No. 251, October 2019, Editor: Fabien Merz

AI in Military Enabling Applications

The public debate over military use of artificial intelligence (AI) mainly revolves around autonomous weapons systems. Looking beyond the specific ethical and political considerations associated with that issue, there are important questions relating to the organizational, technical, and functional integration of AI-enabled systems that determine the balance between potential benefits and risks.

By Niklas Masuhr

In the summer of 2017, Russian President Vladimir Putin argued that the nation that had a leading edge in the sphere of artificial intelligence (AI) would be able to "rule the world". This statement, like other similarly worded contributions to public debates, suggested a unitary technology with revolutionary impact, similar to the atom bomb. The reality, however, is much more complex. Apt analogies would be the introduction of electric power or the rise of the internet – technical achievements that have influenced all spheres of human life in manifold and often contradictory ways.

Joint Operations Command Center in Qatar during the invasion of Iraq in March 2003. Advanced software and AI can massively reduce the personnel numbers of such staff units. *Tim Aubry / Reuters*

Probably the best-known subcategory of AI is *machine learning*. Technical breakthroughs in computing power, especially in terms of processors and video cards, have facilitated rapid progress in this field. Examples of civilian applications based on these developments include automatic image recognition, and natural language processing, as well as artificial "players" of board or computer games. In principle, these programs require multiple components. Machine learning-enabled software must first be trained by experts using – preferably large – datasets. As a civilian example, in order to identify road users, camera images are used as training data. This enables algorithms to generate predictions independently in relation to as-yet unknown data and, ideally, to autonomously improve their own performance over time. Already today, some of these software algorithms are capable of surpassing human talent in their respective areas.

Nevertheless, it is important to note that existing machine learning applications have so far only been able to improve their capabilities in a relatively narrow field, that is, they become more efficient at solving existing tasks rather than tapping into new tasks on their own. This potential for simplifying processes and making them more efficient is what makes AI a key priority for armed forces and intelligence services – which is particularly viewed with skepticism in democratic, liberal societies. Most public debate is focused on advances in the autonomization of weapons platforms in the air, on land and on and under the sea that can attack targets independently. It should be pointed out, however, that advances in machine learning methods are

not sufficient on their own; rather, the future of autonomous weapons systems will also depend on developments in other areas such as sensors and robotics.

Moreover, the impact of AI developments is felt across a broad range of routine operations within armed forces, amongst which the use of autonomous weapons systems is only one of many elements. Accordingly, this analysis will focus on certain aspects of military use of AI that have hitherto received less public attention, specifically those where machine learning methods will play a role – or are already playing a role today. In the following, we will look at a cross-section of issues that illustrate the complexity and diversity of the range of topics involved. To this end, the analysis will first focus on potential outcomes at the level of strategic decisionmaking. Subsequently, it will consider the possible implications of machine learning for the training and organization of armed forces. Finally, it will point out some inferences at the level of military operations.

Strategic Decisionmaking

AI has the potential to support analysis by actors ranging from top-level political decision-makers all the way down to infantry soldiers in the field. This section will focus on the former sphere, i.e., the political-strategic 'brain' of a national security architecture. Here, AI-enabled systems could, for example, predict the behavior of foreign states and societies, predefine policy options, or generate highly complex simulations relating to ongoing crises in real time. The core advantage of machine learning in this context is that it facilitates greater precision and can complement human assessments and predictions, which may always be clouded by emotions and biases. Moreover, in principle it can vastly accelerate decisionmaking processes by enabling governments to understand and analyze situations much quicker than before.

AI has the potential to support analysis by actors ranging from top-level political decision-makers all the way down to infantry soldiers.

At the same time, even machine learning cannot guarantee the absence of biases or analytical errors. Such issues have already manifested themselves in the civilian sector, since the heuristic framework demarcated in the "training phase" can, for example, distort the gathering and categorization of data that ultimately enables AI to carry out autonomous analyses. Thus, it has become apparent that the reliability of facial recognition software varies depending on the target's ethnicity. In the intelligence and military spheres, such issues could have grave consequences if immature systems are deployed and trusted. If we consider the use of AI for decisionmaking in connection with a "Cuban Missile Crisis"-type scenario, the problems associated with use of these new technologies become apparent. Even assuming that it is possible to calculate options for action and potential crisis scenarios with a high degree of precision, the possibility remains that the acceleration of decisionmaking may contribute to the escalation, rather than the de-escalation, of such a crisis, since the actors would see their respective windows of opportunity shrinking.

