Defense and Artificial Intelligence

Tomáš Pojar, Head of Aspen Institute CE Expert Group / Vice-President of CEVRO Institute
This text was written in collaboration with **Sara Polak** and with the assistance of experts from the Ministry of Defense of the Czech Republic, Military Intelligence and National Cyber and Information Security Agency.

Technologies will be the driving force of defense strategies of the twenty-first century. Whoever is able to better combine science and research with business and defense investments will have a significant edge in the protection of their own wealth and freedom in the upcoming decades.

Introduction

Competition between states and civilizations will increasingly take place in the field of technologies. In order to protect the critical infrastructure, modern societies will become more dependent on a symbiosis of state institutions, private companies and science facilities. Modernization, and the vulnerability of entire societies it entails, will depend on mastering emerging disruptive technologies (EDTs), including artificial intelligence (AI), which is slowly becoming an integral part of the modernization of developed countries' armies, and thus also of the rivalry between superpowers.

The bipolar world of the Cold War and the subsequent three decades characterized by the dominance of the United States is now transforming into a more chaotic multipolar world. In light of the growing instability of the world, and the key players' investment in new technologies, there is no doubt that any credible defense of Europe will have to include capabilities based on artificial intelligence. Not only the defense of states themselves, but also the defense of individuals in the digital space, is important. The defense of individuals is often independent of states and has become a problem we ought to address in parallel. The United States and China, in particular, are making long-term, robust and systematic investments into the utilization of modern, disruptive technologies. Russia and a number of other countries strive to follow the same direction in armaments. NATO and the European Union are

therefore also beginning to focus systematically on the utilization of AI. Europe definitely cannot be said, however, to be a world leader in this respect.

The Czech army has long been underfunded and, despite some minor improvement, we are still among the worst performers in NATO in terms of defense spending, although we have increased spending from 1% to 1.42% of GDP in 2020 in recent years. The good news is that we are finally managing to spend the recommended 20% of expenditure on investment. The bad news, however, is that we are far from meeting the criterion of 2% of defense spending on military research and development. We are not even at a quarter. The bare minimum is spent on projects related to EDTs or AI.

> "For decades, Nato allies have been leading when it comes to technology, but that's not obvious any more."[1] NATO Secretary General Jens Stoltenberg

Artificial intelligence is the ability of machines to perform tasks based on mathematical operations and statistics so as to speed up, refine and automate the relevant processes. This system does not have the ability to operate like a human 'at its discretion'. Artificial intelligence is therefore completely dependent on external parameters and data. According to NATO, it is one of the "emerging disruptive technologies" that have the potential to significantly transform the security environment and the balance of power in coming years. This will also allow traditionally weaker actors to promote their interests more easily at the expense of the unprepared. A good example of the use of AI is the area of proliferation of disinformation and cyberattacks. Advanced algorithms using machine learning allow for much more effective forms of political and criminal manipulation, at a minimal acquisition cost. The growing speed of dissemination of information thus dismantles another major barrier to its widespread utilization. Our ability to verify the veracity of information will therefore be increasingly frequently challenged by the ever-growing sophistication of methods of deception and manipulation. In line with this, the security aspect of AI utilization has been emphasized with growing frequency of late, in addition to its clearly revolutionary potential for the civilian sphere of life — be it in transportation, medicine, finance or marketing. It is also important to put an emphasis on educating society, which ought to be able to recognize disinformation and prevent its dissemination.

AI itself has the potential to work not only across technologies, but logically also across operating domains. Just like communications systems or the internal combustion

1) **WARRELL, Helen. Nato Allies Need to Speed Up AI Defence Co-operation.** *Financial Times* **[online]. 2021, 8.6.2021 [retrieved on: 2021-10-19]. Available at: https://www.ft.com/content/61c1945c-d153-4d58-b9c5-dffd99a6919e.**

engine, AI is becoming an indispensable component of ground, air, naval and space forces. It can naturally also create new or refine existing forms of hostile promotion of interests in cyberspace. Equally so, AI enables us to build more effective defenses. Defense and offense are two sides of the same coin. Ultimately, whoever has the stronger will and innovates more successfully will have a better chance of success.

