

THE IMPACT OF AI ON NATO MEMBER STATES' STRATEGIC THINKING

Alex ETL

Ph.D., Institute for Strategic and Defense Studies, Eötvös József Research Center,
National University of Public Service, Budapest, Hungary
etl.alex@uni-nke.hu, alex.etl@europe.com

Abstract: *The incorporation of Artificial Intelligence (AI) into military capabilities creates various challenges for NATO. Since AI will impact the full spectrum of military capabilities, different militaries will have various reactions for these challenges. This article asks how might these reactions impact NATO member states' strategic thinking around AI? To answer this question the article analyzes member state-specific data published by the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) and cross referencing it with specific operator countries. On the strategic level, the article compares the United States' and France's AI defense strategies, highlighting their similarities and differences with regards to their assessments on the strategic environment; emerging threats; as well as objectives and capabilities. The analysis shows diverging development paths among NATO members, thus pointing towards the emergence of different AI-enabled technology clusters in the alliance. The integration of AI-enabled systems into allied military forces shows not only striking disparities but a deep level of fragmentation. The article also identifies a new form of capability gap among those member states, which have more capabilities. In this context, policies pursued by AI great powers are deepening intra-alliance fragmentations, while AI middle powers, like Poland or the Netherlands, are becoming more interoperable with other member states.*

Keywords: *Artificial intelligence; NATO; alliance; capability; cooperation; autonomous weapons.*

Introduction

The rapid spread of new, AI-enabled technologies across the full spectrum of military capabilities poses several unforeseen challenges for the defense sector. AI impacts decision-making processes, the nature of deterrence, but also the use and character of individual capabilities and hence, the modes of warfare. Each militaries have different reactions for these new developments, while they try to cope with the dynamically changing technological landscape. How might these different reactions impact NATO member states' strategic thinking around AI? This article argues that the spread of AI-enabled technologies will enhance already existing strategic divergences within NATO, while creating a new form of capability gap among member states.

The article departs from the implications of AI on military affairs. For this purpose, the article relies on the quickly expanding AI and military affairs literature. The analysis identifies decision-making processes; the enhancement of military capabilities; and the global arms race as three major areas within military affairs, where AI-enabled technologies can have a transformative impact. Whereas these all have important implications for NATO as an alliance, the primary goal is to move beyond theoretical discussions and provide empirical data analysis for the study of intra-alliance capability dynamics. The article does so by relying on the analysis of the member state-specific data published by the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) and cross referencing it with specific operator countries. The article highlights diverging development paths among NATO members, thus pointing towards the emergence of different AI-enabled technology clusters in the alliance. The analysis also demonstrates a diverse spectrum of country-specific AI-enabled programmes leading towards intra-alliance capability fragmentations and a limited level of interoperability. In this context, policies pursued by AI great powers are deepening intra-

alliance fragmentations, while AI middle powers, like Poland or the Netherlands, are more likely to procure AI-enabled technologies from other member states.

Following this endeavor, the article focuses on the strategic level and compares France's and the United States' AI defense strategies, while highlighting their similarities and differences with regards to their assessments on the strategic environment; emerging threats; as well as objectives and capabilities. This will highlight how the use of AI in the armed forces have already manifested itself into diverging strategic thinking in these two influential member states. Finally, the article discusses how these emerging capability fragmentations and strategic divergences within NATO might impact intra-alliance dynamics. Thus, it sheds light on a new form of capability gap in NATO not just among member states who have and have no significant AI-enabled military systems but also among technologically more advanced member states, causing future interoperability and operational problems.

The rest of this article is constructed as follows. The first section provides a survey of the literature concerning the transformative impact of AI on defense and military affairs. The second section turns towards the analysis of AI-enabled technologies in NATO member states' militaries and utilizes the member state-specific data. Following this endeavor, the article compares the United States' and France's AI defense strategies. Finally, the article discusses how these emerging capability fragmentations and strategic divergences within NATO might impact intra-alliance dynamics.

Artificial intelligence in military affairs

Before highlighting the impact of AI on NATO, we need to contextualize how AI can influence military affairs in general. Although the definitions of emerging and disruptive technologies, artificial intelligence and autonomous weapon systems remain contested, a quick survey of the literature around these topics reveals three major areas within military affairs where they can have a transformative impact. These include military decision-making processes; the enhancement of military capabilities; and the global arms race. Whereas this selection is necessarily arbitrary, almost all recent advances within the AI and military affairs literature fall under the umbrella of these three areas.

