NATO PARLIAMENTARY ASSEMBLY

SCIENCE AND TECHNOLOGY COMMITTEE (STC)

Sub-Committee on
Technology Trends and Security (STCTTS)

ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO'S ARMED FORCES

Report

Matej TONIN (Slovenia)
Rapporteur

149 STCTTS 19 E rev. 1 fin | Original: English | 13 October 2019

.

TABLE OF CONTENTS

I. INTRODUCTION 1

II. A BRIEF PRIMER ON AI 2

III. AI IN THE ARMED FORCES: OPPORTUNITIES, CHALLENGES, AND UNCERTAINTIES 3

- A. INFORMATION AND DECISION SUPPORT 3
- B. ROBOTIC AUTONOMOUS SYSTEMS 4
- C. NON-TECHNICAL CHALLENGES TO AI IN THE ARMED FORCES 6
- D. TECHNICAL CHALLENGES TO AI IN THE ARMED FORCES 6
- E. POTENTIAL IMPACT AT THE STRATEGIC LEVEL 8

IV. AI IN THE ARMED FORCES: A GLOBAL SNAPSHOT 8

- A. THE UNITED STATES 9
- B. EUROPE 9
- C. CHINA 11
- D. RUSSIA 11
- E. NATO 12

V. CONCLUDING REMARKS 13

SELECT BIBLIOGRAPHY 14

I. INTRODUCTION

1. Since its beginnings in the 1950s, the scientific field of Artificial Intelligence (AI) has seen periods of intense activities, but also two 'AI winters' when progress slowed down. In the 21st century, however, an extraordinary and sustained growth in AI research, development, and adoption has taken place. AI research began to boom around 2001, and commercial products and services started appearing in large numbers from the early 2010s. In a little over a decade, AI has thus moved out of the laboratories and into the consumer's hands. A few examples illustrate the scale of the AI explosion:

- In the late 1990s, experts believed that AI algorithms would not be able to beat masters of the board game *Go* for a century or longer. In 2016, Google's *AlphaGo* beat 18-time world champion Lee Sedol five times in a row.
- Half of all AI inventions ever registered were filed with patent offices between 2013 and 2018 (WIPO, 2019).
- Between 2016 and 2017, global venture capital investment into AI start-ups more than tripled, reaching EUR 11 billion (EPSC, 2018).
- AI's global economic impact between 2016 and 2026 could amount to between USD 1.5 and 3 trillion (Chen et al., 2016).

2. Undoubtedly, AI technologies and applications will have a tremendous impact. One recent study argues "[i]t is difficult to imagine any segment of society that will not be transformed by AI in the years to come" (EPSC, 2018). For now, the biggest impact is felt in telecommunications; transportation; life and medical sciences; personal devices, computing, and human-computer interaction; banking; entertainment; security; industry and manufacturing; agriculture; and social and digital networks (WIPO, 2019).

3. AI has already begun to make big waves in military and strategic affairs too. Some analysts suggest that AI "has the potential to be a transformative national security technology, on a par with nuclear weapons, aircraft, computers, and biotech" (Allen and Chan, 2017). This could potentially lead to a military revolution and perhaps a redefinition of the very notion of defence (De Spiegeleire, Maas and Sweijs, 2017). Others remain more cautious. They argue that "focusing on the distant prospect of dramatic change may well distract from developing a more nuanced understanding of slower and subtler, but equally significant, changes" (Cummings et al., 2018). However, almost all defence experts agree that potential for the application of AI in the armed forces is certainly "present in all domains […] and all levels of warfare" (Svenmarck et al., 2018).

4. This report informs and supports the Science and Technology Committee's (STC) continuing focus on: a) potentially disruptive technologies with important defence and security implications and b) the Alliance's need to maintain the science and technology (S&T) edge (see Box 1). It was adopted in 2019 by the STC at the 65th Annual Session of the NATO Parliamentary Assembly in London, United Kingdom.

Box 1: Related STC Work

Emerging Technology Reports

- Dark Dealings: How Terrorists Use Encrypted Messaging, the Dark Web and Cryptocurrencies
- The Internet of Things: Promises and Perils of a Disruptive Technology

"Maintaining the Edge" Reports and Resolutions

- NATO Science and Technology: Maintaining the Edge and Enhancing Alliance Agility
- Maintaining NATO's Technology Edge: Strategic Adaptation and Defence Research & Development
- Assembly Resolution 453
- Assembly Resolution 443

Fact-Finding Visits

- San Diego and Silicon Valley
- Berlin, Magdeburg, and Bremen
- Singapore
- London and South England, UK

II. A BRIEF PRIMER ON AI

5. No commonly accepted definition of AI exists. Fundamentally, AI is based on algorithms that are purpose-built to solve specific problems (Sheppard et al., 2018). Such AI "algorithms are being leveraged to collect, compile, structure, process, analyse, transmit and act upon increasingly large data sets" (IISS, 2018). AI is often assessed in comparison with human intelligence, as it seeks to reproduce the human information-processing loop, based upon perception, cognition, and action. AI can therefore also be understood as "the capability of a computer system to perform tasks that normally require human intelligence such as visual perception, speech recognition, and decision-making" (Cummings, 2018).

6. AI is not a dual-use, but an **omni-use technology** (Hoadley and Lucas, 2018). It never appears in isolation, and some analysts thus argue "AI is more akin to electricity or the combustion engine" (Horowitz et al., 2018). A direct consequence is that consumers do not 'buy' AI; they buy products and services that contain AI or upgrade their legacy systems with AI technology.

7. AI products and services bring together many different disciplines, including older AI work on 'expert systems'; natural-language processing; knowledge representation; automated reasoning; computer vision; data science; and robotics. However, the most important discipline for the recent AI boom is machine learning, attracting 60% of AI investment (Renda, 2019). Machine learning aims to enable machines to "automatically learn and improve from experience without being explicitly programmed" (CRS, 2018; see also Box 2). AI systems search and collect data from which they identify patterns and adapt their behaviour by drawing from task-specific instructions. A notable example of an impressive AI programme based on machine learning is Google's *AlphaZero* chess programme: in 2017, it went from learning chess by playing 'against itself' for only four hours to outcompeting one of the leading chess programmes on the market. The personalised recommendation systems for streaming or shopping applications are other common examples of machine-learning algorithms.

