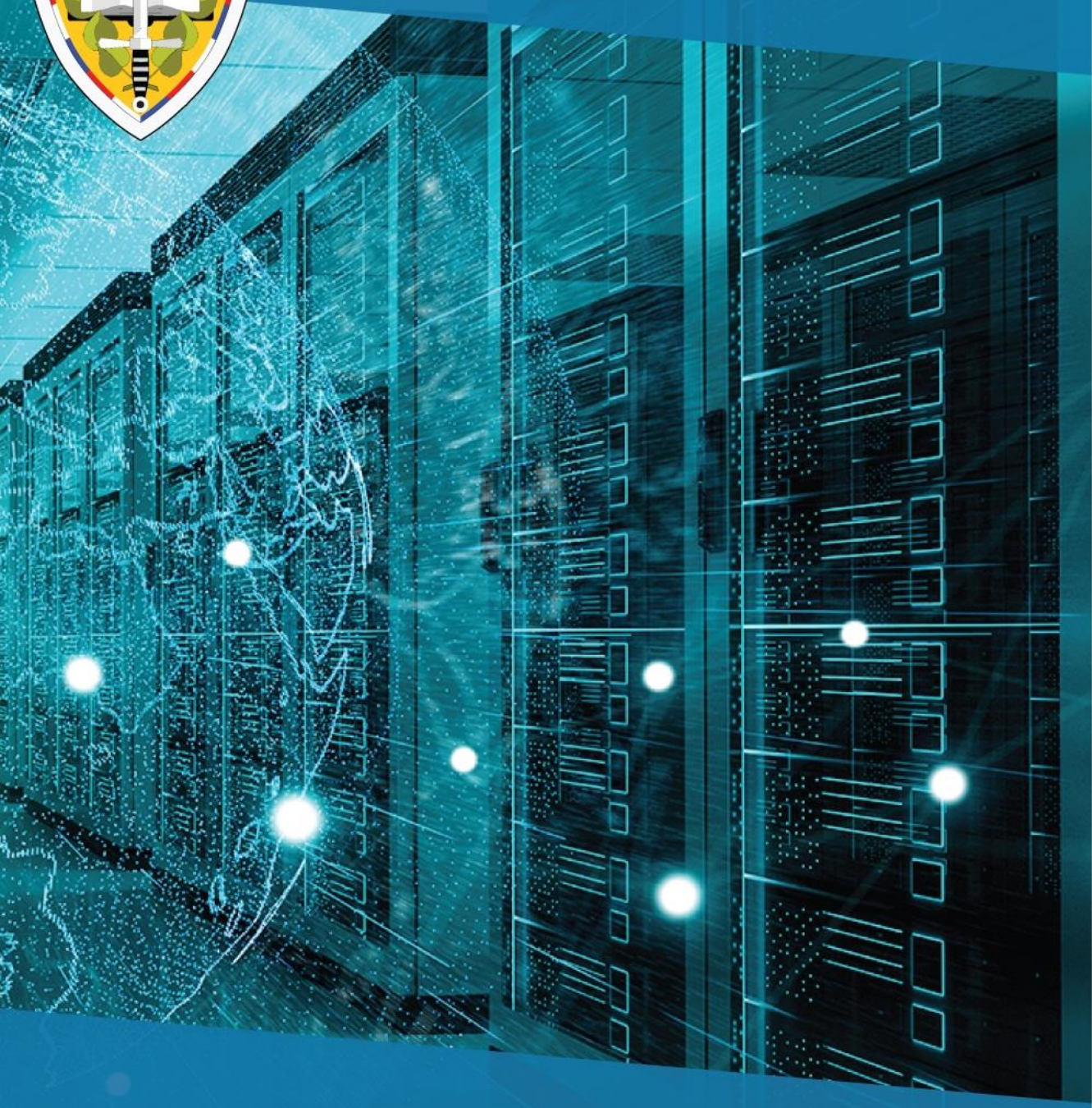
CENTRE FOR SECURITY AND MILITARY STRATEGIC STUDIES
UNIVERSITY OF DEFENCE



TECHNOLOGICAL DEVELOPMENT

IMPLICATIONS FOR THE CZECH ARMED FORCES' CAPABILITIES IN 2020

JAKUB FUČÍK, FABIAN BAXA, LIBOR FRANK, JOSEF PROCHÁZKA

TECHNOLOGICAL DEVELOPMENT

IMPLICATIONS FOR THE CAPABILITIES OF THE CZECH ARMED FORCES 2020

JAKUB FUČÍK ET AL.

BRNO
2021

AUTORSKÝ KOLEKTIV

Mgr. et Mgr. Jakub Fučík, Ph.D.

Ing. Fabian Baxa, Ph.D.

PhDr. Libor Frank, Ph.D.

doc. Ing. Josef Procházka, Ph.D.

This expert study is a partial result of the project DZRO STRATAL - Strategic Alternatives, implemented at the University of Defence.

Reviewers:

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

Col of Gen. Staff doc. Ing. Petr František, Ph.D. - Head of the Department of Informatics and Cyber Operations, Faculty of Military Technology, University of Defence

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

Lt Col of Gen. Staff David Necid, M.A. - Force Development Division of the MoD / Cyber Capability Section

Centre for Security and Military Strategic Studies (CBVSS, Centrum bezpečnostních a vojenskostrategických studií)

CBVSS is part of the University of Defence in Brno and is defined as other workplace for education and creative activity according to Act No. 111/1998 Coll., §22(1)(c). Its mission, in particular, consists in:

- Scientific and research activities in the areas of security studies, strategic leadership, military art, strategic management and defence planning, implemented for the needs of the strategic level of decision-making, management of national defence and the building of the Armed Forces of the CR.
- Preparation of the military and civilian experts of the department of the Ministry of Defence and the armed forces in expert and career courses (General Staff Course, Senior Officer Course).
- Expert, publishing and popularising activities (including the sponsorship of publishing the *Czech Military Review* and *Defence and Strategy* journals).

ISBN 978-80-7582-377-9
DOI:10.3849/978-80-7582-377-9

INTRODUCTION

The aim of the analytical study is to assess the trends in technological development and their implications for the Armed Forces of the Czech Republic in 2020. The ambition of the Centre for Security and Military Strategic Studies of the University of Defence (CBVSS, Centrum bezpečnostních a vojenskostrategických studií) is to provide another contribution to the discussion on the consequences of technological development for the formulation and implementation of an effective defence policy of the Czech Republic, or the building of its armed forces (primarily the Army of the Czech Republic). The document is intended to serve as a periodic assessment of the concerned issue. Thus, not only does it provide evidence for more detailed (observational) research in individual areas, but it can also serve as information support for relevant bodies. In this respect, the study is directly linked to the assessment of technological trends for 2017, 2018 and 2019.[1]

The study is based on the analysis and comparison of open sources, related to the nature of current trends in technological development and its applicable examples. Implications for the Czech Armed Forces (CAF) are analysed using the so-called Main Capability Areas (MCA), defined using the NATO methodology.2 For each trend, areas of competence that are directly affected by its development and of immediate relevance to the body concerned are identified. At the same time, it should be noted that although individual trends and their implications are analysed and described progressively, they cannot be perceived separately in their nature.