Concerning the role of AI in military decision-making processes, the most often debated aspect arises from the general discussion on human-machine collaboration, and its consequences on the nature of warfare. For example, Ekelhof highlights that AI and autonomy has an impact on the whole military targeting process, affecting primarily the intelligence branches of the military, and while they speed up the process of targeting, they also influence critical targeting decisions, and can shift responsibilities within the decision-making structure. (Ekelhof 2018 , 81-83) Verbruggen argues that military AI will drastically reduce the time of various operations, thus providing less time for decision-making and, consequently, less room for consideration (Verbruggen 2020, 14). Since AI accelerates the course of military events, it increases the pressure on decision-makers, which enhances psychological challenges for them (Verbruggen 2020, 14). Johnson introduces how AI threatens strategic stability, through compressing decision-making frames, and how perceptions linked to the irresistible advantages of military AI increases the chances of inadvertent escalation (Johnson 2020, 17). Similarly, the RAND Corporation's 2020 wargaming exercise also confirmed that the speed of autonomous systems might lead to inadvertent escalation (Wong, et al. 2020, xi). On the other hand, Boulanin notes that military AI might also provide flexibility for decision-makers, as the recoverability of these systems (e.g. Unmanned Aerial Vehicles and Unmanned Underwater Vehicles) makes potential de-escalation dynamics also easier (Boulanin 2019, 57).

The literature on the enhancement of offensive and defensive military capabilities is also rapidly expanding as technology advances. Boulanin identifies five general capability areas, in

which autonomy can have a variety of functions: mobility; health management; interoperability; battlefield intelligence; and the use of force (Boulanin 2016, 7-8). Each of these areas incorporate various tasks from navigation, through data collection, to fire control (Boulanin 2016, 7-8). Whereas the discussion on autonomous weapons is usually focusing on the use of force (e.g.: loitering munitions; unmanned aerial/ground/underwater vehicles; missile and rocket defense; guided missiles; anti-personnel sentry weapons; active vehicle protection; sensor-fueled munitions; encapsulated torpedoes and mines etc.) AI and autonomy affect military capabilities in a much broader spectrum (Boulanin 2016, 7-8). At the end, they enhance speed, precision, lethality, data-processing, detection, and C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) capabilities.

The general advantage of AI enabled military technologies points towards the third area: the global arms race. For example, Verbruggen highlights a possible scenario, in which conventional weapons are no longer capable to maintain the pace of operations conducted with autonomous weapons, which therefore creates new incentives for states to develop and acquire autonomous weapons more extensively (Verbruggen 2020, 14). Abaimov and Martellini provide empirical data for the emerging AI arms race, highlighting the rapidly expanding military AI-industry and R&D expenditures on the field (Abaimov and Martellini 2020, 161-165). Whereas Horowitz links the issue of autonomous decision-making to the emerging arms race, arguing that a state, which is more insecure about its own conventional and second-strike nuclear capabilities might be more encouraged to automate nuclear early-warning systems and delivery platforms, hence increasing the chances of inadvertent escalation (Horowitz 2019, 93).

In sum, while there are other areas where AI will be relevant in military affairs, the rapidly expanding AI literature is mainly centered on the observations on military decision-making processes; the enhancement of military capabilities; and the global arms race. The following chapters will aim to answer how might these AI-related changes impact NATO member states' capabilities and strategic thinking?

Artificial intelligence in NATO

The 2010 Lisbon Strategic Concept *Active Engagement, Modern Defense* defines three core tasks for NATO: collective defense, crisis management and cooperative security. Each of these require the alliance to maintain its credibility and its competitive technological edge in military affairs. The publicly released summary of the NATO 2021 Artificial Intelligence Strategy points out that AI is “changing the global defense and security environment” and “will affect the full spectrum of activities undertaken by the Alliance.” (NATO 2021) The NATO AI strategy has four main aims, which include encouraging the development and use of AI in a responsible manner; accelerating AI adoption in capability development and delivery; protecting and monitoring AI technologies and ability to innovate; and identifying and safeguarding against the threats from malicious use of AI. (NATO 2021) As such, NATO aims to “integrate AI in an interoperable way to support its three core tasks.” (NATO 2021) Though the incorporation of AI enabled technologies into member states' strategic thinking and military capabilities is necessary if NATO aims to fulfil the alliance's core tasks, the state of play concerning military AI on member states' level shows several shortcomings.

AI-enabled programmes in NATO member states

So far, the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) 2021 report provides the most comprehensive survey of AI-enabled systems in NATO member states' armed forces. It identifies a capability gap and fragmentation within the alliance due to the differentiated implementation of and access to AI-enabled technologies (Gray and Ertan

2021, 6). The report also points out that AI-related NATO-wide collaborative projects remain limited and highlights four main reasons behind this tendency (Gray and Ertan 2021, 17-18). First, diverging views on military AI within the alliance makes collaborations with only a few preferred partners easier. Second, bilateral tensions can limit the sharing of information and technology even among allies. Third, several countries lack the necessary resources and capabilities for any meaningful contribution, which might push capable partners towards non-NATO collaborations. Fourth, public opposition in various countries towards AI-enabled military technologies hinders a number of NATO countries to move forward on the field.