There are significant pitfalls in a deeper integration of AI into military capabilities, especially at the strategic level: AI could indeed qualitatively transform the deterrence capability in both its forms. The "deterrence by punishment" would be transformed by increasing the offensive capabilities of strategic (including non-nuclear) weapons, for instance, in the areas of target identification and maneuvering. Machine learning could thus be used to detect a force hiding ballistic missiles, distinguish mock-ups from real carriers, and track the movement of mobile launchers. Most importantly, however, nuclear submarines hiding deep under the sea — a key element of safe second strike capability and an indispensable pillar of strategic stability between superpowers — could be detected.

AI offers an equally important implication in the second variation of deterrence, "deterrence by denial". Increased effectiveness of anti-missile systems could give the relevant state a false sense of security from a retaliatory strike, thus providing an excuse for its own action and subsequent conflict escalation. The involvement of artificial intelligence methods is also expected to significantly reduce decision-making time. The speed of interaction of algorithms will go beyond the cognitive capabilities of humans, which may further result in pressure for greater involvement of autonomous systems that do not require decisions by a human operator. War will therefore become more violent and harder to control.

> "Artificial intelligence boosts economic growth. But military use of artificial intelligence could unleash autonomous weapons systems that kill without human control."[2] German Federal Foreign Minister Heiko Maas

Visions of intelligent robots dominating the battlefield of the future have been around since the 1970s. Their materialization can be traced back to the beginning of the millennium, especially in the operations conducted by the US, Israeli and now also Turkish armies in the Middle East. The boom in automation and robotization of 'operational' processes, accompanied by the deployment of unmanned aerial vehicles, is apparent in Afghanistan,

2) Speech by Federal Foreign Minister Heiko Maas at the virtual conference "Human Rights in the Era of AI: Europe as an International Standard Setter for Artificial Intelligence". *Federal Foreign Office* [online]. 2021, 20.1.2021 [retrieved on: 2021-10-19]. Available at: https://www.auswaertiges-amt.de/en/newsroom/news/maas-human-rights-artificial-intelligence/2435928.

Iraq, Syria, Lebanon and Gaza. It has become apparent just how crucial the degree of technological superiority, which can hardly be compensated for by other means, such as superiority in numbers or a willingness to fight even under aggravated conditions, is. AI will certainly play a key role in the imaginary process of 'battlefield transformation'. It is important to note, however, that even behind an autonomous weapon system employing AI, there is a human factor responsible for programming the technology.

Fundamental breakthroughs in the use of AI can be dated back to the last decade, particularly in the context of advances in machine learning, sensing, and the miniaturization of powerful computer technology, which made it possible to overcome major obstacles in the areas of robustness, reliability, high-level decision-making, autonomous control, speech and image processing, etc. Current systems can already solve a broad range of complex decisions and optimization tasks faster and better than humans.

For the purposes of armed forces, AI already offers the achievement of information superiority over adversaries, both in ongoing operations and in preparation and training. The MODES project of the Czech Defense Ministry is being developed, for example, in this spirit. It is a modular expert system using machine learning to automatically recognize and classify data from commercial — and in the future, hopefully also Czech — satellites. AI can already be used within the armed forces in logistics, whether for planning deliveries, maintenance, shifts or supply routes. AI also has its place, for example, in the area of "predictive maintenance", i.e., the sensing of machine sounds and detecting potential defects that will lead to their timely removal, which can substantially reduce the life cycle costs of military equipment.

The computer defeated the world champion in chess, but also in the much more complex game of Go. The human player in cooperation, however, with the computer is unbeatable for the time being. The development of certain military systems is taking precisely this direction. The US, but also the Russian, Chinese or Israeli armed forces are testing cooperation between unmanned aerial vehicles and fighter aircraft. The drone acts as a decoy target, a reconnaissance vehicle or a mobile fuel supply. It can also carry sufficient weaponry to destroy both air and ground targets. The near future belongs to a symbiotic relationship between man and machine, with one compensating for the shortcomings of the other rather than replacing it.

