human organs for transplantation, parts of skeleton (artificial bones), tissue and other parts of the human body.[43]

In this context, nanotechnology represents a qualitative shift in the possibilities of additive production. This area fundamentally influences the development of not only technologies using energy in various progressive forms but also, for example, robotic technologies. The ability to create and influence the structure of individual materials and objects at the level of a billionth of a meter brings along new possibilities for the resilience and protection of the armed forces (e.g. in the form of active reactive camouflage) and means of neutralizing the enemy.[44] The use of the above-mentioned characteristics can be traced, among other things, in testing and acquisition of the so-called micro- and nano-unmanned systems (e.g. nano-UAS Black Hornet 3)[45] for all types of military operations.

Additive manufacturing enables very flexible production of almost any object. This is related to the considerable potential for streamlining and savings not only in the area

---

[40] NATO STO Sensors & Electronics Technology (SET) Panel. *Flexible Displays Technology Watch Card*. 2016.

[41] E.g. LANSARD, Martin. *The 15 Best Construction 3D Printers In 2019* [online]. Aniwaa, 2019. Available at: https://bit.ly/2Xyma01

[42] AKER, Berenice. Made to Measure: The Next Generation of Military 3D Printing [online]. *Army-Technology.com*, 2018. Available at: https://goo.gl/jFKaRY

[43] HOOIJDONK, R. Exciting New Advances in 3D Printing Could Help Solve Cut Organ Transplant Waiting Lists [online]. *The Journal of mHealth*, 2019. Available at: https://bit.ly/2zABJwj

[44] In detail, e.g. WONG, Wilson W. S. Emerging Military Technologies: A Guide to the Issues. Oxford: Praeger, 2013.

[45] KIRVE, Patrik. Small Drones Take Flight for Military Applications [online]. *RBR*, 2018. Available at: https://bit.ly/2yHOZ1S

of logistics, but also, for example, enabling execution of broader concept of the armed forces projection. In this sense, nanotechnologies represent a qualitative shift, which is given by the ability to create and influence the structure of selected materials and objects at the level of a billionth of a meter. Significance for other trends is represented, among other things, by miniaturization, such as UAS and their gradual acquisition.

Implications for the Armed Forces of the Czech Republic

The development of **additive manufacturing**, similar to previous trends in the field of alternative energy sources, reflects efforts to ensure the self-sufficiency of the armed forces and increase their independence during deployment, on top of other aspects. Armed Forces can benefit from a cost reduction in logistics or force projection through the use of 3D printing (areas *Project; Sustain*).

Possibilities such as printing parts of facilities/objects or the production of spare parts can represent an immediate stimulus for the development of relevant capabilities. At the same time, the development of "bio printing" represents a unique tool for military medicine to cure, e.g., amputation or loss injuries. From longer perspective, the importance of miniaturization through nanotechnologies is evident especially in further development of remote-controlled/autonomous systems, man-machine interconnections and energy technologies (areas of *Engage; Protect*).

HYPERSONIC TECHNOLOGY

Hypersonic technologies represent another area of strategic competition among the major powers.[46] These weapons systems operate at speeds higher than Mach 5 (6125 km/hr), which together with high manoeuvrability makes them almost unstoppable by current means of missile defence. The hypersonic phase of flight generally occurs during the return from space or close proximity to the atmosphere or during an atmospheric flight, if the missile is equipped with rocket or scramjet propulsion. Examples of these technologies are, e.g., hypersonic glide vehicles (HGV) or hypersonic cruise missile (HCM). Because of the speed developed, these systems can rely primarily on kinetic destructive effects in the target area. They can also be used as carriers for conventional or nuclear warheads. One example of this category of already tested hypersonic missiles is the Russian missile Ch-47M2 Kinzhal (tested in the Arctic areas last year).[47] Similar attention is paid to anti-ship missiles, which, in Chinese strategic thinking, are considered an ideal means of ensuring the ability of A2/AD against the US Navy (aircraft carrier battle groups), at least for the areas of South China, East China and the Yellow Sea. In 2019, PLA publicly introduced a new type of hypersonic cruise missile - DF-100.[48]