The CCDCOE identifies altogether 84 different AI-enabled programmes within 25 member states. These include already existing and operating military capabilities (e.g. F-35 Next Generation Aircraft; Mistral 2 missile; RQ-11 Raven UAV etc.) but also capabilities that are in their development phase (e.g. Future Combat Air System). Each system is put into one of the four categories (Autonomous Vehicles; Autonomous Air and Missile Defense Systems, Autonomous Missiles, and AI-Enabled Aircraft; Data Analytics; Logistics and Personnel Management) and for each of them the CCDCOE lists the developer and the operator countries as well. While these are valuable primary insights concerning the spread of AI-enabled systems within the alliance, the data provided by the report invites further analysis.

Interrogating this data further and cross-referencing AI-enabled capabilities with specific operator countries helps to demonstrate several intra-alliance dynamics. Figure 1. shows the number of AI-enabled programmes in each member state based on the CCDCOE report. This highlights an emerging capability gap within the alliance, in which 9 member states are operating at least 10 AI-enabled programmes, while 14 member states are operating less than 5. These 14 countries include Iceland, Luxemburg and 12 member states that have joined the alliance after the end of the Cold War, which points towards a major East-West imbalance.

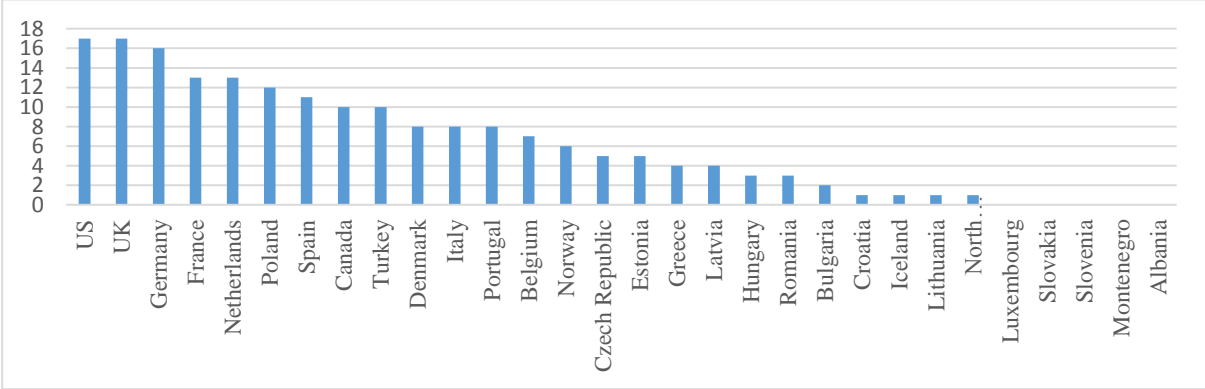


Figure no 1. The number of AI-enabled programmes by member states. The analysis was conducted by the author based on the data published by (Gray and Ertan 2021, 24-29)
The figure was prepared by the author.

Even though the US and Western/Southern Europe are incorporating AI-enabled systems more quickly into their armed forces, the use of different programmes show an extremely fragmented distribution. 61% of all AI-enabled programmes within the alliance are used by only 1 member state, and 26% by 2-4 member states. Only 12% of all programmes have at least 5 operators, and only the RQ-11 Raven is employed by more than 10 member states. (Table 1.) The level of collaboration is limited or simply non-existent when it comes to the use of AI-enabled systems. This leads to the emergence of parallel capability structures, thus limiting the prospects of future interoperability.

Table no 1. The number of operator countries for each AI-enabled programmes in NATO.
The analysis was conducted by the author based on the data published by
(Gray and Ertan 2021, 24-29).

| Number of operator countries | Programmes |
|------------------------------|---|
| More than 10 member states | 1 program (RQ-11 Raven) |
| 5-10 member states | 9 programmes (Harpoon Block II; F-35; ScanEagle; Patriot; Gavia; Puma 3; Remus 100; THEMIS; MU90 Impact) |
| 2-4 member states | 22 programmes (AMRAAM, nEUROn; Skeldar V-200; Aegis; CRAI; Duble Eagle Sarov; FCAS; Iver; Phalanx; Sabuvis; SAMP/T; SWORD; A-18M; A27-M; Barracuda; BlueScan; Goalkeeper; Mistral 2; Naval Strike Missile; SeaRAM; Skylar I-LEX; Tempest) |
| 1 member state | 52 programmes (A9-M; ADATS; AKINCI; Albatros-K; Alpagu; Anka S; AR-4; ARCHANGE; Automatic Imaging Target Acquisition; AWISS; B-Hunter; Boatswain's Mate; Brimstone; C-DAEM; Dardo; F4 Rafale Predictive Maintenance; Harop; HUGIN; Husky; Joint Strike Missile; Kalaetron Attack; Kargu; LIMS IV; Luna; Manta; MANTIS; Mast-13; Mast-9; Mission Master; Mixed Reality Remote Assistant Support System; MQ-9 Reaper; NASAM; Nerva; Perun; Project Maven; Pulat; RQ-4 Global Hawk; SeaCon; SeaHunter; Soprene Project; Spyder; SWIM; Swordfish; Talios; Taranis; TB2; TF-X; TOGAN; Viking 6x6; Warmate; Watchkeeper) |

The table was prepared by the author.