The reader should always take into account the "overarching" topic of the impact of technological development on the armed forces, or society in general, and the interdependence of associated trends. The same comprehensive approach is also relevant to the analytical framework of the MCA used and the specific capabilities identified. The study is time-framed for 2020 and focuses on trends that may have an immediate impact on the armed forces.

INCREASING IMPORTANCE OF "NEW" STRATEGIC DOMAINS

In addition to the traditional domains of strategic thinking and armed conflict - land, sea and air - the importance of space and cyberspace continues to increase, regardless of whether individual states / international organizations consider these domains to be separate or as part of other domains (e.g., cyberspace as part of the information domain under the Russian approach).

OUTER SPACE

As in previous years, the interest of state and non-state actors in this domain is growing. At the level of states, we can see the intensification of new "space races", whose iconic goal is not only to be the first human crew to reach Mars, but also to ensure a permanent

[1] Individual studies are available on the website of the Centre for Security and Military Strategic Studies. Direct link: https://www.unob.cz/en/csmss/Pages/Publications.aspx
[2] MC 400/3, MC Guidance for Military Implementation of Alliance Strategy. 2012.

presence both on this planet and on the Moon. In July 2020, a total of three missions were launched out of the four originally planned. The United States and China want to transport a robotic vehicle to the surface of Mars. The United Arab Emirates launched a probe to the planet's orbit. The joint EU-Russia mission has been postponed to 2022.[3] The strategic implications of space reflect the ongoing development of capabilities of national armed forces. In addition to the traditional powers in the outer space, last year was significant, for example, for Iran, which placed its first military satellite marked as Nur 1 in the Earth's orbit.[4]

The growing importance and role of non-state actors (especially in the form of private companies, such as SpaceX) is apparent in the gradual acquisition of capabilities enabling manned flights, which were originally only feasible through state or interstate organizations. At the end of May 2020, SpaceX successfully delivered a two-man crew to the ISS space station via its Dragon 2 spacecraft.[5] Another similar mission with a crew of four was launched on 15 November, reaching the ISS two days later.[6] In both cases, the reusable Falcon 9 carrier was used. On the one hand, this phenomenon entails, inter alia, better availability of the systems and capabilities concerned (e.g., by reducing the price/cost per kilogram brought to orbit due to competition between individual private companies). On the other hand, however, there is reduced state control over the systems that will be placed in orbit in this way. This situation further "ignores" the problem of *dual-use technologies* described below.

In general, the potential represented by space and relevant technologies can be divided into two areas (civilian and military), the dividing criterion being the nature of the activities or the real artificial bodies (satellites, stations, etc.) operated or located in the outer space. The civilian group includes, for example, the establishment and use of satellite networks designed to monitor weather or transmit TV signals, etc. The military group includes, for example, spy satellite networks, satellite navigation of military units or weapon platforms designed to detect and eliminate ballistic missiles, etc. Similarly, the so-called *anti-satellite weapons (ASAT)* may be located on the ground or sea level, but their use is directly located aimed at the outer space. To date, a total of four countries have officially successfully tested this weapons system (China, India, Russia, US). Last year, these countries continued to develop it, which was demonstrated, for example, by Russia carrying two tests in April and December.[7]

At the same time, it is necessary to state that the boundaries between the two categories are very unclear, or both groups often overlap in their elements, which makes their differentiation in practice quite problematic. Thus, we encounter a persistent phenomenon of dual use of the concerned technologies or activities. As we can see from the examples of the American GPS system or the different types of services that will be provided through the European Galileo system, still under construction, the satellite

[3] STRICKLAND, Ashley. This summer, multiple spacecraft are launching to Mars. Here's why [online]. *CNN*, 2020. Available from: https://cnn.it/2Ry70ZL
[4] Iran's Military Satellite Successfully Launched into Orbit [online]. *Defenceworld.net*, 2020. Available from: https://bit.ly/3g3vvHy
[5] O'CALLAGHAN, Jonathan. SpaceX Makes History With First-Ever Human Rocket Launch For NASA [online]. *Forbes*, 2020. Available from: https://bit.ly/3px7vjj
[6] CAWLEY, James. Crew Dragon Docks to Station, Hatches Open Soon [online]. *NASA*, 2020. Available from: https://go.nasa.gov/3w4AFcb
[7] STROUT, Nathan. The 6 big military space stories of 2020 [online]. *C4ISRNET*, 2020. Available from: https://bit.ly/34VmmuB

navigation network can be used not only to determine the position of civilian entities, but also to coordinate the progress of operational clusters or guiding missiles or unmanned aerial vehicles. Similarly, the usability of the constructed satellite networks for global communication and 5G Internet coverage (currently, e.g., OneWeb or LeoSat) can be assessed.

The use of satellite systems is increasingly available to small states from the point of view of both technological development (miniaturization) and capacity sharing as well as the involvement of space companies. This phenomenon is also demonstrated by the Czech Republic through the operation of the SATCEN Satellite Centre, which is managed by the Military Intelligence and allows the collection and analysis of electro-optical and radar image data from space exploration. Last year, a plan was also published to create our own (national) satellite system under the designation GOLEM.

The outer space has become an important domain for the ability to exercise the (military) power of the state and plays its role in promoting national interests of the state. This aspect is also reflected by NATO through accenting the outer space as a separate operational domain. At the same time, the role of private companies developing capabilities originally reserved for states or international organizations is growing. The use of the outer space is very closely linked to the phenomenon of the so-called dual use, where the boundaries between the civilian and military sectors are blurred.

Implications for the Armed Forces of the Czech Republic

The growing influence of the **outer space** is beginning to be reflected in the Army of the Czech Republic. Proof of this development is, among others, the speech of the Chief of the General Staff of the Army General Aleš Opata at the NGŠ AČR Command Assembly.[8] At the same time, some specific actions by the Czech Republic, which are not directly related to the armed forces, can be identified in this domain. In particular, it concerns the construction of the Military Intelligence Satellite Centre, which was put into full operation in this period.[9] The Czech membership in the EU and NATO institutions also represents a potential for gaining access to individual types of space systems (whether navigation, communication or monitoring) and their use for the development of relevant capabilities. On the part of NATO, this aspect is further strengthened by the approval of the outer space as a separate operational domain, which creates conditions for further cooperation across the whole organization for the Czech Republic. Similarly, the growing opportunities resulting from the privatization/commercialization of this space can be assessed, although at the same time there is a threat of dependence on such an actor, which is associated with potentially different interests or unclear control over its activities. The nature of space as a separate operational domain imposes new requirements on the *Prepare/Training* area of the Armed Forces, which must take into account the specificities of this domain. In connection with the security interests and character of the Czech Republic and its armed forces, respectively, the main focus should

[8] ŠIŠKA, Martin. Velitelské shromáždění AČR: Vzletné fráze i skutečné potřeby vojáků [online]. *CZDefence*, 2020. Available from: https://bit.ly/3purCih

[9] PEJŠEK, Jan Satelitní centrum SATCEN ČR zahájilo operační činnost [online]. MO ČR, 2020. Available from: https://bit.ly/3x5uu7L

be on projects strengthening the main areas of capabilities *of Project; Consult, Command and Control* (C3); *Protect*; and *Inform*. These pre-requisites are met, among others, by the aforementioned development of the Galileo navigation system or the provision of data for the needs of (strategic) IMINT[10] through international cooperation with the European Union Satellite Centre (EU SatCen) or purchase from private providers. The Satellite Centre could be used for similar involvement at national level. Achieving independence from foreign suppliers should be brought about by the involvement of CAF in the aforementioned GOLEM project. Similarly, it is necessary to take into account the outputs of its civilian variants in the form of the HYPERION satellite constellation and links to the broader SPACE 2030 initiative.[11] All these projects are usable not only for the construction/strengthening of the complex C4ISTAR system, but also for ensuring a robust information flow for the control of unmanned and autonomous systems. In this context, the development of a stand-alone satellite system can significantly help strengthen the capabilities of the armed forces in all studied areas.