Box 2: Key machine-learning techniques

Reinforcement learning is based on the idea that optimal behaviour is bolstered by a positive reward. Machines remember the type of actions for which they received a positive outcome and seek to reproduce them.

Deep learning aims to provide machines with the ability to use large amounts of data sources to learn more than just one specific task.

Artificial neural networks aim to replicate the neural networks of human brains by sending signals through an interconnected, layered group of neurons.

8. One general way to understand the sophistication of AI systems is in terms of 'levels' (De Spiegeleire, Maas and Sweijs, 2017). Artificial narrow intelligence is achieved when machine intelligence equals or exceeds human performance for *specific*, highly tailored tasks. Artificial general intelligence is achieved when machine intelligence *equals* human intelligence for *any* task. Artificial superintelligence is achieved when it *surpasses* human intelligence for *any* task. All currently available solutions fall into the category of artificial narrow intelligence. Most analysts believe the latter two levels are far in the future or might never materialise.

9. A more granular view of AI sophistication compares system behaviour to the information-processing behaviour of humans (Cummings, 2018). Today's AI systems are not very good in applying themselves to situations of high uncertainty or in new contexts. They thus mostly exhibit skills- and rules-based behaviour (see Box 3).

III. AI IN THE ARMED FORCES: OPPORTUNITIES, CHALLENGES, AND UNCERTAINTIES

10. AI is already becoming a reality in armed forces around the world. All modern armed forces are, at a minimum, thinking through AI's implications, including the ethical and legal implications, and many are introducing concrete AI solutions (see also Section IV). AI holds enormous potential for the defence sector but also presents a set of technical and non-technical challenges. Moreover, the strategic implications of AI remain unclear.

11. Tackling all opportunities, challenges, and uncertainties in depth would go beyond the scope of this report (see also Box 4). Therefore, this section delves into two key areas of opportunity (information and decision support as well as robotic autonomous systems), crucial technical and non-technical challenges, including the debate about lethal autonomous weapons systems, and some potential strategic implications.

Box 3: Human information-processing behaviour (Cummings, 2018)

Skills-based behaviours: Actions which become highly automatic for humans when properly trained.

Rule-based behaviours: Actions humans perform in situations where complexity is too high to fall back on trained skills and where clear rules are available.

Knowledge-based reasoning: Actions humans carry out in situations where available rules do not exactly match the situation, but where they can fall back on their accumulated knowledge.

Expert behaviours: Actions in highly uncertain and/or time-critical situations where humans apply all their expertise, judgment, and intuition.

A. INFORMATION AND DECISION SUPPORT

12. Humans generally act in an environment of incomplete information. Sometimes, plenty of information is available. In military and strategic affairs, this is decidedly not the case. Political and military leaders must act in the well-known 'fog of war'. Information and decision support by AI systems is thus of high interest to military and strategic decision makers. Such systems can substantially increase both the pace and the quality of the processing, exploiting, and disseminating of information, as well as of human and machine decision-making.

13. In military terms, AI can considerably boost the **speed of analysis and action** of humans and machines. AI-enabled information and decision support systems can, for example:

- vastly improve the reaction times of <u>defensive systems</u> against fast-acting weapon systems, such as hypersonic missiles, cyberattacks, or directed-energy weapons;
- deliver <u>actionable information</u> faster to decision makers, which could potentially deliver a decisive edge on adversaries;
- quickly discover <u>cyber intrusions</u> by detecting evasive malicious codes or by scanning for suspicious patterns of behaviour rather than for specific code; and
- help identify attempts to manipulate citizens through <u>disinformation campaigns</u>.

Box 4: Fields of Applications for AI in Defence (non-exhaustive)

- Combat casualty care
- C4ISR (Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance)
- Cyber security and defence
- Electronic warfare
- Human resource management
- Information and decision support
- Intelligence
- Logistics
- Peacekeeping operations
- Robotic autonomous systems
- Social media
- Training

14. AI can improve the **quality of the decision making** of machines, but also, and perhaps most importantly, of humans. AI's ability to sift through today's data-rich environment and communicate findings in a compelling manner is crucial in this respect and will become ever-more important. While human resources currently allow for the processing of, at best, 20% of the information produced today, this percentage could go down to a mere 2% (Villani, 2018). To put it in the words of an

exasperated British officer, armed forces are already “swimming in sensors, drowning in data, [and] starving for insight” (White, 2019). AI solutions can help by, for example:

- providing better visualisation and interpretation of data (Killion, 2018);
- automatically extracting objects of interest from data feeds for follow-up actions, for example from surveillance video or satellite imagery (CRS, 2018);
- establishing ‘common operating pictures’ from information which emanates from very diverse sources, arrives in very different formats, and is often redundant or incomplete (Killion, 2018);
- highlighting abnormalities for follow-up investigations by comparing data points with previously developed normality models;
- extracting ‘weak signals’ which do not seem alarming by themselves but may be highly significant if linked with other data (Mercier, 2018);
- suggesting a menu of appropriate options and describing each option’s likely effects (Van den Bosch and Bronkhorst, 2018); and
- provide insights into adversarial behaviour through foreknowledge (Demchack, 2018).

B. ROBOTIC AUTONOMOUS SYSTEMS

15. The AI boom has largely coincided with the rapid proliferation of robotic autonomous systems, which are changing military and strategic affairs in their own right. This should come as no surprise as AI is a backbone technology in these systems.

16. While this is beginning to change, most robotic autonomous systems still carry out the ‘dull, dangerous, or dirty’ military tasks by augmenting or replacing human operators. They reduce the risk of human failure due to cognitive overload or, quite the reverse, ‘boredom’; free up human resources for tasks demanding higher cognitive functions; and remove military personnel from dangerous or hostile environments (Hoadley and Lucas, 2018).