Implications for the Armed Forces of the Czech Republic

From the viewpoint of the **hypersonic technologies** development and especially economic costs, these weapons systems do not represent immediate in-hand possibilities for capabilities building of the Armed Forces. On the other hand, because of the Czech Republic's membership in NATO, we have to work with the assumption that these systems

[46] WILSON, J. R. The emerging world of hypersonic weapons technology [online]. *Military & Aerospace Electronics*, 2019. Available at: https://bit.ly/36Ao9VE
[47] NILSEN, T. Russia's top General indirectly confirms Arctic deployment of the unstoppable Kinzhal missile [online]. *The Barents Observer*, 2019. Available at: https://bit.ly/2ZJg6Ez
[48] DF-100 [online]. *Military-Today.com*, 2020. Available at: https://bit.ly/3gsk3U6

represent a clear challenge for the Alliance's territorial effective air defence (*Protect* area). The Armed Forces should monitor this area and take into account the growing capabilities of potential adversaries, both at the practical and conceptual levels.

GENERAL IMPLICATIONS FOR THE ARMED FORCES OF THE CZECH REPUBLIC

The pace of development of the above-mentioned technological areas (not exclusively) is difficult to predict. On the other hand, at least the already known projects have relatively big military implications that the Czech Armed Forces should not overlook. Activities/initiatives that reflect these aspects can be clearly approached positively, whether it is the creation of 533rd Battalion of drones, or the ongoing capacity building of the Cyber Forces and Information Operations Command. International cooperation projects can provide a similar benefit, although it is always necessary to assess their outputs in the context of strengthening the Armed Forces capabilities.

It cannot be assumed whether it is possible for our armed forces to focus on a comprehensive set of capabilities that we are witnessing in the case of the world's major powers - especially the United States. Nevertheless, it is necessary to avoid neglecting even those areas that may at first look seems to be irrelevant and distant from the goals and capabilities of the Czech Army and our national POL-MIL ambitions and security interests.

In summary, there is a need to ensure interoperability of deployed systems, not only with the allies within NATO/EU, but also internally, through generations of weapons and other hardware classes. Interoperability and mutual compatibility strengthen the resilience of the entire structure (robustness and redundancy - substitutability) and increase the efficiency of individual elements.

By blurring the border between the military and civilian dimensions, it can be assumed that the ACR will be confronted with, for example, deployment of an unmanned aircraft, owned or operated by a non-state actor. From this angle, it is clearly desirable to allocate funds for projects that focus on defence against such systems and run the analysis whether the current training (content and methods) takes into account such eventuality. Similarly, it can be assumed that this development will affect the range and nature of suppliers, not only domestic, but also foreign. This creates a certain dependence on these entities, which can manifest itself as negative phenomena such as the threat of espionage or unavailability of services in the event of a conflict between the interests of the armed forces, or the Czech Republic in general, and the concerned entities. At the same time, it should not be forgotten that the development of modern technologies brings new challenges for the arms control and proliferation of individual systems, both nationally and internationally. Particular attention should be paid to the issue of existence of sufficient, up to date (legal, technological, ethical, etc.) standards, ways of their enforceability and regular update.

Title: Technological Development: Implications for Czech Armed Forces Capabilities 2019
Authors:
Mgr. et Mgr. Jakub Fučík, Ph.D.
Ing. Fabian Baxa, Ph.D.
PhDr. Libor Frank, Ph.D.
doc. Ing. Josef Procházka, Ph.D.
Graphic and editorial design: Mgr. Martin Doleček
Publisher: University of Defense in Brno
Year of publication: 2020
Edition: first

https://www.unob.cz/en/csmss/Pages/Publications.aspx