CYBERSPACE

Increasing of the strategic importance of cyberspace is directly linked to the development of information technologies and their present use, in fact, in all areas of human life. Information globalization provides any actor (state or non-state) with almost immediate and unlimited access to a huge amount of data and their subsequent processing and use for their own needs. In this sense, information, or raw data ("big data"), has become a strategic raw material usable both for positioning in this dimension and for influencing the functioning of the real environment. From the point of view 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* - e.g., in the form of the ability to deny the opponent access to this domain - represent important tools for achieving the set goals,[12] generally characterized not only by a very favourable ratio in the cost vs. profit assessment of the activities in question, but also by a reduced degree of attributability or punishability by the damaged party. In 2020, the United States was the target of the largest spy attack ever detected. Throughout the year, protected data leaked from both private entities (e.g. Microsoft, SolarWinds or FireEye) and ministries and other state entities (including the Cybersecurity and Infrastructure Security Agency or the National Security Agency).[13] As the need for and interest in electronic communication systems (videoconferencing), remote access, and other means of "working from home" related to the COVID-19 pandemic grew, so did the number of attacks against these utilities.[14] Similarly,

[10] The acronym denotes the intelligence discipline of *imagery intelligence*.
[11] GROHMANN, Jan. Česká vojenská družice GOLEM [online]. *Armádní noviny*, 2020. Available from: https://www.armadninoviny.cz/cesky-satelit-golem.html
[12] Cf., e.g., NATO. Strategic Foresight Analyses. 2017.
[13] HAUTALA, Laura. SolarWinds not the only company used to hack targets, tech execs say at hearing [online]. *CNET*, 2020. Available from: https://cnet.co/3zaEChm
[14] NABE, Cedric. *Impact of COVID-19 on Cybersecurity* [online]. Deloitte, 2020. Available from: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

companies involved in the development and delivery of vaccinations against this virus (e.g., Pfizer/BioNTech) became the target.[15]

The development of the so-called *Internet of Things (IoT)* is gradually escalating into the form of the so-called *"Internet of Everything" (IoE)*, which not only enables much more effective use of the benefits associated with all-embracing information interconnections (e.g., ensuring monitoring and real-time decision-making), but it also deepens the overall dependence on the stable and effective functioning of this space, resulting in increased user vulnerability. Construction and development of 5G information networks brings the discussed issue to a qualitatively higher level, both in terms of opportunities and possible threats. Ensuring security, in particular for the critical information infrastructures, must necessarily take this trend into account at present. Especially when taking into account the potential misuse of a large number of discussed devices within the so-called botnets to carry out targeted attacks against information systems of both relevant state and non-state entities. In this respect, last year brought a further increase in the frequency of such cases.[16]

Simultaneously with the intensification of the interconnection of humanity within this space, there is an increase in the number of networks that are created and used on a distributive basis, i.e., without the existence of a central control or management "node". The advantages of this approach can be demonstrated In the so-called "cloud computing" (or its more advanced variant in the form of "edge computing"), which, on a distributive basis, provides, inter alia, a flexible approach to storing and processing large amounts of data or provides new possibilities for increasing the computing power. Another example is the so-called "blockchain" technology. It is currently used by cryptocurrencies and is being gradually introduced in other areas (e.g., supply chain management in agriculture and industry).[17] As a result, the development of decentralized networks translates into an increase in the importance of the so-called "deep web", or, respectively, in a narrower sense involving security aspects the "dark web" and "darknet".[18] In particular, darkweb/darknet is directly linked to illegal activities across all areas (from illegal information gathering to trafficking in arms, addictive substances or human beings). Moreover, in addition to organized crime, similar means/possibilities are used, for example, by terrorist organizations and, in principle, by the states themselves. In fact, there is a further weakening of state power in the form of the ability to control, regulate and intervene against the activities and actors concerned, which is associated, among other things, with the conflict between the protection of national interests (in a broad sense) on the one hand and the usefulness of such networks on the other.

The interconnection of all areas of human society with cyberspace also further develops interdependence in terms of the availability of information itself. The digitization of the administration and the transfer of links between the citizen and the state to this domain

[15] PORTER, Sophie. Pfizer COVID-19 vaccine data leaked by hackers [online]. *Healthcare IT News*, 2020. Available from: https://bit.ly/3g6QrxL

[16] STAHIE, Silviu. *IoT Botnet Attacks on the Rise in 2020* [online]. Bitdefender Box, 2020. Available from: https://www.bitdefender.com/box/blog/iot-news/iot-botnet-attacks-rise-2020/

[17] DELOITTE. *5 Blockchain Trends for 2020* [online]. 2020. Available from: https://bit.ly/2Taq9S8

[18] For more details on these terms, cf., 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 from: https://goo.gl/AztPdM

(e.g., in the form of electronic identity cards or voting in elections) directly reflects this phenomenon, which, however, also brings along new forms of vulnerability (e.g., the issue of manipulation of electoral systems). From this perspective, the Internet makes it possible to increase the transparency of almost all activities in the real environment. Social media such as Facebook, Instagram, Twitter, YouTube, TikTok or last year presented Clubhouse allow almost constant supervision and monitoring of the 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. Control over these networks, or their providers, can therefore be seen as an important prerequisite for the ability to control and influence public opinion in general. On the other hand, similarly, this aspect helps to effectively defend against the influential activities of a potential opponent. Such ambitions can be identified, among others, in building the separate Russian Internet RuNet or extending the scope of the so-called "Great Firewall of China" to Hong Kong following mass demonstrations of its citizens.[19]

The full introduction of quantum (computing) technologies, which by their very nature fundamentally surpass the current performance of individual systems, will be crucial (not only) for this domain. This subsequently brings new possibilities, e.g., in the processing and storage of large data ("big data") or even corresponding threats/opportunities for current encryption tools and procedures, i.e., data and information protection itself. During the last year, new state and non-state actors joined the imaginary race for dominance in this area.[20] On the other hand, ensuring the widespread use of this technology is still a matter of long-term research and development.

The essence of cyberspace is also intrinsically linked to the development of elements of artificial intelligence/ machine learning. This trend is discussed in more detail in the following chapter in the context of the development of autonomous systems.

Information technologies are already linked to all areas of human life (including the citizen-state links). Gradually, there is a shift from the "Internet of Things" to the "Internet of Everything", which is associated with its misuse to perpetrate, for example, large DDoS attacks against state or non-state entities. At the same time, state power is further weakened through illegal darkweb/darknet activities. Increased attention is also paid to the development of quantum technologies that have the potential to significantly influence current approaches, e.g., in the field of cryptography. From the point of view of information operations (information activities, including dissemination of disinformation), social media / networks and actors who are able to process and use big data can play an important role.