Global Race

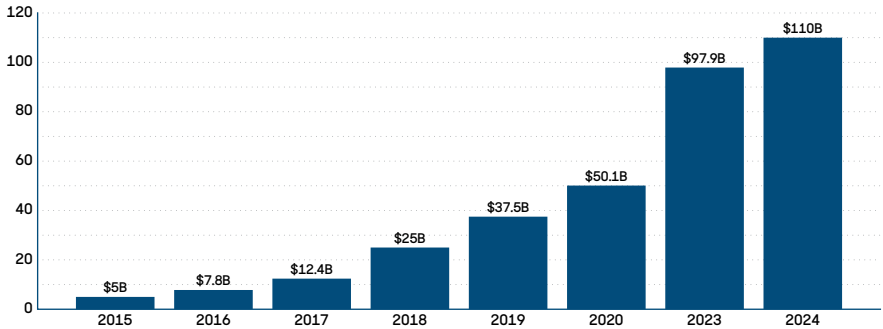
Revenues from systems using cognitive and artificial intelligence around the world will grow from $5 billion in 2015 to $110 billion in 2024.[3] Global AI and robotics expenditure in

3) Global AI Spending To Surge 120%, Hit $110 Billion by 2024. *Startupanz.com* [online]. 2020, 21.10.2020 [retrieved on: 2021-10-19]. Available at: https://startupanz.com/global-artificial-intelligence-spending-surge-120-hit-110bn-2024/.

the defense industry reached nearly $40 billion in 2018, with an estimated annual increase of about 5% over the next ten years, to $61 billion in 2027, a cumulative total of nearly $500 billion over ten years.[4]

Chart 1: Cognitive and artificial intelligence systems market revenue worldwide from 2015 to 2024 (in billion U.S. dollars)

Source: Statista, IDC Worldwide Artificial Intelligence Systems Spending Guide



The number of scholarly publications published in individual years can serve as one of the indicators of the importance of AI and the focus of research activities in this area: while it has been growing worldwide, China began to dominate it in 2005. The United States ranked second, followed by India, Great Britain, Germany, Japan, France and Canada. China only overtook the U.S., however, in the number of scientific literature citations dedicated to AI in 2020.[5] As regards research, development and implementation of AI in the military, the U.S. military is still on top, but countries such as Israel, Japan, South Korea and Turkey, as well as China and Russia, do not want to be left behind either.

For China, artificial intelligence has become a central technology through which it intends to wipe out the current military superiority of the United States. According to 2018 data, Beijing already spends almost as much on research and development ($468 billion) as the U.S. ($582 billion) in nominal terms.[6] Quantifying the total amount spent specifically to support AI is difficult because of its spread across many technology areas. According to the

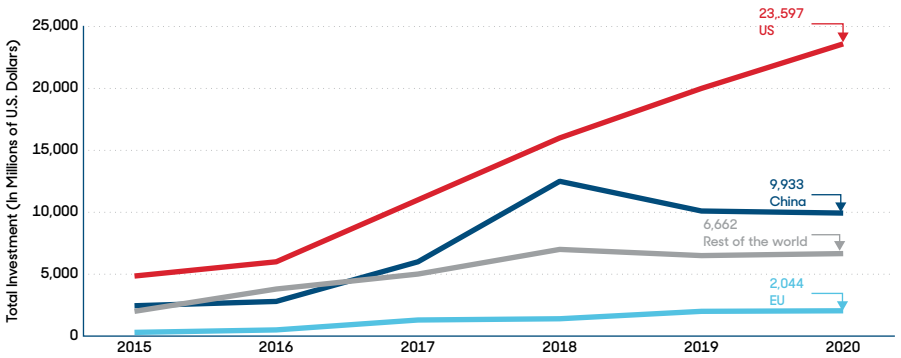
4) AI & Robotics in the Global Defense Industry to Reach $61 Billion by 2027. *Businesswire* [online]. 12.3.2021 [retrieved on: 2021-10-19]. Available at: https://www.businesswire.com/news/home/20210312005141/en/AI-Robotics-in-the-Global-Defense-Industry-to-Reach-61-Billion-by-2027---Robotics-Anticipated-to-Account-for-the-Largest-Share-of-Expenditure---ResearchAndMarkets.com.