Although bigger and more capable member states tend to use more AI-enabled programmes, several of these programmes are only used by 1 member state within the whole alliance. For example, Turkey has 10 different programmes but 9 of these are only used by Turkey (Figure 2.). The situation is similar, although less dramatic in the case of France (5 out of 13 programmes used by only France), Germany (6 out of 16 used by only Germany), the UK (7 out of 17 used by only the UK) and the US (6 out of 17 used by only the US).

Table no 2. The number of AI-enabled programmes that are only used by 1 member state.
The analysis was conducted by the author based on the data published by
(Gray and Ertan 2021, 24-29).

| Member State | Number of programmes used by only this member state | Programmes |
|--------------|---|---|
| Turkey | 9 | Kargu; Anka-S; Pulat; TB2; Albatros-K; AKINCI; TF-X; TOGAN; Alpagu |
| UK | 7 | Watchkeeper; MAST-13; Taranis; Viking 6x6; Brimstone; MAST-9; Manta |
| Germany | 6 | Harop; SWIM; Kalaetron Attack; AWISS; Luna; Mantis |
| US | 6 | C-DAEM; SeaHunter; Project Maven; LIMS IV; Project Salus; MQ-9 Reaper |
| France | 5 | Talios; F4 Rafale Predictive Maintenance; ARCHANGE; Nerva; Automatic Imaging Target Acquisition |
| Canada | 3 | Mixed Reality Remote Assistant Support System; Boatswain's Mate; ADATS |
| Portugal | 3 | SeaCon; AR-4; Swordfish |

| Member State | Number of programmes used by only this member state | Programmes |
|----------------|---|-----------------------|
| Poland | 2 | Warmate; Perun |
| Latvia | 2 | A9-M; Husky |
| Netherlands | 2 | HUGIN; Mission Master |
| Lithuania | 1 | NASAM |
| Italy | 1 | Dardo |
| Norway | 1 | Joint Strike Missile |
| Czech Republic | 1 | Spider |
| Belgium | 1 | B-Hunter |
| Estonia | 1 | RQ-4 Global Hawk |
| Spain | 1 | Soprene Project |

The table was prepared by the author.

Therefore, the level of interoperability and the number of AI-enabled systems used by multiple member states remain limited. Figure 2 demonstrates intra-alliance network established by these capabilities. Arrows symbolize the AI-enabled programmes that are used by both countries. The thicker the arrow the higher the number of these systems. The level of interoperability is the highest between the UK and the US (6 programmes used by both countries). The connections around the center are stronger with having multiple systems used by several countries. Although member states with a higher number of AI-enabled programmes naturally tend to gravitate closer towards the center, this is not a necessity. For example, countries with only a moderate level of AI-enabled capabilities (e.g. Denmark or Belgium) have stronger intra-alliance relations than countries with more capabilities (e.g. Turkey or France). Meanwhile, connections between these countries and the periphery remain weak and are even weaker within the periphery (see the external circle on Figure 2).

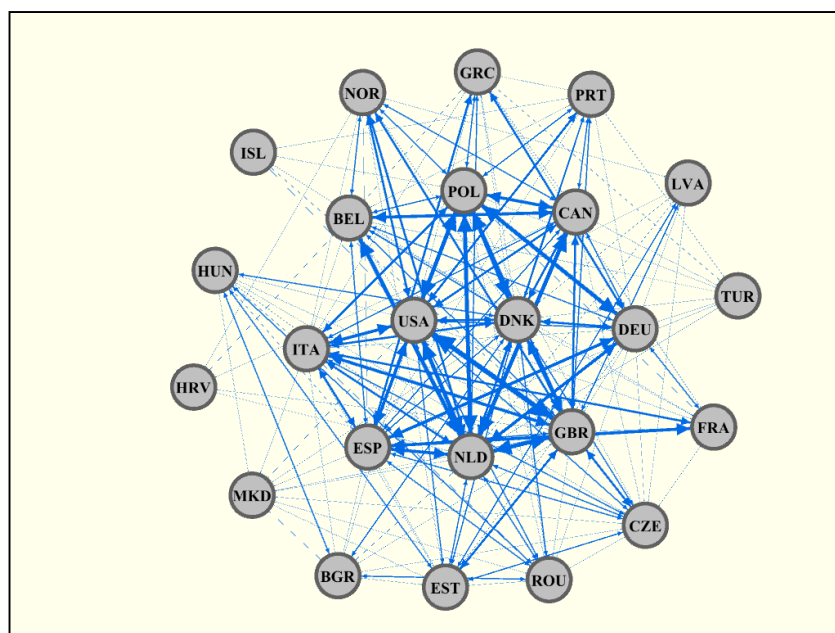


Figure no 2. The intra-alliance network of AI-enabled capability connections. The analysis was conducted by the author based on the data published by (Gray and Ertan 2021, 24-29). Countries with 0 connection are not represented

The figure was prepared by the author.