Implications for the Armed Forces of the Czech Republic

From the perspective of the latest operational domain, **cyberspace** places increased demands on training and preparation, both to maximize its benefits and to suppress vulnerabilities resulting from the use of information technologies. The importance of the trends discussed above for CAF can be further identified for in the areas *Project; Engage; C3; Protect; Sustain* and *Inform*. Capacity development in these areas will be linked, inter

[19] KUO, Lily. China's Great Firewall descends on Hong Kong internet users [online]. *The Guardian*, 2020. Available from: https://bit.ly/3w1UXTG

[20] E.g., HACKETT, Robert. Quantum computing is entering a new dimension [online]. *Fortune*, 2020. Available from: https://bit.ly/34VlYek

alia, to systems enabling the processing of large volumes of data, as well as systems supporting operational changes in the level of centralization and decentralization of command and control. Completing the comprehensive interconnection of C4ISR in the environment of the Czech Republic should not only prevent the lagging behind more developed states in this area, but also provide an important competitive advantage both in the context of "small" and "large" armed conflicts. Military-adjusted "cloud" service elements can provide support for this development. The "blockchain" technology and the possibilities of its implementation for decentralization and data security (e.g., from unmanned reconnaissance devices) or increasing the resistance of CAF systems to the effects and consequences of electromagnetic pulse (EMP) or other methods of disrupting the operation of information and communication systems can also be used here. In all of these areas, the importance of cyberspace and the trends described above for information activities should not be overlooked. Attention must be paid 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 the action of the Czech Armed Forces against the opponent, as well as defence against such activities by the opponent. Ensuring consistent and continuous strategic communication (StratCom) toward domestic and foreign audiences plays a central role here. The *Engage* area also offers the possibility of combining with the abilities and elements of electronic warfare – e.g., in the form of introducing malware into the opponent's 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 experiencing attacks against hospital facilities in the Czech Republic, the biggest damage suffered by the Brno University Hospital. This threat has been further exacerbated by the ongoing COVID-19 pandemic. Similarly, it is necessary to ensure continuous evaluation of applications used mainly on business devices, including targeted search for so-called "zero date" vulnerabilities. However, this recommendation needs to relate not only to traditional platforms, but also to the area of the Internet of Things / Internet of Everything or the opportunities/threats associated with the development of quantum computing. Building on the experience, e.g., from the US, it can be assumed that these devices will be used not only as targets of cyber attacks in the near future, but also as a means for their implementation. Therefore, even for the armed forces of a state like the Czech Republic, it is necessary to ensure A2/AD capabilities in this domain, which would enable a stable use of this environment, and on the contrary deny access to the opponent. *Protect* also includes equally important *resilience* of the staff of the Czech Armed Forces. Permanent access to the information environment makes it an ideal target for both influential operations and specific cyber attacks perpetrated by the enemy. It will be necessary to ensure the development of both mental resilience and critical thinking or information literacy. In the *Sustain* area, experience from the ongoing pandemic points to increased demands on permeability and usability of all communication tools. For the Czech Republic, this implies the need to strengthen its IT infrastructure in order to avoid disrupting the stability of connections and remote access.

DEVELOPMENT AND DISSEMINATION OF REMOTELY CONTROLLED MEANS AND AUTONOMOUS SYSTEMS

Unmanned Aerial Systems (UAS) are currently used by the armed forces of more than sixty countries in the world for reconnaissance, exploration or monitoring purposes. The group of states that have combat (strike) drones is also gradually expanding. It can be assumed that this general trend, i.e., increasing the number of states possessing individual categories of unmanned assets, will only increase in intensity. Compared to piloted aircraft, lower acquisition and operating costs and the absence of direct threat to the human "crew" (operators) are preferred.

Through the development of, in particular, additive production and nanotechnologies (see ch. Additive production), new categories of UASs – micro and nano - are gradually introduced, with their dimensions approximating the size of insects. This aspect, among other things, gives them an advantage over traditional sensors and thus the ability to infiltrate secured areas undetected.

In superpowers in particular, it is possible to identify both the noticeable increase in the number of individual types of unmanned vehicles and the expansion of the range of tasks (e.g., supplies or transport) which they are used for. This trend can be very well demonstrated by the example of the United States, when its armed forces still had only two types of UASs in 2000.[21] There are currently at least 19 of them, including UASs equipped with weapons systems. The range of their tasks is illustrated, for example, by their deployment for targeted killings, as confirmed by the liquidation of Iran's leading General Qassem Soleimani using the unmanned MQ-9 Reaper at the beginning of 2020.[22] The above-described benefits of the UASs were further demonstrated by Turkey at the turn of March and April 2020 during Operation Spring Shield against the Syrian Armed Forces.[23] The crucial moment, however, was only the re-outbreak of the armed conflict over Nagorno-Karabakh in the autumn of the same year (for more details on the conflict, see ch. Military sector). On the side of Azerbaijan, the UASs of mainly Turkish and Israeli production complemented and, where necessary, effectively substituted the air force throughout the conflict. Unmanned assets were used both for reconnaissance and guidance, as well as for the destruction of ground targets, including anti-aircraft defence systems.[24] In principle, this was one of the first interstate conflicts involving a large-scale deployment of the UASs.

Unmanned Ground Systems (UGS) are so far represented in smaller numbers and variability within the armed forces of individual states compared to UASs. Their role is often directed to the disposal of booby traps and unexploded ordnance, handling of

[21] Office of the Secretary of Defence. *Unmanned Aircraft Systems Roadmap: 2005-2030* [online], p. 3. Washington, D. C., 2005. Available from: https://goo.gl/RBfrij
[22] U.S. Drone Strike in Iraq Kills Iranian Military Leader Qasem Soleimani [online]. *American Journal of International Law*, 2020, Vol. 114, No. 2, pp. 313-323. Available from: https://bit.ly/34VKdtR
[23] CRINO, Scott – DREBY, Andy. Turkey's Drone War in Syria – A Red Team View [online]. *Small Wars Journal*, 2020. Available from: https://bit.ly/3gg8QXI
[24] URCOSTA, Ridvan B. Drones in the Nagorno-Karabakh [online]. *Small Wars Journal*, 2020. Available from: https://smallwarsjournal.com/jrnl/art/drones-nagorno-karabakh

hazardous substances or short-range exploration (e.g., in urbanized areas). The Israeli army also uses these resources (Guardium project) to guard border areas and protect their bases. In addition to sensors designed to detect an enemy (intruder), the vehicles also carry weapons systems of both lethal and non-lethal nature.[25] Similarly, a remotely controlled modification of the latest Russian armoured vehicle on the Armata platform or individual US projects under the auspices of DARPA, directly linked to the needs/assumptions embedded in the so-called third offset strategy, should be in the development phase.[26]

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 in the case of unmanned systems, this approach is associated with the ability to control the so-called *swarms*, i.e., a high number of (small) means that will allow the congestion of the opponent's (air) defence. Intensive testing of these technologies takes place, for instance, in China, which is currently referred to as at least one of the leading countries.[27] Their use is assumed both for the execution of separate tasks (e.g., destruction of set targets), as well as for the support of other units or aircraft with human crew. Actually, there is also the development and strengthening of functional links between the various means to achieve synergies.