5) ZHANG, Daniel, Saurabh MISHRA, Erik BRYNJOLFSSON, et al. Artificial Intelligence Index Report 2021. *OECD.AI* [online]. Stanford University, 2021 [retrieved on: 2021-10-19]. Available at: https://pp.wp.oecd.ai/app/uploads/2021/03/2021-AI-Index-Report.pdf.

6) Is China a Global Leader in Research and Development? *ChinaPower* [online]. 2018 [retrieved on: 2021-10-19]. Available at: https://chinapower.csis.org/china-research-and-development-rnd/.

data available, the United States leads over China in this comparison thus far, mainly due to private investor support which exceeds government expenditure.[7] Private investment into AI in particular increased by 9.3% in 2020 as compared to 2019. China's latest five-year plan, however, speaks clearly: it views AI support as an integral part of the technology and arms race between the superpowers.

Chart 2: Private Investment in AI by Geographic Area, 2015–20
Source: The AI Index 2021 Annual Report



Russia has naturally long focused on militarizing AI. In 2017, Vladimir Putin declared that whoever becomes the leader in AI will become the master of the world. A year later, the Ministry of Defense published a 10-point plan integrating AI into the core of the Russian military's modernization through consortia that include government institutions, the academia and industrial companies. Russia views AI mainly as an 'enabling technology' for the development of unmanned air, ground, sea and underwater platforms. Another area of interest for Russia is the involvement of AI in command, control and communication systems and, of course, its use in information warfare and intelligence operations. Russia's progress in the field of EDTs is nonetheless limited by a lack of foreign cooperation, funding (according to the OECD, only about 1% of Russia's GDP is spent on science and research), and a desire for self-sufficiency in electronic components.

China's 'top-down' model and civil-military cooperation setup allows Beijing to act fast, but such speed will come at the expense of the quality of the outcome. The West, on the other hand, hopes that the emergence of an ecosystem built on competition between

7) ARNOLD, Zachary. What Investment Trends Reveal about the Global AI Landscape. *Brookings* [online]. 2020 [retrieved on: 2021-10-19]. Available at: https://www.brookings.edu/techstream/what-investment-trends-reveal-about-the-global-ai-landscape/.

states, private companies, universities and science facilities will bring faster and better results. Such a race certainly cannot be won without robust financial support and efforts to integrate disruptive technologies into the armed forces' armaments and the protection of critical infrastructure systems.

NATO and the European Union

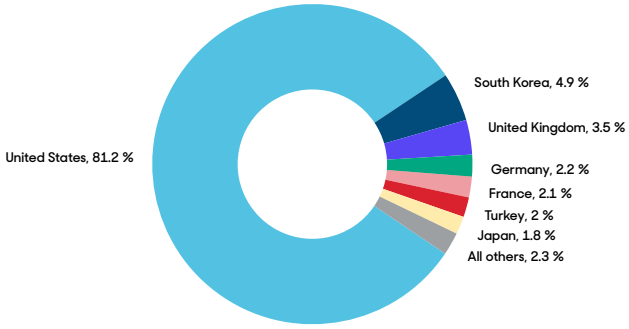
Research and deployment of new technologies in the military — particularly by China and Russia — has forced NATO to reconsider its own strategy and focus its efforts specifically on the development of AI and data processing. Although NATO has been officially addressing the issue in the context of autonomous systems since 2013, AI itself was only included in the priority areas at the 2018 summit. AI and big data are the first technology areas for which a specific implementation strategy is being developed. Once again, the main emphasis is on collaboration between private entities, government and academia, based on the recognition of the private sector's leadership role. The 2021 European AI regulation will also play an important role.

> "For decades, a lot of technological development would happen within the defence sector. Now, it goes the other way around. It's a civilian sector which is leading in the development of artificial intelligence, quantum computing, and many of the new disruptive technologies." NATO Secretary General Jens Stoltenberg

Cooperation between Member States in sharing experience and achieving standardization and interoperability of advanced systems is also a key aspect. At the last summit, Member States agreed on two key actions that will enable them to support the development of new and existing innovation capabilities and ensure the integration of EDTs into the capabilities of the Alliance: the DIANA initiative and the establishment of the Innovation Fund. Efforts are also underway to systematically integrate AI into military exercises. At the recent Spring Storm joint military exercise involving representatives from France, Denmark, Belgium, Estonia and the UK, AI-based systems were used, for example, to assess the environment and provide tactical information.