This becomes even more striking when we focus our attention on those strong connections that are featuring at least four programmes used by both countries (Figure 3.). Only 11 member states have any connections in this category and even their network is fragmented. The US, Poland and the Netherlands maintain the most diverse and interoperable network with each of them featuring 5 strong connections. Spain and the UK equally have 4 strong connections, while Germany and Canada have 3, Denmark, Belgium, Italy have 2 and France has only 1. This is especially a notable achievement in the case of middle-powers including Poland and the Netherlands, but also Canada Denmark and Belgium, whose military capabilities are relatively limited compared to the European great powers. Their level of interoperability with regards to AI-enabled programmes tend to outperform the traditionally biggest European military spenders like Germany, the UK, France, Italy, Turkey or Spain that have weaker intra-alliance connections. Once again, this is especially notable in the case of France and Turkey whose level of interoperability falls short of their relatively high number of AI-enabled programmes.

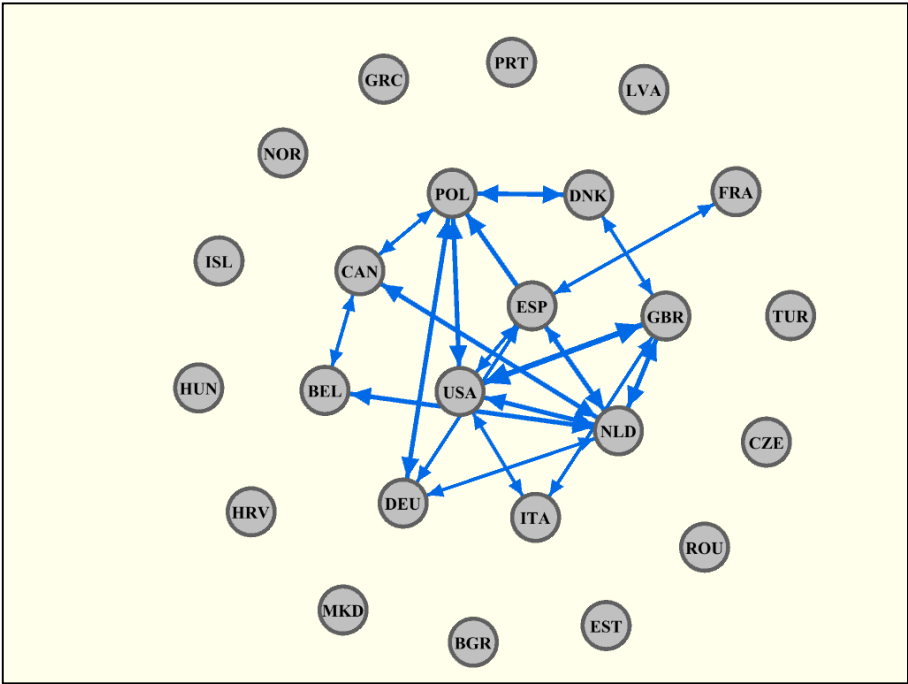


Figure no 3. The *strong* intra-alliance connections of AI-enabled capabilities (at least four programmes used by both countries). The analysis was conducted by the author based on the data published by (Gray and Ertan 2021, 24-29)
The figure was prepared by the author.

Defense AI strategies in NATO

How NATO member states’ strategic thinking converge and diverge around AI? Although NATO prepared its own Artificial Intelligence strategy, and AI-related programmes are emerging within the alliance’s armed forces, defense and military AI strategic documents on member states level are lagging far behind this process. Several NATO members refer to the role of AI and/or emerging and disruptive technologies in their national security/defense strategies, albeit these are usually lacking any details concerning their impact on strategic affairs. Similarly, the already published country-specific, general AI strategies tend to avoid the field of security and defense, making it even more difficult to deduce any meaningful conclusion with regards to the strategic thinking of member states (Gray and Ertan 2021, 17).

The two major exceptions are so far the United States and France, which have prepared their own AI defense strategy in 2018 and in 2019 respectively. The documents are different in their style and characteristics, which makes their comparison methodologically difficult, however, they can still provide an important point of reference, when analyzing the strategic thinking and directions of these countries. Reading the documents of France and the United States in parallel, key differences become apparent concerning their strategic thinking on AI, showing patterns of divergence within the alliance. The areas where these differences are present, include the transformation of the strategic environment; the newly emerging threats; as well as objectives and capabilities. (Table 3).