17. Robotic autonomous systems are, *inter alia*, being used for explosive-ordinance disposal; counter-mine operations on land or underwater; rescue missions; logistical support; and even combat operations. The increasing autonomisation of military systems could greatly impact force structures in the future. The integration of robotic autonomous systems into combat formations, for example, could reduce a unit’s personnel number substantially. Autonomisation could also fundamentally change operational concepts. For example, swarms of robotic autonomous systems could be employed to overwhelm anti-access/area-denial defence postures (Hoadley and Lucas, 2018). At the strategic level, the fielding of robotic autonomous systems could give countries a significant military advantage and change the character of war.

18. The question of how military personnel and robotic autonomous systems will work together becomes central as more and more such systems enter the armed forces (this extends to non-robotic AI-enabled systems as well). Scientists and engineers are increasingly focusing on such human-machine teaming.

19. Humans and AI algorithms have different strengths and weaknesses (Madni and Madni, 2018). In some areas, humans perform better than machines. In others, machines outperform humans, and in certain areas, humans and machines perform equally well or equally bad. Human-machine teaming, thus, focuses on finding the right balance between human and machine in carrying out tasks. In some situations, the human-machine team will achieve the best results if the human is ‘in the loop’, with military personnel retaining a great deal of control. Operators must retain appropriate human involvement in decisions about the use of force(see below). However, humans may very well want to retain such control in other situations, too. For example, in times of heightened political crisis, operators would likely want to retain more control over unmanned aerial vehicles near unfriendly territory. In other situations, operators could merely choose to be ‘on the loop’. For example, as unmanned trucks follow a manned lead vehicle, an operator may wish to keep a close eye on the convoy but would only interfere if problems arise. In yet other circumstances, operators may decide

to stay out of the loop. For example, an unmanned underwater vehicle could be set to explore the oceanic environment autonomously to maintain communication silent to avoid detection.

20. Human-machine teaming need not be static (Madni and Madni, 2018). Increasingly, researchers seek to adapt the balance dynamically. For example, when humans perform under high cognitive load, machines could take more of the burden off the soldier. Humans can then step back into the loop when machines reach their limits. This could be in situations where they must deal with complex unstructured data, non-deterministic analysis, instances which they have not been trained for, or physical requirements beyond their capabilities (UK Ministry of Defence, 2018).

21. Implementing adequate human-machine teaming faces many hurdles. Perhaps most importantly, machines must be reliable enough to carry out the tasks, and operators must trust that they can do so (UK Ministry of Defence, 2018). As the human no longer supervises the machine at all times and in all contexts, it is crucial that the machine earns and keeps human trust (Madni and Madni, 2018). Furthermore, new human-machine teaming principles will require militaries to adapt operational concepts, training routines, personnel structures, organisational frameworks, institutional culture, and more. Designing suitable human-machine interfaces, for example augmented reality interfaces, and determining how many systems an operator can control will also be crucial. Technical challenges abound, too, for example ensuring sufficient processing power and developing secure operational cloud computing.

22. More than any other moral, legal, or ethical question concerning AI, the spectre of lethal autonomous weapon systems (i.e. systems with the capacity to kill without appropriate human supervision (see also Box 5), has attracted most of the attention. Within the Committee, this question has frequently been addressed and discussed with officials of the International Committee of the Red Cross, independent experts, and government and industry representatives. It was also a central concern during the STCTTS visit to the UK in June 2019 where AI and autonomous systems were at the heart of the agenda.

Box 5: Degrees of autonomy

Humans are **'in the loop'** if they retain a great degree of control over robotic autonomous systems.

Humans are **'on the loop'** when the system can autonomously take actions, but humans retain the ability to abort these actions.

Humans are **'off the loop'** if they are neither asked to confirm action nor can abort such actions.

23. Although no settled definition exists, lethal autonomous weapon systems do not yet exist under almost all definitions, and no nation has stated its intention to develop such systems. Moreover, general agreement exists in the international community that humans must retain appropriate human involvement in decisions about the use of force, although what this means exactly remains a matter of debate (Welsh, 2018). However, some experts doubt Russian and Chinese sincerity of intentions.

24. Alarmed by the prospect that some states could develop lethal autonomous weapon systems in the future, a number of civil society groups, parliamentarians (including members of the Committee), and states have advocated for a pre-emptive ban of such systems. Among others, they argue such systems, if they were ever developed, would:

- violate the laws of humanity and requirements of the public conscience;
- not be able to live up to international and national ethical and legal principles;
- weaken accountability principles when it comes to taking human life;
- lack the distinctiveness of human agency, for example, the ability to feel pain, pleasure, or empathy;
- be an affront to human dignity; and
- lower the threshold for military intervention.

25. It should be noted that some experts disagree with many of these arguments. They make the case that properly programmed autonomous systems could, in fact, more consistently live up to

moral, ethical, and legal obligations, and they underline the positive effects of removing emotions from combat.

26. In November 2017, a UN Group of Government Experts took up the question of lethal autonomous weapon systems. To date, around 30 countries have expressed their support for a pre-emptive ban, with Austria the only OSCE country to do so (Busby and Cuthbertson, 2018). China has advocated for a ban on using such systems, but not their development or production. However, some analysts doubt China's sincerity. In a 2018 UN position paper, China defined a "bizarrely narrow definition of lethal autonomous weapons" (Allen, 2019). Some countries would be amenable to banning systems with very little human control. However, a majority of states remains either uninvolved or unconvinced by a pre-emptive ban. The latter often argue that a ban is still premature and a better understanding of these systems is needed. For now, talks in the Group of Government Experts remain ongoing.

C. NON-TECHNICAL CHALLENGES TO AI IN THE ARMED FORCES

27. Introducing new technologies into the armed forces comes with distinct challenges – an issue the Committee has examined in great detail in other reports, visits, and activities over the last few years. In the context of this report, three of them stand out.