Figure 3: Government spending on science and research in the defense sector of OECD countries in 2017

Source: OECD



The United States of America is the undisputed leader in the development of AI-related technologies in the free world: the Pentagon alone plans to invest $874 million in this area next year. Washington's total investment in AI, including civilian projects, is then expected to reach six billion dollars in 2022.[8] Even in the EU, the development and implementation of AI, particularly in the industrial sector, is at a relatively good level. There are concerns, however, that Europe will not be able to maintain the pace. The development and implementation of AI in the defense sector in Europe is affected by the long-term lack of defense spending coupled with a still relatively good security situation. It can be seen, however, that countries such as Germany, France, the UK and Italy are striving to make up a certain deficit in this respect. The reality is such that, for instance, as regards software companies with the highest research and development expenditure, only twelve are based in the EU as compared to fifty-eight in the U.S. and fifteen in China. European countries as a whole stand out, however, in terms of the number of AI researchers.[9]

The EU itself views key technologies of the future similarly to NATO. In the area of security, it places an emphasis on the achievement of strategic autonomy and technological self-sufficiency, at least rhetorically. It should be added, however, that strategic autonomy is an empty slogan in light of the long-term underfunding of European armies and the resulting dependency on the United States. Nevertheless, during the recent Portuguese EU Presidency, a conference on EDTs was organized in cooperation with the European

8) HARPER, Jon. Federal AI Spending to Top $6 Billion. *National Defense Magazine* [online]. 2021 [retrieved on: 2021-10-19]. Available at: https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-$6-billion.

9) CASTRO, Daniel and Michael MCLAUGHLIN. Who Is Winning the AI Race: China, the EU, or the United States? — 2021 Update. *Information Technology & Innovation Foundation* [online]. 2021 [retrieved on: 2021-10-19]. Available at: https://itif.org/publications/2021/01/25/who-winning-ai-race-china-eu-or-united-states-2021-update.

Defence Agency (EDA). The meeting aimed to promote the idea of increasing funding of innovation in emerging and disruptive technologies and their integration into defense capabilities. The need for synergies at two levels was also declared: between NATO and the EU and between the civilian and defense sectors, in line with the recently presented EU *Action Plan for Synergies Between the Civilian, Space and Defence Industries*.

The Czech Republic

Compared to global leaders, the Czech Republic is rather lagging behind in AI status and development. The 2019 *National Strategy for Artificial Intelligence* ought to help. According to the *AI Readiness Report 2020* compiled by the Oxford Insights think tank, the Czech Republic certainly does not lack vision and was awarded a full score in this category. Overall, the Czech Republic was ranked 32nd, and we are 18th among EU countries, i.e., in the worse half. The fact remains that putting ambitious strategies into practice is not our strong suit — the army could testify to that, and not only with regard to unfulfilled promises in the budgetary area. Nevertheless, the national strategy has been at least partially reflected in the grant mechanisms of the Technology Agency of the Czech Republic (TAČR) or the Grant Agency of the Czech Republic (GAČR).

The entities dedicated to the development of artificial intelligence in the Czech Republic are mostly small and medium-sized enterprises or start-ups. A very interesting use of AI is provided for instance by the Brno-based firm SpaceKnow, which focuses on real-time analysis of satellite images. To ensure the security of cyberspace, AI is also used, for example, by Avast, whose software is able to adapt to the latest threats using machine learning and upgrade its customers' protection in real time. AI is also a core element of a product offered by resistant.ai which uses its system to detect financial fraud and counterfeit documents.