Table no 3. The comparison of the United States’ and France’s defence AI strategies

| | United States | France |
|-----------------------------|--|---|
| Document | Summary of the 2018 Department of Defense Artificial Intelligence Strategy | Artificial Intelligence in Support of Defense |
| Year | 2018 | 2019 |
| Strategic Environment | Comprehensive AI-related transformation, impacts every corner of the DoD, catalysing power competition across the globe. | Pivotal moment is yet to come, AI is still limited. Differentiating between AI superpowers (US and China); aspiring intermediate powers (EU); and a second circle of countries (e.g. France). |
| Threats | Chinese and Russian investments in AI are eroding the technological advantage and destabilizing the global status quo. | Three major categories: 1) Threats posed by adverse AI (e.g. predicting modes of action). 2) Emerging global arms race creates new threats by state and non-state actors. 3) Threats posed by the use of AI (e.g. technology dependence). |
| Objectives and Capabilities | Protecting US service members and civilians, citizens and critical infrastructures. Reducing organizational inefficiencies, scaling AI with partners. Priority areas include situation-awareness and decision making; increasing safety; predictive maintenance; and the use of AI technologies for highly manual, repetitive tasks. | Keep freedom of action and interoperability with allies; the assurance of trustworthy, controlled, and responsible AI; the resilience and upgradability of systems; preserve sovereignty concerning AI technologies. Priority areas include decision and planning support; collaborative combat; logistics; intelligence; robotics and autonomy; and the use of AI in support services. |

The table was prepared by the author.

Strategic environment

Both countries tend to emphasize that the emergence of AI brings forth global competition and fundamental technological shifts. The US expects that AI-related transformation will “impact every corner” of the DoD (Department of Defense 2018, 5). This not only means technological or organizational changes but also that the very “character of the future battlefield” will undergo such a transformation, making the harnessing of AI a necessity (Department of Defense 2018, 4). Thus, the strategic environment is a pivotal moment that catalyzes power competition and provides an opportunity for adversaries of the US, to disrupt the country’s military-technological edge. France, however, tends to argue that this pivotal moment is not yet around the corner, since in the current state of affairs, AI applications remain limited and defense AI technologies still require fundamental progress,

before they “can be used in a controlled way” (Ministère des Armées 2019, 4). For France, the application of AI in the military aims foremost at maintaining operational superiority, or a mean (and not an end) to “continue to perform their missions” (Ministère des Armées 2019, 3). Whereas the US specifically names its adversaries (China and Russia), the French perspective provides a more elaborate world view: differentiating between AI superpowers (US and China); aspiring intermediate powers (EU); and a second circle of countries (France, Germany, UK, Japan, South Korea, Singapore, Israel and Canada), noting that the latter group’s autonomy depends on their cooperation and their niche strategies (Ministère des Armées 2019, 7). It is interesting though that France does not mention the role of Russia on the field, which creates a significantly different strategic assessment compared to the United States’ analysis.

Emerging threats

The US is also more explicit in its strategy concerning the perceived threats caused by Chinese and Russian AI-related technologies, emphasizing that the two’s investments in the field raise various questions regarding international norms and human rights (Department of Defense 2018, 5). From the US perspective these investments generate a destabilizing effect, while threatening to erode technological and operational advantage. As such, the US primarily links the issue of AI and defense to the maintenance of the global status quo, in which Washington’s advantage can be disrupted by rapid technological developments. Thus, the strategy puts the emphasis on the quickest possible adaptation of AI technologies to counter these efforts (Department of Defense 2018, 5).

France sees four areas of particular concerns on this field, including the possibility that adverse AI will predict modes of action; the paralysis of command capabilities as a result of the neutralization, deception or diversion; influence operations; and proliferation of high frequency hostile actions in the cyber sphere (Ministère des Armées 2019, 6). Apart from these, the French strategy reflects to a resuming arms race on the field. Although, France follows a more cautious policy than the US and does not link threats directly to China or Russia, the strategy still notes that the spread of AI will lead to an emerging arms race, in which several countries might try to alter the “established hierarchy of military power” (Ministère des Armées 2019, 6). This arms race also provides more room for non-state actors to achieve strategic objectives, while the technological changes also create new imbalances and encourage escalation, due to the fear of being on the wrong side of technological surprise; the advantage of pre-emptive use; and the rapidity of technological progress, that reduces time for political cooperation (Ministère des Armées 2019, 7). In contrast to the US, France also highlights threats posed by the use of AI, including the deception of human perception; risks arising from AI learning techniques; and technology dependence (and the potential loss of human skills) (Ministère des Armées 2019, 7).

Objectives and capabilities

The US and France are all interested in maintaining the global status quo, and the primary underlying objective behind their strategies is to invest into their AI capabilities as much as needed to maintain their perceived technological edge. This investment tackles a wide range of action in both cases, including not only the investment into technological development projects but also into workforce, civilian sector, companies, academia and allies as well.