Similarly, projects for the joint operation of piloted/controlled systems and remotely controlled or autonomous systems are being developed. A manned device in such a combination generally plays the role of a leader supported by robotic systems. The result is a synergistic increase in the capabilities of such a set in practically all aspects. For example, under the *Skyborg* programme, the US is preparing an autonomous aircraft to accompany F-15s and F-35s.[28] Similar projects can be found, in principle, in all remaining domains (including cyberspace).

Compared to remotely controlled means, autonomous systems assume either no or minimal "interference" by the human operator. Individual systems should be able to not only obtain information about the surrounding environment independently, but also to process (evaluate) it and make appropriate decisions. The motivation to establish these systems stems directly from the increase in combat efficiency. Similar to remote-controlled devices, the idea of minimizing human losses on the part of own armed forces and non-participating persons is manifested here.[29] Systems based on elements of AI / machine learning more effectively suppress and remove limits resulting from human

---

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

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

[27] 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

[28] INSINNA, Valerie. These 3 companies will build prototypes for the Air Force's Skyborg drone [online]. *Defence News*, 2020. Available from: https://bit.ly/2RvMits

[29] Inter alia, cf. STOJAR, Richard. Bezpilotní prostředky a problematika jejich nasazení v soudobých konfliktech. *Obrana a strategie*. 2016, 16(2). Available from: https://goo.gl/dYJsZ2

physiology (including the need for sleep and the effect of fatigue, even in human operators, or the impact of stress).

On the other hand, serious questions arise here, including the degree of autonomy that should be granted to these systems and whether, at least from an ethical point of view, a decision can be taken to kill a human being by purely using these means. This aspect is increasingly being discussed across the professional community and provides an incentive for efforts to establish and enforce a control regime at international level (e.g., under the auspices of the UN).[30] On the other hand, it is necessary to critically point out that, following historical examples (e.g., cluster munitions, anti-personnel mines, etc.), the likelihood of reaching an overall ban across all states and enforcing it is rather unrealistic.

Certain elements of these technologies can already be identified today for air defence systems (e.g., the Phalanx close-in defence system[31] or Guardium's autonomous vehicle mode)[32]. In November 2020, they were used for the liquidation of Iran's leading nuclear scientist Mohsen Fakhrizadeh, presumably by Israel. According to the available information, the weapon system had, among others, satellite guidance and the ability to determine the target based on facial recognition.[33]

In systems based on AI / machine learning elements, significant potential can also be identified in relation to cyberspace, respectively to the collection, evaluation and handling of data and information in general. Their development and performance brings new possibilities, for example, for the areas of detailed analysis of a large number of documents, image elements or voice expressions. Subsequently, the ability to imitate them accurately and create copies or completely new elements (e.g., a virtual TV reporter) almost indistinguishable from reality/originals (in the form of the so-called *deepfakes*) is associated therewith. At the end of last year, this aspect was demonstrated through a false Christmas speech by Queen Elizabeth II, broadcasted by Channel 4 to warn about the potential *of fake news*, or *deepfakes*.[34]

Much attention is paid in general to the development of both unmanned and autonomous systems. For the time being, reconnaissance UASs are most represented in the armaments of individual states, but from individual projects of combat UAS or UGS, it is possible to conclude that a gradual expansion of this range will take place. New micro- and nano-categories are also being introduced. Research and development also focus on the ability to simultaneously deploy and control large quantities (swarms), especially of UASs. 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 dependent on the level of development of AI elements and affects resources and activities in all domains. At the same time, however, there is an intense debate on the moral/ethical aspects of using (not only) this type of technology for military purposes.

---

[30] E.g., Autonomous Weapons: An Open Letter from AI & Robotics Researchers [online]. *Future of Life Institute*, 2017. Available from: https://goo.gl/X2N6CA

[31] RAYTHEON. *Phalanx Close-in Weapon System: Last Line of Defence for Air, Land and Sea* [online]. Available from: https://goo.gl/Ky3RD1

[32] ARMY-TECHNOLOGY.COM, ref. 25.

[33] FARRELL, Stephen. Iranian nuclear scientist killed by one-ton automated gun in Israeli hit: Jewish Chronicle [online]. *Reuters*, 2020. Available from: https://reut.rs/3pvpN4x

[34] SAIGOL, Lina. 'Deepfake' Queen Elizabeth II will deliver alternative Christmas message warning about fake news [online]. *Market Watch*, 2020. Available from: https://on.mktw.net/2RBAqX4

Implications for the Armed Forces of the Czech Republic

The development of remotely controlled means and autonomous systems will primarily affect the areas of *Prepare/Training* and *Protect* not only in terms of their use, but also the ability to respond to their deployment by the opponent (regardless of their nature). However, the development of these devices definitely must not neglect the emerging categories of micro- and nano-UASs (see ch. Additive manufacturing). An interesting perspective in this area *(counter-UAS)* is provided by the use of a combination of a radar and directional jammer, or a powerful laser, however, not currently available in the Czech Republic. On the other hand, this development is already taking place in the Czech Republic, e.g., at the Military Technical Institute or the Academy of Sciences of the Czech Republic.[35] In this context, the orientation of counter-air defence should not focus solely on protection against individual UASs. On the contrary, it is necessary to develop, in particular, the capabilities enabling the destruction of whole swarms of such resources. Similarly, it is necessary to ensure the implementation of system measures aimed at preventing the misuse of our resources by the opponent (whether it is about obtaining intelligence or taking control of the affected system). From this point of view, the technological dimension of protection and defence as well as their overall procedural and legislative set-up cannot be overlooked. Due to the nature of CAF, in the areas *of Project; Engage; Sustain;* and *Inform*, it is necessary to emphasize the potential of "flocks/swarms" of remotely controlled means and the joint operation of piloted/controlled systems and remotely controlled or autonomous systems. Both areas make it possible to compensate for the size of the armed forces (or even the unfavourable demographic development and lack of the required personnel) and to cover a wide range of tasks (from survey to direct encounter with the opponent). Similarly, the use of autonomous systems (elements of AI / machine learning) creates opportunities for the development of skills not only in "physical" domains, but also in the already discussed cyberspace. Effective use of "flocks/swarms" of UASs and UGSs depends on the necessity to have sensors, communication systems and systems processing a huge amount of data about the surrounding operation of these means (see the issue of cyberspace). At the same time, it is also necessary to answer the above-mentioned legal and ethical questions related to the use of autonomous systems in particular, ideally before their potential acquisition.

DEVELOPMENT OF THE HUMAN-MACHINE INTERFACE

In addition to the above-mentioned trend of "robotization of the battlefield", projects are developed that make it possible to achieve more effective interconnection between the human and the machine component. In general, this should enable increasing the capacities of the human potential, whether in relation to the control of other systems, or individual physical and mental abilities of a person, reducing their vulnerabilities, and also eliminating the consequences of accidents or diseases.

In the first case, it is possible to identify the effort to provide all information from sensors to the human operator in real time, to eliminate the delay between the human response

[35] ŠIŠKA, Martin. Vojenský technický ústav chce vyvinout antidronové laserové dělo [online]. *CZDefence*, 2020. Available from: https://bit.ly/3v5fPb8

and the controlled system, while ensuring the execution of individual commands as if the person in control was the system concerned. In 2020, pilots of American fighter aircraft of the fifth generation F-35 were equipped with a new type of helmet (third generation),[36] which enable creating a comprehensive image from six infrared cameras and other connected sensors and providing information about the entire surrounding environment and the position of the opponent.[37]

The discussed area is very closely connected with technologies enabling the creation of the so-called augmented or plain virtual reality and, if possible, full human involvement and interaction with it. In this sense, the importance of information technologies and cyberspace, usable not only in the above-described (combat) activities, but also in planning combat operations and training and preparation of combat units, is emphasized again. The development of augmented and virtual reality makes it possible to simulate very faithfully, in our case, combat situations and environments which the units will operate in, including the possible behaviour of the opponent. Similar applications can also be identified for "non-combat" activities (e.g., healthcare or logistics).