According to Eurostat data, we rank among the top three countries with the highest number of companies using AI for artificial speech synthesis and analysis: in the Czech Republic, this applies to 3% of all companies with more than 10 employees. A broad segment of companies is also working on facial and gesture recognition in CCTV footage. One such company is Eyedea Recognition. Neuron Soundware is engaged in machine sound analysis and predictive maintenance; their customers include giants such as Airbus, Siemens and BMW. Czech companies also have the advanced ability to analyze and classify large amounts of data and offer preliminary conclusions. Companies such as Tovek and Cogniware should be mentioned here. The latter firm is also able to use AI to track the dissemination of information in cyber-space, where it is able to map the progress of a particular narrative, such as disinformation, across websites and social networks.

As regards cooperation between the state and private entities and the creation of a common ecosystem, mention should also be made of university research taking place mainly in Prague and Brno. The main areas of interest are autonomy, cybersecurity, image data recognition and segmentation, speech processing and artificial speech synthesis. In addition to the Academy of Sciences of the Czech Republic, the leading facilities include the Artificial Intelligence Centre (AIC) and the Czech Institute of Informatics, Robotics and Cybernetics (CIIRC) attached to the Czech Technical University. Advanced research is also carried out at Charles University, especially at the Faculty of Mathematics and Physics. Also worthy of note is the Periculum Centre of Excellence at the Faculty of Social Sciences of Charles University, which explores the human-machine interface from a transdisciplinary perspective. Several research groups can be found at the Brno University of Technology, for instance, BUT SPEECH@FIT, which focuses on data mining from speech. Despite these solid individual results, the Czech Republic certainly does not stand out among EU countries in the number of disciplines and courses dedicated to AI according to the current ranking compiled by Stanford University.

The situation within the military is difficult both because of the accumulated internal debt and the resulting need to invest in the renewal of obsolete weapon systems, but also because of the deep-seated Czech caution in introducing new technologies, especially those that have not yet been operationally proven. AI is therefore currently not being systematically implemented into the military through advanced technological systems (such as autonomous and robotic means). The army and the Ministry of Defense have at least defined, however, their intent in addressing the area and supporting its implementation in the *Long-Term Defense Outlook 2035* and the *Army-building Concept 2030*.

Last year, the Pentagon established the AI Partnership for Defense, which, in addition to the U.S., includes Australia, Canada, Denmark, Estonia, France, Finland, Israel, Japan, South Korea, Norway, Sweden and the UK. This year, the Netherlands, Germany and Singapore have joined. Perhaps the best indication of how serious we really are about the whole issue is the fact that the Czech Republic is missing from this group.

Conclusion

Israeli army officials announced that during the May war with Islamist Hamas, the army used AI on a massive scale for the first time. While the experience there has, on the one hand, demonstrated the benefits of involving AI in combat operations, it has also clearly shown the current limitations of its use. While reaction times have been accelerated and strikes intensified, it was still not enough to achieve a clear victory. Nevertheless, the clashes in the Middle East have long demonstrated that the trends manifested there will sooner

or later affect the rest of the world. The use of AI-based technologies in military operations will be no different.

Automated driving of vehicles in the civilian sector will presumably reach full autonomy within a decade. Similarly, a high proportion of AI can be expected in military applications, and the deployment of AI will be an integral part of any operation carried out by the armies of developed countries. The trends may therefore trigger considerable instability not only in the global economy but also in the defense and security sectors. It is thus high time for AI development to be included among the Czech Republic's current national priorities, including armaments priorities in line with the example set by our richer allies within the alliance.

Given the state budget deficits, pressure for cuts in the defense sector will undoubtedly grow. It would be a fundamental mistake, however, to cut spending on investment and science and research. It is precisely investment in the modernization of the military, coupled with the development of modern technologies and the engagement of domestic research facilities and domestic industry, that is the best formula for preserving security, freedom and employment in the long run, as well as for boosting prosperity and competitiveness.

Recommendations

1. **Systematically support both civilian and military research in the area of AI.**
2. **Spend 2% of the GDP on defense, and of that, 20% on investment.**
3. **Spend 2% of defense expenditure on science and research, including EDTs.**
4. **Involve the Czech Republic in international initiatives, whether on the basis of the EU, NATO or like-minded countries.**
5. **Have the courage to introduce new technologies in the armaments area.**
6. **Support systematic education of the public on options for AI utilization, so as to attain its widespread implementation, in order to help initiate social change.**