Besides this underlying principle, the US DoD follows four broadly defined goals: it aims to protect US service members and civilians affected by military operations, through the reduction of risks and increase of precision; it aims to use AI to protect US citizens and critical infrastructures through enhanced prediction and identification of threats; it wants to

significantly reduce organizational inefficiencies; while it aims to become a pioneer in scaling AI with interagency, allied and coalition partners (Department of Defense 2018, 6). The strategy also provides a few examples, where the emphasis will be put in capability development projects (Department of Defense 2018, 11). These are not concretely defined projects but rather priority areas, in which AI-related technologies can play a major role, including situation-awareness and decision making (e.g. imagery analysis or exploration of new courses of action); increasing safety of operating equipment (e.g. in complex and rapidly changing situations); predictive maintenance and supply (e.g. predicting failure, automating diagnostics, data-driven maintenance and optimizing inventory levels); and the use of AI technologies for highly manual, repetitive and frequent tasks (to optimize DoD resources to higher-value activities).

Similarly, the French strategy builds on four major guidelines for a controlled defense AI. First, to keep freedom of action and interoperability with allies, which reflects on the capacity to counter adversary AI, but also on the increasing capability gap within the alliance that makes maintaining interoperability standards more difficult (Ministère des Armées 2019, 9). Second, the assurance of trustworthy, controlled and responsible AI, referring to the use of secure, transparent and human controlled systems in the military (Ministère des Armées 2019, 9). Third, the resilience and upgradability of systems, emphasizing the long term upgradability of systems, but also preserving the knowledge to conduct operations with AI systems in a degraded mode (Ministère des Armées 2019, 9). And fourth, the French strategy consequently emphasizes the notion of sovereignty concerning AI technologies, especially in the case of the military and the need to maintain a French controlled core of technologies to avoid dependence on foreign countries – including allied countries, like the United States (Ministère des Armées 2019, 9). In this context, France identifies seven priorities for AI-related capability development, and compared to its US counterpart, these are more concretely defined areas (Ministère des Armées 2019, 14-17): Decision and planning support (e.g.: synchronized detection of the tactical situation); Collaborative combat (e.g. management of radiofrequencies in coalition); Cyber security (e.g.: cyber-attack detection); Logistics and operational readiness (e.g.: predictive alerts, differentiated maintenance cycle); Intelligence (e.g. smart data mining); Robotics and autonomy (e.g.: multi-robot cooperation, drone swarms, automatically coordinated mobile robots, sentry robots); AI in support services (e.g.: decision support; automation of repetitive tasks, connected sensors; augmented agents or users; new recruitment methods).

Implications for intra-alliance dynamics

How might these capability and strategic fragmentations influence intra-alliance dynamics within NATO? Recently published works highlighted several challenges caused by the rapid spread of AI-enabled technologies across the alliance. For instance, Lin-Greenberg identifies the following obstacles on the operational level (Lin-Greenberg 2020, 62-67): new burden-sharing problems, due to the different capabilities among member states, creating new divisions between those countries that have and that have not significant AI capabilities; data sharing and standardization problems among allies; and vulnerability issues concerning the application of AI, making it more exploitable for adversary manipulation. Besides, the use of AI in alliances might hamper allied decision-making because it is compressing the timeline of decision-making processes on both political and military levels, and because of the uncertainty associated with AI technologies across the alliance, which again creates diverging national perceptions and policies concerning the use of AI (Lin-Greenberg 2020, 68-70).

Indeed, the analysis above demonstrates that many of these obstacles are already present in NATO. Capability gaps were always visible in the alliance (Fiott 2017, 418-423)

but the use of AI-enabled military technologies might easily lead to the emergence of a new form of capability gap. At this point, the integration of AI-enabled systems into allied military forces shows not only striking disparities but a deep level of fragmentation. This creates a broad variety of different capabilities, which however are employed by only a small number of countries. Hence, the AI-enabled capability gap creates a new division of intra-alliance labor as well. Evidently, countries with more programmes will become more capable for future modes of warfare, while others with less resources will have only limited capabilities to contribute to allied operations.

But today, it is no longer only about having or not having various advanced capabilities as it was often the case in the past. Of course, this remains and will remain a significant factor in the alliance, since there will be always member states, which have more resources and are militarily more capable than others. However, the current state of affairs is not solely influenced by the question of resources, and gaps are emerging among those members of the alliance, which have more capabilities.

This poses several questions for the future of NATO. On the one hand, the spread of different AI-enabled programmes creates future interoperability problems for future allied operations. On the other hand, their implications also weaken the internal cohesion among member states, since the most AI-capable member states are becoming each other's competitors. This has industrial and political motives as well, since member states, which are capable to develop their own capabilities tend to be reluctant to procure AI-enabled technologies from other sources. Besides, many of them are also cautious to share their most sensitive technological innovations, due to the broadly varying level of trust among member states. Hence, policies pursued by AI great powers are deepening intra-alliance fragmentations, while AI middle powers, like Poland or the Netherlands, are more likely to procure AI-enabled technologies from other member states. In the long run, they might become even more interoperable with other allies than AI great powers like the US, the UK, Germany, France or Turkey. Of course, the use of different systems requires different training, logistics and doctrines, which in the long run can lead to longstanding organizational impacts as well, hence generating a cascading effect and further widening the gaps among allies. Moreover, as the examples of France and the United States demonstrate, these differences are already transforming into diverging strategic paths among these two AI great powers. These differences are affecting their basic assessments on the strategic environment, threats as well as objectives and capabilities. Although NATO member states are still in the early process of adjusting their strategic thinking to the emerging technological developments, these early strategic divergences show that the spread of AI-enabled systems will pose new and unforeseen challenges for the alliance on various levels.