In the second topic (increasing the performance of human abilities/activities), projects aimed at creating robotic combat suits (so-called exoskeletons) cannot be omitted. Benefits can be seen not only in the increase of strength, endurance or speed of a person (soldier) equipped with this means, but there is also another step in the protection, e.g., against enemy fire. Hydraulic systems, among others, increase the load capacity and greatly simplify the handling of "armour" (if we use the analogy with medieval warfare), which otherwise human individual would not be able to carry alone or perform any activity. The current stage of development can be demonstrated at tests of exoskeletons of Lockheed Martin or Raytheon, which should not only take on the weight of the armaments and equipment carried by a fighter and allow for possibly carrying (and manipulating) more load, but also increase the speed of movement and the distance the user is able to cover.[38] In 2020, this development was followed up by the United States Marine Corps, who decided to start testing the Guardian XO robotic exoskeletons.[39] In contrast, the functional model of "armour" has not yet been presented, although it can be expected that this situation will change in the coming years.

Apart from the exoskeleton projects, however, also technologies directly interfacing the human body, thus becoming its (integral) part, cannot be omitted. In particular, robotic limb replacements that should/could allow for perfectly compensating for such types of (combat) injuries, as well as eye or hearing replacements, may be considered. On the other hand, however, the potential of these technologies cannot be limited only to these situations and it can be very well assumed that with progress in the field of cybernetics, neurobiology, etc., it will become increasingly "lucrative" to increase human abilities through various muscle, sensory, etc. implants or the possibility of replacing a healthy

[36] INSINNA, Valerie. The Pentagon has cut the number of serious F-35 technical flaws in half [online]. *Defence News*, 2020. Available from: https://bit.ly/3gjvgXU
[37] LOCKHEED MARTIN CORPORATION. *The F-35 Helmet: Unprecedented Situational Awareness* [online]. 2016. Available from: https://goo.gl/MD6gDK
[38] E.g., HUSSEINI, T. US Army trials exoskeletons for military use [online]. *Army Technology*, 2019. Available from: https://bit.ly/2XCXZ0n
[39] HARKINS, Gina. Marines to Test Exoskeleton Suit That Can Do the Work of Up to 10 Troops [online]. *Militray.com*, 2020. Available from: https://bit.ly/3v6rQx4

organ or limb in order to achieve the above-described benefits. At present, however, neither ethical nor legal aspects related to the retention or removal of these implants after the termination of their active service, e.g., in the armed forces, are addressed in principle.

The development of human-machine interconnection is very closely linked to aspects of information technologies. Firstly, it is about streamlining the control of other systems – e.g., UASs – and developing elements of augmented and virtual reality. The second topic is the actual increase of human potential through its "reinforcement". In addition to the development of exoskeletons, there is also a possibility of replacing individual parts of human body, not necessarily when needed to compensate for the consequences of (devastating) injuries.

Implications for the Armed Forces of the Czech Republic

In the area *Prepare/Training*, trends in the **development of the human-machine interface** enable, through augmented and virtual reality, increasing the effectiveness of training programs and creating conditions for the needs of preparation of members of the Czech Armed Forces, for instance, closely resembling the real combat deployment. Currently, positive experience can be highlighted, among others, from the training of pilots, air controllers or service works in (aviation) technology, including the possibility of professional guidance or direct takeover of works by the manufacturer. Especially in training applications, it is also possible to consider interconnections with machine learning systems that could allow for better adaptation of the training load to the individual. Similar implications also arise for the areas *C3* and *Inform*, including through the creation of a comprehensive image of the battlefield and its mediation to relevant entities. More efficient control of other systems – e.g., UASs - and improvement of human capabilities both through exoskeletons and the replacement of human limbs and organs represent an important potential for the *Project; Engage; Protect* areas, where, in particular, 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 direction towards forming and reinforcing the human individuals, their descendants and possibly human civilization as a whole. The application of these trends in the military basically serves as a stimulating element for the human factor of the armed forces and its importance in military operations.

The nature of this discipline does not represent a new trend in the history of human society (e.g., in reference to the use of micro-organisms in the form of biological weapons). On the other hand, the developments in the area of genetics or the above-mentioned nanotechnologies bring new opportunities for achieving these ambitions. These overlaps are visible, among others, in the comprehensive nutrition projects, through which the effects of sleep deprivation are limited or muscle growth can be

stimulated.[40] The use of small animals and micro-organisms as components of the sensor network can be viewed in a similar way.[41]

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 "superhuman"). Similar to robotic technologies (human-machine interface), there is clearly a possibility of compensating for damage caused, e.g., by "combat injuries". However, compensation does not take place through prosthetic replacement, but, for illustration, by stimulating the growth of a new limb. Similarly, the broad issue of the so-called biological weapons, as one of the categories of weapons of mass destruction, cannot be overlooked. Through this area, they can, inter alia, acquire the "necessary" attributes of targeting specific persons or groups of persons or controlling the effects on them. On the other hand, these implications reflect probably the greatest degree of controversy and ethical/moral challenges for human society as a whole compared to other areas of technological development trends discussed.

Biotechnology represents the ability to shape and influence the nature and basis of living organisms, including the human individual. From the point of view of the military, it is essentially associated with the focus on the human factor of the armed forces. In general, it covers a wide range of aspects ranging from modification of the nutritional regime to the so-called genetic manipulation. At the same time, this area is probably characterized by the highest degree of controversy and the presence of moral/ethical challenges.

Implications for the Armed Forces of the Czech Republic

Implications of **biotechnology** for the CAF currently result primarily from the areas *Prepare/Training; Engage; Sustain*. Here, possible uses can be identified through the inclusion of nutritional supplements in the nutritional support of staff, both during training and deployment in military operations. Similarly, permanent evaluation and monitoring of the effectiveness of exercise processes and their impact on the development of the human body are also considered. The *Protect* area subsequently includes the issue of protection against biological weapons and the gradual need to take into account the possibility of using genetically modified micro-organisms by the opponent (state or non-state actor) not only against the armed forces, but also the civilian population.

DEVELOPMENT OF POWER TECHNOLOGIES

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

The first direction is directly associated with the energy demands of, for example, the above-mentioned robotic exoskeletons, the use of which is currently significantly limited

[40] E.g., SCHARRE, Paul – FISH, Lauren. *Human Performance Enhancement* [online]. Centre for a New American Security, 2018. Available from: https://1url.cz/gM4z8
[41] SOUTH, Todd. From Shellfish to Plankton [online]. *Navy Times,* 2018. Available from: https://1url.cz/LM4zA

by this aspect (in terms of performance or operating time). Efforts to find an effective substitute for fossil fuels in this respect are motivated (in addition to the general tackling of the issue of climate change by state and non-state actors) by the need to have mobile or easily transportable energy sources available and to decentralize the production itself.[42] At the same time, there is also the logic of reducing dependence on external actors and local resources and increasing self-sufficiency.