An already complex situation would become even more critical as soon as multiple states or actors have proprietary intelligent support programs at their disposal. For one, multiple AI systems that have been trained in different ways might come to contrary conclusions. It would thus be wrong to think that they could generate outcomes based on perfect rationality. Moreover, even high-performance algorithms are not immune to being misled by fairly traditional means of espionage and deception. For instance, it is conceivable that AI might mistakenly assess certain patterns of behavior as innocuous if they occur often enough without entailing the feared outcomes – even assuming that the data base can become much more finely granulated than has hitherto been the case. Of course, such issues are especially concerning if AI-enabled analyses are given a great deal of credence or if it is impossible to verify the validity of their recommendations.

This is precisely where a potentially major problem becomes apparent: AI-generated analyses and inferences could gain an oversized degree of authority in political decisions. In essence, it is difficult to judge from an external viewpoint how precise or trustworthy an AI-generated assessment really is. Though it is true that similar problems also arise where no intelligent software is used, there is a real chance that the technology may be used as an exclusive "oracle" in public debate by governments or corporations. The question of who exactly has access to AI, and thus, who is in a position to contextualize and interpret its results, is therefore of utmost importance for society at large. In democracies, civil-military tensions may be exacerbated if, for example, the armed forces have sole access to analytical AI that recommends certain military options for action, based on simulations. But even within a security apparatus as such, access to AI systems and the implications for actors' authority may be problematic, depending on how and where the AI is embedded in existing institutional decisionmaking processes and hierarchies. It is conceivable, for example, that different ministries or military commands may be provided with divergent results and recommendations. The situation is further aggravated by the fact that more complex AI, in particular, may be capable of predicting or at least predefining scenarios, without the underlying logic, considerations, and prioritizations necessarily being comprehensible. Such issues, from the dangers of immature AI to the power relations within and between governments and societies, illustrate the importance of first embedding AI in a political and institutional context to minimize serious risks. Thus, certain safeguard mechanisms are required at the strategic decisionmaking level.

Training and Organization

The problems described above at the level of strategic decisionmaking are similarly applicable to the organization and training of armed forces themselves. One of the most interesting aspects of machine learning in this context relates to the education, training, and selection of military enlisted and officer personnel. Much like in the civilian sphere, AI can be used here to create and continuously update personalized curricula. For instance, depending on the student's learning style, it could decide to explain a concept in terms of mathematical formulae, visualizations, or sports analogies. Within military structures, AI could ensure that promotions and postings are carried out more objectively, based on an improved ability to assess candidates in a holistic manner.

Another advantage is seen in the potential ability to design virtual or real-life exercises in a more realistic or challenging manner, allowing commanders and staff officers to prepare better for combat operations – in particular with a view to engaging with "enemies" who are capable of thinking dynamically. By using intelligent algorithms either to "play" the roles of adversaries and

populations or to conduct more finely grained analyses, new operational concepts and tactics could be developed independently of personal and institutional experience. Moreover, through highly complex simulations, AI can help to predict the best ways to use new technologies and integrate them into existing systems. Especially in combination with advances in virtual reality (VR), complex algorithms are expected to considerably improve the realism of tactical training. In addition to AI's huge potential for military education and training, it should not be forgotten that even with "intelligent" syllabi and assessments, the heuristic framework is in the first instance defined by human programmers and analysts. Therefore, a lack of objectivity in terms of military or personal criteria will potentially be reflected in algorithms. The same applies to the value of intelligent simulations, maneuvers, and wargames: Their results may not replicate the realities of a certain theater of operations or scenario – or they may be given inordinate degrees of credence.