28. **The Investment Challenge**: to reap the benefits of AI, nations must allocate sufficient financial resources to develop and adopt AI systems in their armed forces, in line with their national defence AI goals. In this context, it bears repeating that nations should redouble their efforts to reach the 2% of GDP benchmark for defence spending by 2024 and allocate at least 20% of their total defence spending toward new equipment purchases and research and development (R&D).

29. **The Innovation Challenge**: armed forces must become better at adopting and integrating technologies from the non-defence commercial sector. Today, potentially disruptive inventions and innovations, including those based on AI, are increasingly driven by smaller and more commercially oriented companies. It goes beyond the scope of the report to delve deeply into the subject, but hurdles include:

- inadequate acquisition processes;
- cultural and organisational barriers in the armed forces as well as between the defence and civilian sectors;
- diverging incentive structures between the defence and civilian sectors; and
- a lack of commercial interest in certain militarily relevant niche areas.

30. **The Workforce Challenge**: this challenge is common to the introduction of all digital technologies into the armed forces. Globally and nationally, the pool of AI talent is shallow. More importantly, governments often cannot compete with the big technology companies in recruiting the best AI scientists and engineers. In the armed forces, military personnel also need to adapt to the new technologies through education, training, and exercises for example. In certain areas, AI systems can also crowd out personnel by taking over their tasks, which could have important effects on overall workforce developments.

D. TECHNICAL CHALLENGES TO AI IN THE ARMED FORCES

31. The adoption of AI in the armed forces also raises technical challenges common to all AI adopters. Most of them centre on the data available for AI, as the quantity and quality of data, is the main 'ingredient' for good AI algorithms. Two key problems stand out in this respect.

1. Data-Diet Vulnerability

32. Data input is central to AI algorithms. The quality of an AI algorithm depends, on the one hand, on its training data before integration into a product or service and, on the other hand, on the incoming data when applied in the real world. This leads to a so-called **data-diet vulnerability** (Osoba and Welser IV, 2017).

33. Since it is particularly difficult to collect data sets that are sufficiently large and representative to reflect real-world situations, AI reproduces biases present in its training data (Osoba and Welser IV, 2017). For example, the GloVe algorithm, which associates words of semantic similarity, was trained on 840 billion examples drawn from the web: it strongly tended to reproduce sexist and racist biases (Noël, 2018).

34. Even well-trained algorithms can be very brittle. Most importantly perhaps, AI-enabled systems are unable to adapt or adapt badly to new contexts, even if they are highly similar to the human mind (Hoadley and Lucas, 2018).

35. The data-diet vulnerability can sometimes be much greater in the defence sector. In certain parts of the defence enterprise, data is very scarce, compared to the civilian sector. For example, the data available to air forces on the behaviour of their aircraft in combat operations pale in comparison to the data pool commercial airline companies can access. Moreover, military personnel must often operate in environments where data is severely limited and situations are highly uncertain, for example in austere environments like Afghanistan (Sheppard et al., 2018). In other parts of the defence enterprise, data can be abundant, however. For example, the armed forces possess a vast trove of personnel data, which could lend itself to AI applications for human resource management (but also leads to hard questions for data privacy).

36. Scientists are working on overcoming the data-diet vulnerability through various means. One promising approach relies on older AI concepts, which are based on top-down models to mimic human intelligence – rather than relying on the availability of large volumes of data (Wilson, Daugherty, and Davenport, 2019). Moreover, this approach provides the added advantage of being explainable because they rely on clear and comprehensible logic (see also below).

2. Reliability Problems

37. If military personnel are asked to adopt AI-enabled systems, they must be able to trust that these systems work as intended. Yet, AI systems still suffer from severe **reliability problems**. In many cases, the level of trust must be much higher in the defence sector than in wide swaths of the civilian world. If an online shop recommends products the consumer is not at all interested in, little harm is done. If military AI systems make mistakes, the consequences can be much more serious, in the extreme leading to the loss of life.

38. Today, it is still very difficult and sometimes impossible to understand if AI systems draw the right conclusions and even *how* they arrive at those conclusions. The systems often appear as 'black boxes' to researchers and operators. Algorithms sometimes produce 'odd' results, solve problems in a counterintuitive or false manner, and sometimes even 'cheat' (Sheppard et al., 2018). The concept of 'explainable AI' and the need for new validation and verification processes specific to AI have thus become critical, as Committee members also learnt during their visit to the UK's AI Lab in June 2019.

39. Since AI systems are highly dependent on the accurateness of data, they are also highly vulnerable to input manipulation, including through cyber operations. Although the amount of processed data is often large, even the introduction of a small change in an algorithm could have catastrophic effects. In the case of image classifiers, for example, it has been proven that modifying only one pixel could be enough to mislead an AI algorithm (Svenmarck et al., 2018). A minor change

– intentionally or unintentionally – can thus lead the system to complete failure (Noël, 2018). In another recent study, an image classifier could be fooled into identifying a machine gun as a helicopter (Hoadley and Lucas, 2018). Another angle of attack is the training data. Deep neural networks often use models which are 'pre-trained' on third-party data. This third-party data could be an attractive target for adversaries (Svenmarck et al., 2018). AI systems as a whole can also be the target: malicious actors, including terrorists, could attempt to steal or replicate the systems, which they could then integrate into their own AI systems or use to find ways to neutralise the defender's systems (Hoadley and Lucas, 2018).

E. POTENTIAL IMPACT AT THE STRATEGIC LEVEL

40. It is still unclear whether the adoption of AI products and services in the armed forces will have minimal, evolutionary, or even revolutionary effects, but strategic thinkers are increasingly tackling these issues.

41. A number of them argue that AI will revolutionise military and strategic affairs. Several arguments stand out. First, military AI-enabled capabilities could begin to overmatch traditional military capabilities. All else being equal, AI-enabled military systems will likely outcompete similar systems which do not have AI built into them. More traditional high-tech systems could be vulnerable to novel disruptive AI-enabled systems. The military balance could thus shift decisively to those states who have the advantage in military AI systems (Payne, 2018). Second, in a world where humans are more and more remote from battlefields with large numbers of AI-enabled systems, societies might, over time, be less exposed to the consequences of military conflict, most importantly the death and destruction it often leads to. This could lower the threshold of war (Payne, 2018). Third, the emergence and adoption of new military technologies have, in the past, often led to an exacerbation of the so-called security dilemma (Meserole, 2018). Similarly, the proliferation of military AI systems could lead to uncertainty between potential adversaries and, ultimately, perhaps to an all-out 'AI arms race'. Fourth, AI could have even more extreme effects on strategic thinking. One analyst has argued that "[f]or the first time since the cognitive revolution began tens of millennia ago, human strategy may be shaped by non-biological intelligence that is neither embodied nor encultured" (Payne, 2018). This change, if it turns out to be true, would be more profound than the advent of nuclear weapons.

42. Other experts are far more sceptical AI will lead to such revolutionary changes. The adoption of military AI systems could merely be "a continuation of developments in the Information Age: leveraging data and computing power to gain advantage in a domain" (Sheppard et al., 2018). For the foreseeable future, AI in the military will thus be used to do "things humans do not have the time or capacity to do or do very poorly" (Sheppard et al., 2018). It should be noted that, while these changes might not be as profound as those mentioned above, they would certainly still change the armed forces significantly.

43. Ultimately, it is too early to tell what the effects of AI in the military and strategic affairs will be, in part because of decisions states have yet to make. This has been the case in the past when new military technologies emerged. What remains almost certain, however, is that the adoption of AI will have an impact across the full spectrum of force, as well as all other defence tasks, given AI's omni-use aspect.

IV. AI IN THE ARMED FORCES: A GLOBAL SNAPSHOT

44. To illustrate the increasing focus on AI in armed forces around the world, this section provides brief snapshots of key leaders in military AI inside and outside the Alliance, as well as of NATO-level efforts.

A. THE UNITED STATES

45. As the global leader in AI, the United States has actively sought to integrate AI into its military capabilities. Defence-related AI continues to be a big part of the efforts started under the Obama administration's Third Offset Strategy, aimed at the preservation of the US military advantage. In 2018, the US Department of Defense (DoD) published its own AI strategy, which will certainly be reinforced by the national American AI Initiative launched by the Trump administration in February 2019.

46. The DoD continues to invest significant resources in AI-related programmes and initiatives. A 2017 report estimated that, between 2013 and 2017, approximately USD 1.76 billion were devoted to three categories of relevant DoD spending (learning and intelligence; advanced computing; and AI systems) (Govini, 2017). In 2018, the Defense Advanced Research Projects Agency (DARPA) announced an additional USD 2 billion between 2018 and 2023. In 2016, the DoD created the Defense Innovation Unit (DIU) to facilitate the integration of commercial technology into the military. As the STC learned when meeting with DIU officials in October 2018, AI is a key area of the DIU's activities. In 2018, the DoD also established a Joint Artificial Intelligence Center (JAIC), whose Chief Architect laid out JAIC's aims during the October 2018 STC visit. JAIC has been allocated a budget of USD 1.75 billion for six years to oversee and coordinate DoD AI efforts.

47. The US military is engaged in numerous AI-related projects and programmes. A few examples illustrate the breadth of these activities:

- DARPA's **Target Recognition and Adaptation in Contested Environments (TRACE)** programme has delivered promising technologies, such as an automatic target-recognition system to assist pilots.
- The US Air Force is currently developing such a system, called **Multi-Domain Command and Control**, to better integrate the extensive data collected from its wide range of sources.
- **Project Maven** is an important information, surveillance and reconnaissance (ISR) programme, developed together with US tech giants such as Google, Microsoft, and Amazon. It helps human analysts, through computer-vision technologies, to process up to two to three times as much data in the same time period (CRS, 2018). The system is already in use in counter-Daesh operations.
- The US Army is testing **Uptake's Asset Performance Management** application to employ predictive maintenance in its M-2 Bradley infantry fighting vehicles. The STC delegation heard more about this topic from Uptake's leadership during the 2018 Silicon Valley visit.
- The Army is working on optionally manned **Next-Generation Combat Vehicles**.
- The Air Force Research Lab has initiated the **Skyborg** programme that seeks to train US Air Force pilots through an AI system, possibly hosted on an unmanned aircraft (Insinna, 2018).
- DARPA held a **Cyber Grand Challenge** pitting autonomous machines against one another. Each of these machines was designed with vulnerabilities, and contestants had to create AI algorithms capable of identifying and fixing these weaknesses while attacking their opponents (Hoadley and Lucas, 2018).
- The US Army is developing a tool called **Macroscope** which uses data produced by social networks to better understand social environments.

B. EUROPE

48. European states and the EU have increasingly recognised the growing importance of AI technologies and applications. Indeed, all EU member states and the European Commission have now adopted AI strategies. Many countries and the EU itself have substantially increased AI funding and set up organisational structures and entities to deal with the opportunities and challenges of AI. However, Europe is confronting a number of structural challenges. In terms of hardware, European actors still rely heavily on US chipmakers. Moreover, it faces intense competition from the United States where salaries are more attractive to European researchers. Europe is also

comparatively less successful at translating research into commercial products. Finally, Europe's comparatively stricter data security rules, which most Europeans value very highly, restrains its access to data pools (Franke, 2019). To deal with privacy and other ethical concerns, an EU High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence in April 2019.

49. As the EU builds up its defence initiatives, notably the European Defence Fund and the Permanent Structured Cooperation, defence-related AI R&D could certainly play an important role. For now, however, most efforts are designed and implemented at the national or bilateral levels, with the United Kingdom and France taking the leading role within Europe.

50. The **United Kingdom** government has committed GBP 1 billion to make the country a global AI leader. Once again, a few examples convey the range of defence-related AI projects and programmes:

- The Ministry of Defence and the Government Communications Headquarters have signed a **Defence and Security Partnership** with the Alan Turing Institute, a prime institute for data science and AI. The Partnership is focused on long-term projects, but also provides a training platform for government staff.
- The government has created an **AI Lab** to enhance the country's defence capabilities in AI, machine learning, and data science. The Lab focuses on autonomous vehicles, countering information operations, and improving cyber defences.
- The Defence Science and Technology Laboratory (Dstl) has organised several AI-related **challenges, competitions, and hackathons**.
- The Dstl has developed a radar tracking system, **Moonlight**, which uses machine learning to autonomously update information about enemy radars. It also provides indications and warnings to deployed units.
- The Royal Navy's **Project Nelson** aims to use AI to develop "a ship's mind" which should improve decision-making processes on its naval vessels. A core element is the creation of a fleet-wide data platform, making all relevant data available in highly usable interfaces.
- The Dstl, along with industry partners, has developed **SAPIENT**, an autonomous sensor system designed to reduce intelligence operators' workload.
- **Robotic autonomous systems** also draw continued investment. In 2018, the Armed Forces have tested five unmanned transport systems to supply troops on the front line, for example.

51. **France** has committed EUR 1.5 billion over five years to AI R&D and announced the creation of Interdisciplinary Institutes of Artificial Intelligence, connecting public and private researchers. The government has also recognised the military benefits of AI:

- Its newly established **Defence Innovation Agency** will focus a substantial part of its EUR 100 million in annual funding on AI-related activities (Anderson and Townsend, 2018).
- The French government has launched a three-year project on **man-machine teaming** for its combat aircraft systems and allocated a EUR 30 million budget to this effort. It focuses on smart/learning sensors; future cockpits and independent systems; and improved man-machine teaming.
- The **Artemis project** aims at developing an AI-powered system for data storage and management of the massive defence data France collects. The project aims to draw in civilian start-ups, laboratories, and small -and medium-sized enterprises.
- The ***Commandement et contrôle des operations armées*** project seeks to relieve operational leadership from repetitive, low-value-added tasks through big data solutions, AI, virtual reality, and other techniques.
- **Earthcube**, a Parisian start-up, has created an image-analysis software for satellite imagery and has signed four contracts with the French Ministry of Defence.

52. **Germany** has committed to a EUR 3 billion investment for AI R&D up to 2025. It also pledged to create 100 university chairs and a network of 12 research centres focused on AI. AI development and adoption in the armed forces appear to be sparse at this point. That being said, Germany has proposed closer cooperation with France on AI, among other initiatives. One example where AI will likely play a big role is the joint Franco-German Future Combat Air System project. The project likely seeks to incorporate virtual pilot assistance; automatic generation of mission plans; adaptation of sensors to the environment; adjustment of the man-machine interface depending on the pilot's cognitive load; and predictive maintenance (Pagot, 2019). In August 2018, Germany also launched a DARPA-style agency to focus on "disruptive" technology in cyberspace. Undoubtedly, AI will play a role in these efforts too.

C. CHINA

53. AI has become a top priority for Chinese leaders, both for commercial and military applications. As articulated in the 2017 New Generation AI Development Plan, China is aiming to become the global AI leader and develop a domestic AI market worth USD 150 billion by 2030. Already today, the government and industry have begun to believe that China has "largely closed the gap with the United States in both AI R&D and commercial AI products" (Allen, 2019). However, significant gaps remain in a number of areas, for example AI talent, technical standards, software frameworks and platforms, and semiconductors (Allen, 2019). China-based companies already play a significant role in the global development of AI technologies. Not only is China investing at home, but the country has also been investing abroad, which draws increased scrutiny by Allies.

54. As two Committee speakers outlined at the 2019 Spring Session, the entanglement of the private sector with public institutions, such as the party-state and the armed forces, significantly facilitates the incorporation of AI technologies into the defence sector, since top-down coordination clearly guides companies' development priorities. The emphasis put by President Xi Jinping on "military-civil fusion" is likely to sustain this trend (Sheppard et al., 2018). Moreover, China has been an early adopter of AI technologies for domestic surveillance applications. This lowers the barriers to adoption of AI-enabled systems by the military (Allen, 2019). Lower privacy standards compared to North America and Europe, combined with the sheer numerical advantage of the private data collected, provide a key advantage for developing new AI algorithms, too.

55. Analysts believe China's efforts to integrate AI into its military spectrum are informed by AI developments in other countries, notably the United States. China believes in a "military revolution of intelligentisation" (De Spiegeleire, Maas, and Sweijs, 2017). The Chinese government views the disruptive potential of AI as an opportunity to "leapfrog" the United States by investing heavily in novel disruptive systems, rather than only sustaining legacy systems (Allen, 2019). For example, Beijing has focused on the potential of AI for enhanced battlefield decision-making, cyber capabilities, cruise missiles, and autonomous vehicles in all military domains – all technologies which could present great difficulties for the United States in a conflict.

D. RUSSIA

56. President Vladimir Putin has declared that "AI is the future […]. Whoever becomes the leader in this sphere will become the ruler of the world". Although Russia still lags behind the United States and China, it has demonstrated its commitment to catching up with its competitors – at least in certain areas. Nevertheless, while Chinese and US companies spend billions of US dollars in AI, the Russian private sector only invested an estimated RUB 700 million annually (less than USD 11 million at the time of writing) (Horowitz et al., 2018). New reports indicate, however, that the Russian Direct Investment Fund has recently raised USD 2 billion from foreign investors to support the domestic AI sector (bne IntelliNews, 2019).

57. The Ministry of Defence, along with elements of the defence industry, has assumed a leading role on AI. For one, the Russian Military Industrial Committee seeks to make 30% of its military

equipment remotely controllable by 2025 (Allen and Chan, 2017). As part of this push, the Russian government created the Advanced Research Foundation, Russia's response to DARPA, whose annual budget stands at approximately RUB 4 billion (about USD 62 million at the time of writing). The agency has so far focused on technologies imitating human thinking, data analysis, and assimilation of new knowledge. It has also singled out four main lines of effort that AI developments should follow: image recognition; speech recognition; control of autonomous military systems; and life-cycle support for weapon systems (Bendett, 2018). Russia's AI national strategy is expected to be published in June 2019. In May 2019, President Putin outlined some of the strategy's priorities: training programmes, public-private partnerships, new legislation, and building on the country's strengths in science, technology, engineering and mathematics (Bendett, 2019). He and several ministers also hinted that up to USD 1.4 billion could be invested into domestic AI efforts to develop "technological sovereignty" in AI (Bendett, 2019).

58. Russian industries are integrating AI into weapons systems, especially robotic autonomous systems (Hoadley and Lucas, 2018). The Kalashnikov Group has reportedly developed an AI-controlled ground vehicle with neural network AI technology (IISS, 2018). The radio-electronic company KRET has reportedly been working on "unmanned systems with swarming and independent decision-making capabilities" (IISS, 2018). Moreover, the Russian Air Force has announced the development of AI-guided missiles. Analysts also argue that Russia's robust development of civilian technologies on image and speech recognition will likely be incorporated into Russian information operations (Bendett, 2018). It must be noted that Russia's ambitious AI plans may be hindered by structural challenges such as the weakness of Russia's technology industry and falling defence budgets (Hoadley and Lucas, 2018).

E. NATO

59. AI has never been on the agenda at a NATO summit. However, its political and military leadership was exposed to AI themes when the North Atlantic Council and the Military Committee focused their 2018 away day on disruptive technology, including AI. Across the NATO structures, however, several NATO entities have launched AI-related activities or included AI in their other activities in recent years:

- The **NATO Science and Technology Organization (STO)** has made AI and Big Data for Military and Decision-Making as well as Autonomy two of the three S&T themes. This designation, along with a large specialist meeting on the former theme, led to more AI activities in its Collaborative Program of Work, for example on appropriate human involvement in decisions about the use of force, AI-enabled cyber defence, and AI's contributions in the information environment.
- **Allied Command Transformation (ACT)** organises a number of events focused on AI's opportunities and challenges, for instance during its NATO-Industry Forums and International Concept Development and Experimentation Conferences.
- The **NATO Communications and Information Agency (NCI Agency)** made AI a central topic during its 2018 NATO Information Assurance Symposium. In November 2018, the NCI Agency also organised a Hackathon for Good to develop big data analysis, data visualisation, and machine learning tools against information operations. AI will also be one of the many topics on the agenda at the NITEC19 industry conference.
- The **NATO Industrial Advisory Group (NIAG)** has also engaged with AI issues. It recently produced two related studies: one on the use of big data by NATO and another one on the impact of autonomy on NATO planning and operations (Blunt, Riley and Richter, 2018).
- The **Science for Peace and Security Programme** explicitly solicited proposals on AI for countering terrorism in its 2017 call for proposals.

60. On a practical level, the Alliance has already used big-data approaches and machine learning, for instance for the elimination of duplicate or redundant copies of data sets collected by its mission in Afghanistan, as well as in anomalous-behaviour detection in log-file systems (Street et al. 2018). During a 2018 disaster-response exercise with NATO's partner Serbia, AI products and services were also used.

V. CONCLUDING REMARKS

61. As STC Special Rapporteur Leona Alleslev argued in 2018, the Alliance must, at a minimum, continue to fulfil two key objectives to ensure that NATO maintains its S&T edge, and these two objectives apply in equal measure to AI.

62. First, defence innovators in the Alliance must maintain their leadership positions. The Alliance must have the most advanced defence capabilities at its disposal to deter and, if that fails, defend against the threats facing the Allies. Given AI's potential for the armed forces, NATO's S&T leaders – in particular, the United States, the United Kingdom, France, and Germany – must invest in defence-related AI R&D to match developments outside the Alliance. It is encouraging to see that defence innovators in the Alliance are indeed investing substantial resources into defence-related AI, with the possible exception of Germany.

63. Second, the defence technology gap between Allies must remain small enough to be bridged by interoperability. The large diversity of Allies is ultimately a primary source of NATO's strength, but it also means that large differences exist in defence capabilities. There is a danger that the significant investment in AI in leading Allied nations could lead to substantial interoperability problems and a loss of NATO's overall military effectiveness in the future. However, the good news is that AI efforts do not need to be capital intensive, as the Committee witnessed during its fact-finding visit to Singapore in May 2019. Small- and medium-sized Allies with smart scientists and engineers can play an outsized role in AI development and adoption if they so choose. This could indeed be a very effective contribution to Allied burden sharing from the smaller Allied nations. To increase interoperability, cooperation through NATO' structures has a large role to play. Interoperability should be at the heart of AI efforts carried out by the STO, ACT, the NCI Agency, NIAG, and others. Allies leading in the S&T sector should encourage open architecture standards and regulations for technology sharing and transfer among Allies in order to narrow the technology gap, in line with all national obligations and the sensitive nature of technologies

64. Allied armed forces alone will not be able to solve the AI-specific challenges laid out in this report, including the ethical and legal questions. This will need a much broader push across the entire AI ecosystem. However, governments, NATO, and the EU can and must play a critical role in overcoming the investment, innovation, and workforce challenges of adopting AI. Just as national governments across the Alliance are rising to the challenge of AI, so should their armed forces. They should move beyond scanning the horizon and, instead, invest in real research, experimentation, development, and adoption efforts. It should be underlined that all dual-use and military AI efforts should, however, tackle all ethical, legal, and social questions right from the beginning, including privacy considerations and the definition of appropriate human involvement in decisions about the use of force. Allies should consider examining whether an ethics code of conduct could put the adoption of AI in the armed forces on a more stable foundation. At a strategic level, Allies must also address the geopolitical challenges, including the ones arising from Chinese and Russian investments in military AI systems. As this report has shown, Russia and China see AI as critical to future military power and invest heavily into AI-enabled military systems. For its part, the NATO PA Science and Technology Committee will continue to monitor AI developments in the defence sector through fact-finding visits and expert testimony.