The second direction can be divided into three main categories of weapons systems. The distribution reflects the use of energy technologies to achieve both lethal and non-lethal effects. These are *Directed Energy Weapons (DEW),* weapons using energy pulses (EMP) and electromagnetic weapons. In general, the development is distributed across all these categories. In the first and third, the potential to replace "traditional" firearms can be identified. In contrast, the second category - EMP – has a more specific focus. In particular, it is designed against the electronic systems of the opponent in order to achieve elimination or destruction thereof. Central attention is paid to the development of non-nuclear assets that would be deployable without the need for conflict escalation or using nuclear weapons. Progressively, however, the possible use of microwave radiation against the opponent's staff is also developed.

In DEW and electromagnetic weapons, there are projects aiming at using these means in the framework of air and maritime combat, possibly as an alternative to missile defence elements. An example is the deployment of the Israeli system Lahav-Or (Light Blade) designed to shoot down, e.g., incendiary balloons[43] or the ongoing testing of DEW by the US Navy[44]. Similarly, according to sources,[45] the PRC navy has been increasing the capacity of its vessel generators for the future installation of electromagnetic cannons since last year. This orientation is conditioned by factual limits related to obtaining an efficient source of energy and its use to perform the required tasks (e.g., temporary or permanent blinding of sensors, destruction of a vessel or an incoming missile). For this reason, usability in the field of small arms is significantly reduced, where it is precisely the issue of energy requirements that does not yet make it possible to achieve greater efficiency compared to "traditional" weapons (e.g., due to weight, mobility or destructive effect). On the other hand, even the Chinese example (pistol and rifle prototypes published last year[46]) shows clear efforts to overcome these limitations.

At the same time, the usefulness of these technologies in the form of non-lethal weapons, i.e., means designed to "only" temporarily paralyze or neutralize the opponent, cannot be overlooked. The advantage is the general minimization of the loss of life of the civilian population, which becomes more relevant especially in the case of fighting in residential

---

[42] Cf. FUTURE ASSESMENT DIVISION. *Notes from the Edge: Insights into Evolving Future*, pp. 1–2. 2017.
[43] I24NEWS. *Israel unveils new laser air defence system against Gaza balloon terror* [online]. 2020. Available from: https://bit.ly/34W4Y95
[44] STARS AND STRIPES. *Navy warship uses a new high-energy laser to shoot down drone in mid-flight* [online]. 2020. Available from: https://bit.ly/3w81dJu
[45] PETTIT, Harry. Chinese Navy adds mega-generators to warships to power high-energy laser weapons and rail guns [online]. *The Sun*, 2020. Available from: https://bit.ly/3v3HDwL
[46] Chinese PLA Shows Rifle-size Electromagnetic Railgun Weapon [online]. *Defenceworld.net*, 2020. Available from: https://bit.ly/3g38bdm

areas or even in the performance of tasks not directly related to combat activities (e.g., when securing public order).[47]

The development of energy technologies focuses both on the search for / acquisition of alternative energy sources and their use in weapons systems. For weapons systems, three basic categories can be identified - weapons using directed energy, weapons using energy pulses (in particular, electromagnetic radiation) and electromagnetic weapons. In DEW and electromagnetic weapons, there are currently developments in the framework of air and maritime combat usage, possibly as an alternative to missile defence elements. The fundamental limit is in obtaining a stable and efficient source of energy and at the same time meeting the requirements for performance or mobility.

Implications for the Armed Forces of the Czech Republic

From the point of view of **energy technologies**, the development of (new) alternative energy sources can currently be considered relevant for CAF. In the areas *of Project; Engage; Sustain; Protect*, general efforts to ensure the self-sufficiency and independence of the armed forces are directly manifested not only during their deployment. At the same time, the so-called footprint on the battlefield is being reduced, i.e., the burden, for example, on the logistics of the armed forces, and the associated streamlining of the use of expended (material, human and financial) resources. From the point of view of developing the capacities of CAF, it is possible to fund these projects, inter alia, through the newly established European Defence Fund, which should also accentuate these areas.[48] In the *Protect* area, it is necessary to ensure cooperation with entities involved in the development of, in particular, energy systems applicable against unmanned aerial vehicles (see ch. *Development and dissemination of remotely controlled…*), and ensure their acquisition. It is also necessary to point out the threat of using the electromagnetic pulse by the opponent. In this respect, it is necessary to ensure the resilience of individual systems and, similarly to the response to large-scale cyber attacks, prepare alternatives (backups) in the event of their neutralization.

ADDITIVE MANUFACTURING AND NANOTECHNOLOGIES

Additive manufacturing ("3D printing" in particular) is a very rapidly developing industrial area. In the US, for example, around two-thirds of manufacturers use 3D printing at some stage of development and production.[49] Similarly, this technology is increasingly being used for the "construction" of buildings/objects,[50] which, from the point of view of the armed forces, represents a potentially easier and cheaper method of the construction of bases or outposts, e.g., in remote or difficult to access places. On the other hand, overall expansion and use of this method of production is only

[47] For more details, see, e.g., ARTICLE36. *Directed Energy Weapons* [online]. Discussion paper for the Convention on Certain Conventional Weapons, 2017. Available from: https://goo.gl/fiV7AW
[48] EUROPEAN EXTERNAL ACTION SERVICE. *Climate Change and Defence Roadmap*, p. 8 [online]. 2020. Available from: https://bit.ly/2T2M4KR
[49] NATO STO Sensors & Electronics Technology (SET) Panel. *Flexible Displays Technology Watch Card*. 2016.
[50] E.g., LANSARD, Martin. *The 15 Best Construction 3D Printers In 2019* [online]. Aniwaa, 2019. Available from: https://bit.ly/2Xyma01

expected in the next ten years. However, it is already possible to create spare parts for weapons systems and reduce storage and transport demands in a very flexible way, compared to traditional production methods. Although this example shows the importance for logistics, the usability itself extends over a much wider field of armed force projection or the production of the required (weapons) systems.[51] Similarly, the healthcare sector is developing rapidly. Additive production (3D printing) is an opportunity for the creation (printing) of human organs for transplantation, bone replacements, parts of tissue, and other parts of the human body.[52]

In this context, nanotechnologies represent a qualitative shift in the possibilities of additive production. This is an area that fundamentally affects the development of not only energy technologies, but also, for example, robotic technologies. The ability to create and influence the structure of individual materials and objects at the level of one billionth of a metre brings along new possibilities for both the resilience and protection of the armed forces (e.g., in the form of active masking) and the means of neutralizing the opponent.[53] The use of these aspects is visible, among others, in testing and acquisition of the so-called micro- and nano- unmanned systems (e.g., nano-UAS Black Hornet 3, etc.)[54] in all types of combat activities. In principle, the so-called chemical robotics (droplet-based liquid robots) can be included in a similar category. The wide application of nanotechnology also enables a higher level of biological protection of staff through nanofibre fabrics and membranes. In connection with the COVID-19 pandemic, these options were used in the production of nano masks and respirators.[55] Similarly, the protection of materials against weather and other external influences can be provided by special coatings. An example is the photovoltaic functional coating, which the building of the Czech Embassy in Canada was covered with in autumn 2020 (previously also used in embassies in London, Budapest and Washington. It removes harmful emissions and undesirable viruses and bacteria from the air through the effect of sunlight.[56]

Additive production allows very flexible production of almost any object, which is associated with a significant potential to streamline not only the area of logistics, but also, for example, a broader concept of the projection of the armed forces. In this respect, nanotechnologies represent a qualitative shift, which is given by the ability to create and influence the structure of individual materials and objects at the level of one billionth of a metre. The miniaturization of UASs or the use of nanofibre in biological protection, among others, represent importance for other areas.