Advantages and Disadvantages of AI in the Military Field

	Benefits and Potential Advantages	Disadvantages and Risks
Strategic Decisionmaking	- More precise, faster situation assessments and analyses - Offsetting emotions and prejudices - Rational behavior in crisis situations	- Low crisis stability due to acceleration of decisions - Prejudices can be inherent in algorithms - Problems regarding the balance of power within states, for example between the military and the civilian leadership.
Training and Organization of Armed Forces	- Personalized training, fair assessments and promotions - More realistic exercises, maneuvers and simulations - Credible simulations of future technologies and their applications	- Overestimation of AI-generated results - Cultural and personnel problems due to incompatibility between military culture and values held by specialized personnel - Military cast system due to higher technical specialization
Military Operations	- More efficient processing of data from different sources - Reduction of administrative and staff work through forward-looking logistics - Reduced risks for troops through autonomous logistics - Improvement of support and reconnaissance systems	- Potential dependencies that cannot be replaced in the field - Risks in supply chains due to lack of inventories and reserves - Unclear whether autonomous vehicles can be used in complex scenarios - Reduction of strategic stability

Other issues arising in connection with training and education relate to the changing nature of military careers and professional pathways as a result of increasing use of – and thus dependence on – artificial intelligence. Armed forces are already confronted with cultural issues in the context of cyberspace, since they are compelled to recruit people whose interests and qualifications do not necessarily match the traditional self-perception or external image of the military. It is likely that similar problems will occur in the context of militarily harnessing AI. Specifically, the question arises whether AI specialists serving in military headquarters should even be required to undergo basic infantry training and to which extent military standards of physical fitness should apply to such recruits. This debate is already underway in the US, polemically reduced to the shorthand notion of "blue-haired soldiers". As part of these 'lateral entry' schemes, expert civilians are inducted into the forces and ranked from the start as officers or non-commissioned officers, which is viewed as problematic within the Army and Marine Corps in particular. Nevertheless, it is unclear how armed forces will be able to compete with multinational technology corporations for young talent if they continue to insist on basic infantry training and a traditional military organizational culture. The problems in connection with AI described above, especially those relating to the correct interpretation and weighting of the results it generates, can only be offset by hiring personnel with specialized skills. Nevertheless, concerns that lateral hires and varying physical standards based on specializations might create a caste system within the armed forces should not be disregarded.

Military Operations

Generally, the assumption is that AI will support armed forces in collecting, categorizing, and analyzing data more quickly and efficiently than is currently possible. For example, current cooperation between ground and air forces is often hampered by different data processing systems and applications requiring manual harmonization of data. AI-enabled systems can, for example, assist with collecting images or signals collected by drones and categorizing and transmitting them according to the requirements of multiple recipients. Thus, a reconnaissance drone's data could be transmitted in real time to a frontline artillery unit as well as to an HQ intelligence cell without requiring time-consuming "translations" at various interfaces.

Furthermore, intelligent software could also relieve human operators on the ground in terms of essential communications tasks, for instance by automatically switching between radio frequencies to prevent interception or jamming. The question here, though, is how a centralized analytical system whose strength lies in the amalgamation of very diverse information would be able to cope with the failure of individual sensors, i.e., whether such a failure would lead to a complete system crash or potentially fatal diagnostic errors. Other examples of applications in this area include programs to support radar or sonar reconnaissance, which make it easier to detect and localize potential targets. Russia in particular seems to be investing heavily in machine learning to bolster its integrated air defense system. Ultimately, AI could help to significantly degrade the edge of supposedly "invisible" platforms such as nuclear submarines and stealth aircraft. In certain situations, this could negatively impact the strategic stability between the nuclear superpowers.