SELECT BIBLIOGRAPHY

Allen, Greg and Chan, Taniel, *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, 2017

Allen, Gregory C., *Understanding China's AI Strategy*, *Center for a New American Security*, 2019

Anderson, Wendy R. and Townsend, Jim, "As AI Begins to Reshape Defense, Here's How Europe Can Keep Up", *Defense One*, 18 May 2018

Bendett, Samuel, "Putin Drops Hints about Upcoming National AI Strategy", *Defense One*, 30 May 2019

Bendett, Samuel, "The Development of Artificial Intelligence in Russia" in *AI, China, Russia and the Global Order: Technological, Political, Global and Creative Perspectives* (ed.: Wright, Nicholas D.), US DOD and Joint Chiefs of Staff, 2018

Blunt, Richard, Riley, Chris and Richter, Marc, "Using Data Analytics and Machine Learning to Assess NATO's Information Environment", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

bne IntelliNews, "Russia Raises $2Bln for Investment in Artificial Intelligence", *The Moscow Times*, 31 May 2019

Busby, Mattha and Cuthbertson, Anthony, "'Killer Robots' Ban Blocked by US and Russia at UN Meeting", *The Independent*, 3 September 2018,

Chen, Nicholas et al., *Global Economic Impacts Associated with Artificial Intelligence*, Analysis Group, 2016

CRS (Congressional Research Service), *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, CRS, 2018

Cummings, Mary et al., *Artificial Intelligence and International Affairs: Disruption Anticipated*, Chatham House, 2018

Cummings, Mary L., "Artificial Intelligence and the Future of Warfare", in *Artificial Intelligence and International Affairs: Disruption Anticipated* (eds.: Cummings, Mary L. et al.), Chatham House, 2018

De Spiegeleire S., Maas M. and Sweijs T., *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers*, The Hague Centre for Strategic Studies, 2017

Demchak, Chris C., "Four Horsemen of AI Conflict: Scale, Speed, Foreknowledge, and Strategic Coherence" in *AI, China, Russia and the Global Order: Technological, Political, Global and Creative Perspectives* (ed.: Wright, Nicholas D.), US DOD and Joint Chiefs of Staff, 2018

EPSC (European Political Strategy Centre), *The Age of Artificial Intelligence: Towards a European Strategy for Human-Centric Machines*, EPSC, 2018

Franke, Ulrike, *Harnessing Artificial Intelligence*, European Council on Foreign Relations, June 2019

Govini, *Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy*, Govini, 2017

Hoadley, Daniel S. and Lucas, Nathan J., *Artificial Intelligence and National Security*, CRS, 2018

Horowitz, Michael C. et al., *Strategic Competition in an Era of Artificial Intelligence*, Center for a New American Security, 2018

IISS, "Big Data, Artificial Intelligence and Defence", in *The Military Balance 2018*, IISS, 2018

Insinna, Valerie, "Introducing Skyborg, your New AI Wingman", *C4ISRNET*, 14 March 2019

Killion, Thomas H., *How AI, Machine Learning and Big Data is Transforming ISR & C2 Capabilities*, ICPQ, 2018

Madni, Azad M., and Madni, Carla C., "Architectural Framework for Exploring Adaptive Human-Machine Teaming Options in Simulated Dynamic Environments", *Systems*, vol. 6, no. 44, 2018

Mercier, Denis, "How Will Artificial Intelligence and Disruptive Technologies Transform Military Operations and Organizations?", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

Meserole, Chris, *Artificial Intelligence and the Security Dilemma*, Brookings, 2018

Noël, Jean-Christophe, *Intelligence Artificielle : Vers une Nouvelle Révolution Militaire ?*, IFRI, 2018

Osoba, Osonde A. and Welser IV, William, *Risks of Artificial Intelligence*, RAND, 2017

Pagot, Yves, "*Le SCAF raconté par ses concepteurs"*, Portail Aviation, 31 January 2019, *http://www.portail-aviation.com/blog/2019/01/31/le-scaf-par-ses-concepteurs/*

Payne, Kenneth, Artificial Intelligence: A Revolution in Strategic Affairs, *Survival: Global Politics and Strategy*, vol. 60, no. 5, 2018

Renda, Andrea, *Artificial Intelligence: Ethics, Governance and Policy Challenges*, Centre for European Policy Studies, 2019

Sheppard, Lindsey R. et al., *Artificial Intelligence and National Security: the Importance of the Ecosystem*, CSIS, November 2018

Street, Michael et al., "Lessons Learned from Initial Exploitation of Big Data and AI to Support NATO Decision Making" in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

Svenmarck, Peter et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

UK Ministry of Defence, *Joint Concept Note 1/18: Human-Machine Teaming*, Development, Concepts and Doctrine Centre, 2018

Van den Bosch, Karel and Bronkhorst, Adelbert, "Human-AI Cooperation to Benefit Military Decision-Making", in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*, NATO Science and Technology Organisation, 2018

Villani, Cédric, *Donner un Sens à l'Intelligence Artificielle : pour une Stratégie Nationale et Européenne*, Mission confiée par le Premier Ministre Édouard Philippe, 2018

Welsh, Sean, "Kill Switch", *Jane's Intelligence Review*, March 2018

White, Andrew, "Reality Check: Applying AR and AI Technology Across the Battlespace", *Jane's International Defence Review*, January 2019

Wilson, H. James, Daugherty, Paul R., and Davenport, Chase, "The Future of AI Will Be About Less Data, Not More", *Harvard Business Review*, 14 January 2019

WIPO (World Intellectual Property Organization), WIPO Technology Trends 2019: Artificial Intelligence, WIPO, 2019