---

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

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

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

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

[55] BREJLOVÁ, Iva. Jsme v nich vážně dobří. Česko se může stát v nanotechnologiích světovou velmocí, říká nanoexpert Jiří Kůs [online]. *Czech Crunch*, 2020. Available from: https://bit.ly/2TEB06T

[56] MVZ ČR. Česká nanotechnologie pomáhá v Kanadě v boji proti emisím i šíření Covid-19 [online]. 2020. Available from: https://bit.ly/3v6NEbL

Implications for the Armed Forces of the Czech Republic

Similar to previous trends in alternative energy sources, the development of **additive production** reflects efforts to ensure self-sufficiency and independence of the armed forces not only in the conditions of their deployment. The Czech Republic can benefit from the reduction of demands placed on logistics or force projection through the use of "3D printing" (*Project; Sustain* competence areas). The possibilities of constructing buildings/objects or producing spare parts are what provides an immediate incentive to develop associated capabilities. At the same time, the development of "bioprinting" provides a unique means for military medicine to ensure the healing of, inter alia, amputation or loss injuries. In the longer term, the importance of miniaturization through nanotechnologies is evident; from among the described trends, it affects, in particular, the further development of remotely controlled/autonomous systems, human-machine interfacing and energy technologies (related areas of *Engage; Protect*). In the *Protect* area, it is necessary to take into account the contribution of nano-fabrics to the development of biological and chemical protection capabilities. Similarly, new approaches are offered in the military healthcare sector (targeted transport of medicines or new types of dressing materials) or in logistics (protection of materials described above) (*Sustain* area). Among other things, CAF can benefit from the fact that Czech companies and institutions are among the world's leading players in this field. Generally speaking, it would not be dependent on foreign sources and would be able to cover its requirements from domestic suppliers.

HYPERSONIC TECHNOLOGIES

Hypersonic technologies represent another area of strategic competition among major powers.[57] These weapons systems operate at speeds higher than Mach 5 (6125 km/h), which together with high their manoeuvrability makes them almost unstoppable by the current means of missile defence. The hypersonic phase of their flight generally occurs during the return from space or its close proximity to the atmosphere or during their atmospheric flight powered by rocket or *scramjet* propulsion. Examples of these technologies are *hypersonic glide vehicles (HGV)* or *hypersonic cruise missile (HCM)*. Due to the velocities achieved, these systems can rely primarily on kinetic destructive effects. On the other hand, they can also be used as carriers of conventional or nuclear warheads. Similar attention is paid to anti-ship missiles, which are considered in Chinese strategic thinking to be the ideal means to ensure A2/AD capability against the American navy (aircraft carrier groups), at least for the South China Sea, East China Sea and Yellow Sea regions. In 2020, the PRC, the RF and the US tested their weapons systems.[58]

[57] WILSON, J. R. The emerging world of hypersonic weapons technology [online]. *Military & Aerospace Electronics*, 2019. Available from: https://bit.ly/36Ao9VE

[58] JUDSON, Jen. US-developed hypersonic missile hit within 6 inches of target, says Army secretary [online]. *Defence News*, 2020. Available from: https://bit.ly/3ipNDgp; China Reveals Hypersonic Cruise Missile Engine Test Success [online]. *Defenceworld.net*, 2020. Available from: https://bit.ly/3g1Tirr

Implications for the Armed Forces of the Czech Republic

From the point of view of the level of development of **hypersonic technologies**, and especially associated economic costs, these weapons systems do not constitute an immediate option for increasing the capabilities of the Czech Armed Forces. On the other hand, following the Czech Republic's membership in NATO, the assumption that these systems pose a clear challenge to the effective provision of defence against them, i.e., missile protection (the *Protect* area of capabilities), cannot be overlooked. Thus, even the Czech Republic should gradually take into account the increasing capabilities on the part of potential opponents, both at the practical and conceptual levels.

GENERAL IMPLICATIONS FOR THE ARMED FORCES OF THE CZECH REPUBLIC

It is very difficult to predict the pace of development of the above and other technological areas. On the other hand, at least well-known projects have relatively significant military implications, which even the Armed Forces of the Czech Republic should not ignore. The activities/initiatives that reflect these aspects can be clearly positively evaluated (whether it concerns the acquisition of unmanned assets, the subsequent construction of the 533rd battalion of unmanned systems of CAF, the ongoing building of capabilities of cyber forces and information operations, or the operation of the military intelligence satellite centre). Similar benefits can be provided by international cooperation projects, although it is always necessary to assess their outputs in the context of strengthening the capabilities of CAF.

Of course, it cannot be assumed that a comprehensive set of capabilities could be aimed at, as witnessed in the cases of major world powers (especially the US). Nevertheless, it is necessary not to neglect even those areas that may seem at first glance irrelevant and distant from the objectives and possibilities of the Czech Armed Forces as tools to pursue national interests. Otherwise, we run the risk of falling behind, which may no longer be possible to overcome. As a minimum, monitoring activities across alliance and European institutions should be encouraged to transfer the necessary know-how if any forward-looking project or direction of development is identified. For current examples of such activities, we can identify the involvement in NATO STO or EDA CapTech research panels.

In summary, the need to ensure the mutual compatibility and resulting interoperability of the deployed systems (not only within cyberspace) not only with allies, especially within NATO/EU, but also across their individual generations cannot be overlooked. Benefits linked to the ability to flexibly centralize and decentralize the chain of command and control and to establish interconnections between the different components of the armed forces can only be obtained if the above-mentioned requirement is met. At the same time, mutual compatibility also strengthens the resilience of the entire structure (robustness and redundancy – substitutability) and increases the effectiveness of its individual elements.

By blurring the border between the military and civilian dimensions, it can be assumed that the Czech Armed Forces will also be confronted, both abroad and possibly in the domestic environment, with the use of, for example, an unmanned aircraft or their swarm by a non-state actor. From this point of view, it is clearly desirable to allocate funds to projects aimed at comprehensive defence against such systems and, where appropriate, to assess whether, for example, current training also takes into account such a possibility.

Similarly, it can be assumed that this development will affect the nature of suppliers, not only domestic, but also foreign ones. Civilian (non-state) entities can increasingly be used for research/development and acquisition of the technologies concerned. Secondly, there is a certain dependence on these entities, which can manifest itself in 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 respective entities.

At the same time, it should not be forgotten that the development of individual technological trends and areas entails new challenges for arms control or the proliferation of individual systems, both at national and international levels. Increased attention should be paid, in particular, to the adequacy of current (legal) standards, how they are met and how they can be supplemented.

Technological Development. Implications for Czech Armed Forces Capabilities 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.

Graphic and editorial design: Mgr. Martin Doleček
Publisher: University of Defence
Print: Department of Publishing and Management of Study Resources
Circulation: 70 pc
Year of publication: 2020
Edition: first

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