One area where machine learning and related applications are likely to have a significant impact is in connection with staff work, which has so far accounted for a great deal of personnel resources and time expenditure. Such work involves, for example, planning for patrols or reconnaissance flights, administrative tasks, and logistical organization. Reductions in the sizes of staffs and headquarters are not only based on cost considerations, but also on military

necessity, especially in connection with the resurgence of great power rivalry and its attendant deployment scenarios. Faced with modern sensors and standoff weapons, Western armed forces can no longer rely on expansive bases and installations as they did in Afghanistan. Beyond staff work, the potential of machine learning for military logistics seems especially promising. For instance, the US Air Force has already introduced "predictive logistics" for several fleets of aircraft types, i.e., the intelligent calculation of repair and maintenance tasks. This allows commanders to assign tasks and targeted maintenance intervals to individual aircraft much more efficiently than was hitherto possible. Unsurprisingly, the latest generation of fighter aircraft operated by the US and its allies (especially the F-22 *Raptor* and the F-35 *Lightning II*) are equipped with specific internal sensors and analytical software designed to make full use of these logistical advantages. Of course, as highlighted in particular during the debate over the F-35, there are certain risks involved in excessive dependence on AI applications. As with the concept of "just-in-time" operations in the private sector, such reliance may prove precarious if unforeseen events should imperil the integrity of the supply chain.

Further potential benefits accrue from the automation of transport vehicles. The advantages here are in the areas of efficiency gains as well as force protection. On the one hand, fewer personnel would be needed to transport equipment and supplies over long distances; on the other, soldiers (or private contractors) would be less exposed to ambushes. Especially during the early phase of the occupation of Iraq in 2003, this was a major issue for US forces, despite their massive military superiority and modern technology. The idea of automated resupply doubtlessly has great potential and already seems to be at a fairly advanced stage of development. Thus, the US Army aims to deploy AI-supported trucks by 2020 for operations in convoys in which only the lead vehicle is manned *(Expedient Leader-Follower)*. Nevertheless, the success of such systems depends not only on developments in the field of machine learning, but also on fully developed robotics and sensors. However, once again, this raises the specter of potentially premature introduction of systems and technological dependencies in key military functions or in too complex scenarios. While it is certainly desirable to put fewer personnel in harm's way on convoys through contested territory, one may question, for example, whether and when autonomous vehicles will be able to operate in a conflict scenario within a major city.

AI is best understood as a cluster of enabling technologies that will be applied to most aspects of the military sphere.

AI as an Enabling Technology

The effects of AI and machine learning on the military and the future of warfare cannot be credibly predicted in terms of a few succinct keywords or uniform trends. AI is best understood as a cluster of enabling technologies that will be applied to most aspects of the military sphere. Even if technological progress accelerates, the systems and platforms powered by it will not be absorbed simultaneously or with equal effectiveness and efficiency into the technical arsenal of the armed forces. Neither does it make sense to view AI as an isolated technology, given its manifold interactions with other technological fields, which make consistent and generalized predictions difficult. Accordingly, it is hard to agree with the statement by Russian President Vladimir Putin that mastery of AI implies political hegemony: Alongside the technological component, the organizational and political context must also be taken into account. For instance, the idea that AI will automatically imbue a dysfunctional security apparatus with objectivity and the capacity for rapid decisionmaking is wishful thinking. Moreover, in military operations, dependency on AI must be carefully calibrated. For armed forces in particular, the challenge lies in deciding to what extent and how quickly traditional, historically evolved organizational structures and doctrines should be replaced by new, technology-centric concepts – a challenge for which military-technical history offers no clear answer.

Niklas Masuhr is researcher in the Global Security Team at the Center for Security Studies (CSS) at ETH Zurich. Among other things, he is the author of "Lessons of the War in Ukraine for Western Military Strategy".

CSS Analyses is edited by the Center for Security Studies (CSS) at ETH Zurich. Each month, two analyses are published in German, French, and English. The CSS is a center of competence for Swiss and international security policy.

Editors: Lisa Watanabe, Fabien Merz, Benno Zogg
Layout and graphics: Miriam Dahinden-Ganzoni
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000367663

Feedback and comments: analysen@sipo.gess.ethz.ch
More issues and free online subscription:
www.css.ethz.ch/en/publications/css-analyses-in-security-policy

Most recent issues:

Russia and China: The Potential of Their Partnership No. 250
Kazakhstan: A Centrepiece in China's Belt and Road No. 249
European Strategic Autonomy and the US No. 248
Europe and the Global AI Race No. 247
UN Mediation in Libya: Peace Still a Distant Prospect No. 246
Resilience to Disaster Is No Small Measure No. 245