Conclusions

This article sought to answer how the spread of AI-enabled technologies across the full spectrum of the militaries transforms NATO member states' strategic thinking. The article argued that the spread of AI-enabled technologies will enhance already existing strategic divergences within NATO, while creating new forms of capability gaps among member states.

For this purpose, the article highlighted the transformative impact of AI-enabled technologies on armed forces based on the rapidly spreading AI military literature. After that, the article focused on the empirical level to highlight intra-alliance capability and strategic fragmentations. It analyzed the member state-specific data of NATO CCDCOE and cross referenced it with operators and analyzed France's and the United States' AI defense strategies with regards to their assessments on the strategic environment; emerging threats; as

well as objectives and capabilities. Based on these results, the article also discussed how these capability and strategic fragmentations might affect intra-alliance dynamics, while creating new forms of interoperability problems and fragmentations among member states. The analysis demonstrated that NATO is facing an emerging gap not just between those who have and have not AI-enabled capabilities but also among member states with more AI-enabled systems. In this process, AI-capable great powers are becoming each other's competitors, while AI middle powers are more likely to become more interoperable with other allies. Differences among AI great powers are also appearing on the strategic level, as the assessment of France's and the United States' AI defense strategies highlight diverging strategic paths in several respects between these two influential member states.

It is important to note that the integration of AI-enabled systems into NATO member states' militaries is still in its early phase, although this process will rapidly accelerate during the next decade as AI will spread more quickly across the technology spectrum. Therefore, the fact that NATO is showing the signs of significant capability and strategic fragmentations already in this early stage is posing a serious risk for the future interoperability among member states and the internal cohesion of the alliance in the long run.

Bibliography

- Abaimov, Stanislav, and Maurizio Martellini. 2020. "Artificial Intelligence in Autonomous Weapon Systems." In *21st Centruy Prometheus – Managing CBRN Safety and Security Affected by Cutting-Edge Technologies*, by Maurizio Martellini and Ralf Trapp, 141-178. Cham: Springer.
- Boulanin, Vincent. 2016. *Mapping the Development of Autonomy in Weapon Systems – A Primer on Autonomy*. Stockholm: Stockholm International Peace Research Institute.
- Boulanin, Vincent. 2019. „The future of machine learning and autonomy in nuclear weapon systems.” In *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk – Volume I.*, szerző: Vincent (ed.) Boulanin, 53-63. Stockholm: Stockholm International Peace Research Institute.
- Department of Defense. 2018. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*.
- Ekelhof, Merel A. C. 2018. „Lifting the Fog of Targeting: "Autonomous Weapons" and Human Control through the Lens of Military Targeting.” *Naval War College Review* 71(3) 61-94.
- Fiott, Daniel. 2017. „A Revolution Too Far? US Defence Innovation, Europe and NATO's Military-Technological Gap.” *Journal of Strategic Studies* 40(3) 417-437.
- Gray, Maggie, and Amy Ertan. 2021. *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence.
- Horowitz, Michael C. 2019. „Artificial intelligence and nuclear stability.” In *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk – Volume I.*, szerző: Vincent Boulanin, 91-98. Stockholm: Stockholm International Peace Research Institute.
- Johnson, James S. 2020. „Artificial Intelligence: A Threat to Strategic Stability.” *Strategic Studies Quarterly* 14(1) 16-39.
- Lin-Greenberg, Erik. 2020. „Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making.” *Texas National Security Review* 3(2) 56-76.
- Ministère des Armées. 2019. *Artificial Intelligence in Support of Defence - Report of the AI Task Force*.

- NATO. *Summary of the NATO Artificial Intelligence Strategy*. 2021. 10 21. https://www.nato.int/cps/en/natohq/official_texts_187617.htm (hozzáférés dátuma: 2022. 05 10).
- Verbruggen, Maaïke. 2020. „The extensive role of artificial intelligence in military transformation.” In *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk - Volume III.*, szerző: Petr (ed.) Topychkanov, 11-16. Stockholm: Stockholm International Peace Research Institute.
- Wong, Yuna Huh, et al. 2020. *Deterrence in the Age of Thinking Machines*. Santa Monica: Rand Corporation.

* SUPPORTED BY THE ÚNKP-21-4-I-NKE-19 NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY FOR INNOVATION AND TECHNOLOGY FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND.