OFFPRINT FROM *STRATEGIC OUTLOOK 8*

Artificial intelligence – opportunities and challenges for Sweden's national security

Christer Andersson, Tove Gustavi and Maja Karasalo

Artificial intelligence (AI) is expected to have a significant impact on the development of society over the next few years. AI will be applied in a wide variety of technical systems, which means that AI will also influence vital elements of Swedish defence capability and national security in a broad sense. The question is: are the Swedish authorities, and society in general, prepared to make the most of the opportunities offered by this technology and – not least – to face up to the challenges and threats presented by AI in the new security policy landscape?

Artificial intelligence – a contentious concept

Some would say that artificial intelligence (AI) involves making computers imitate human behaviour. Others consider it to be computer systems that, unlike humans, reason and behave 'rationally' in all situations. There is no universally accepted definition of AI, but generally the term refers to the ability of a computer system to reason sensibly or behave correctly on the basis of information available and previous experience.

In purely technical terms, AI is created by processing information using mathematical methods and logic. Thus, AI is not based on a specific technology but may involve for example statistical methods in addition to various types of machine learning. Machine learning can be described as methods that use available information to train mathematical models of their environment. The models are then used to interpret and analyse the environment. The more information available for training, the more precise models and better analysis results can be anticipated.

Attention has been focused on AI in recent years as certain key technologies have reached such levels of maturity and reliability that they can be incorporated into products and used in society. For machine learning in particular, the maturity of the technology is linked to the development of powerful computers, and to the digitalisation of society which has made large volumes of data accessible to the public. These conditions have helped bring about a development of algorithms and methods that was not previously possible.

AI is a field with no clear boundaries between civilian and military applications. Essentially, a technical system developed to identify microscopic cancer cells can also be taught to identify bombing targets in satellite images. As much of the technology is freely accessible, it is difficult to obtain an overview of who is using it and for what purposes. The accessibility and dual use bring both advantages and disadvantages from a national security perspective.

AI opportunities and challenges for total defence

Reporting on practical military use of AI is characterised partly by technology optimism, where various successful applications of AI methods are described; and partly by concern for what the development towards more independent technical systems may involve.

For Sweden's total defence, AI methods may lead to improvements in several respects. For the Armed Forces, AI systems may contribute to military operational and tactical advantages, and for the total defence in general, AI provides an opportunity to streamline administrative tasks by introducing different levels of automation.

FOI Memo 6869
Project Nr I181103
Approved by Mike Winnerstig

October 2019

FOI

AI applications

In today's armed conflicts, conventional military warfare often includes elements of hybrid warfare, such as cyberattacks or propaganda campaigns on social media. Thus, analysis of large volumes of data from various domains is necessary to maintain situation awareness. Given this fact, considerable advantages can be derived from the use of AI. Due to the ability to quickly classify and identify patterns in large data volumes, AI technology is well suited for use in sensor data processing and intelligence analysis.

In military sensor systems, AI enables simultaneous and integrated analysis of different types of sensor data, such as radar signals and sonar data, and supports the ability to draw conclusions at high speed. Data processing results can either help the AI system to take independent action or be used to create decision guidance and recommendations for human decision makers. For instance, in a conflict where large numbers of sensors interact with multiple weapon systems, AI systems can help to supply an updated general overview of rapid developments. In today's combat situations, where the need for rapid decisions are constantly on the increase, the ability to quickly analyse large data volumes may be a crucial survival factor.

In intelligence applications, AI offers an opportunity to identify the unexpected – the so called 'black swan' – by analysing large volumes of traditional intelligence data in combination with open web data. With the amount of data produced today, traditional analysis methods fall short. Processing of data is therefore frequently limited to a known context and a subset of the available data. As a result, the chances of detecting unforeseen incidents are reduced. History has provided us with a number of examples where intelligence efforts have failed to predict forthcoming incidents in time, including the attack on Pearl Harbor and 9/11. AI has the potential to enhance security policy analyses by facilitating detection of both rapid and lengthy sequences of events. With AI, less obvious information or even information that appears to be irrelevant at first glance can be included in the analysis.

AI could become a powerful tool for improving and developing the capability of a range of functions within Sweden's total defence. For the Swedish Armed Forces, AI could offer quality and efficiency enhancements in terms of sensor data analysis and the handling of complex command and intelligence operations. In other parts of the total defence, AI could – for example – be used to detect variations in network traffic that could indicate ongoing cyberattacks on critical infrastructure such as power and water supplies. The scope of potential applications, coupled with the potential for improvement, makes AI technology attractive for financial reasons as well. However, know-how and human resources are needed if the opportunities are to be brought to fruition.

"AI could become a powerful tool for improving and developing the capability of a range of functions within Sweden's total defence. For the Swedish Armed Forces, AI could offer quality and efficiency enhancements in terms of sensor data analysis and the handling of complex command and intelligence operations."

Managing new vulnerabilities

As AI development progresses, there is growing concern in society as to what this technological development entails in terms of reduced transparency and control of autonomous and intelligent systems.

There are plenty of examples of how 'intelligent' systems that usually produce good results sometimes make remarkable errors. One example involves an automated system from Amazon, which had been developed to evaluate job applications. The system had been trained to analyse applications, but after a period of use it was found to discriminate against female applicants. The reason was found to be that there were so few CVs from women in the data used to train the system that greater precision was achieved during training if these applications were rejected. This unwelcome outcome highlights one aspect of machine learning that is important to bear in mind; the behaviour of the system will be governed by the data used to train it. If training data fails to reflect

the desired system behaviour, AI-based systems will occasionally make unexpected and sometimes extremely inappropriate 'errors' which could have serious consequences in security-sensitive contexts.

Besides accidental errors of this kind, there are examples of how AI systems can be manipulated by hostile stakeholders. Studies have shown that with knowledge of how a particular AI method works it is possible to manipulate the method so that the AI system gives incorrect answers. For example, by applying subtle pixel-level alterations to an image – alterations which would be unnoticeable to a human observer – one could cause an AI system to misinterpret the image content completely. Furthermore, it has been demonstrated that image recognition systems designed to identify road signs of various kinds can be manipulated to incorrectly interpret a sign if a certain sticker is applied to it. One important aspect of the vulnerability problem is that a great deal of AI technology is openly available. This means that the latest methods for exploiting vulnerabilities in AI systems may be available also for terrorist organisations and criminal networks.

In the light of examples such as those outlined above, there is an ongoing debate concerning the ethical aspects of AI use. One debated topic is the accountability for decisions made and actions implemented by AI-based systems. A key issue in this regard is how to ensure that AI systems work reliably and intelligibly. AI safety is a growing research field investigating issues such as:

- Transparency – how should intelligent systems be designed in order to make them transparent and interpretable by humans?
- Well defined objectives – how can it be assured that the objective defined for an intelligent system will actually result in the desired system behaviour, with no harmful side effects?
- Robustness and stability if conditions change – how can it be assured that unexpected changes to system conditions (power failures, communication problems, etc.) do not result in serious adverse effects?
- Managing vulnerabilities – how should systems be designed and trained in order to minimise the risk of misjudgements due to deliberate manipulation?

In applications linked to defence and security, it is – quite reasonably – more critical than elsewhere that AI systems work robustly and with no adverse side effects. In many military applications, it is also crucial for systems to be transparent so that decisions that have been made can be tracked and explained. As AI offers major benefits, it must be assumed that the technology will nevertheless be used in both military systems and vital societal functions such as electrical power distribution, healthcare and financial trading. Therefore, knowledge of the vulnerabilities of the technology, and of contingency measures for dealing with potential incidents, are necessary elements of Sweden's total defence.

Premises for Sweden in a changing world

In 2017, Vinnova[1] conducted a study into the development and potential of AI in Swedish industry and society. This study concluded that Swedish AI research currently offers 'limited international competitiveness'. It refers to inadequate investments in AI by companies of all sizes, a lack of government control and a brain drain of AI talent. However, the study emphasises that Sweden has a technology-friendly population, outstanding technical expertise, a well-developed innovation infrastructure, and that the country is at the forefront in terms of IT and digitalisation. Hence, essential prerequisites are in place for Sweden to become a more important AI stakeholder.

One alarming conclusion of the report is that 'other countries are investing more money, faster than Sweden'. In the long term, this kind of development could have major consequences for the competitiveness of Swedish industry; and for national security as well. Countries at the cutting edge of AI development will be able to adopt a position of information superiority, which could alter the security policy landscape. Internationally, China distinguishes itself by making major investments in AI. Countries more on par with Sweden are also investing actively in AI development. Examples of this include France, which in 2018 launched an AI initiative worth more than SEK 15 billion up to 2022; and Finland, which in 2017 became the first EU nation to develop a national AI strategy. In Sweden, the single largest AI initiative is the Wallenberg AI Autonomous Systems

[1] Sweden's government agency for innovation.

and Software Program (WASP), where SEK 1 billion is specifically reserved for AI research. However, WASP is a private initiative funded by the Knut and Alice Wallenberg Foundation. The WASP programme cannot be expected to cater to the interests of the Swedish government, but should rather be viewed as a complement to government initiatives.

The conclusions drawn by Vinnova imply that the Swedish defence sector – both authorities and the defence industry – is in a good position for introducing more AI-based systems. It is worth noting in this context that in combination with other technology, AI could have a significant impact on what has long been one of the major challenges facing the Swedish Armed Forces; namely surveillance of a vast and, in parts, very sparsely populated territory. The extensive coastline in particular presents a challenge from a defence standpoint. Autonomous watercraft and submersibles in combination with intelligent sensor systems could help to improve border surveillance conditions.

Specialist expertise is needed to enable Sweden's total defence to embrace and deploy AI technology. At the same time, the overall knowledge of AI needs to increase within related organisations. AI specialists are greatly in demand on the civilian market, and thereby hard to recruit to the public sector. If maintenance of competence issues are not resolved, it may impede the transfer of AI technology to defence authorities, and the knowledge gap between public and private sector may widen even further.

In addition, both Swedish companies and public authorities are competing on a global market, where large pay gaps between nations can lead to brain drain from nations that cannot offer competitive pay or attractive working conditions. To avoid a future where Sweden's national security is entirely dependent on foreign experts, action must be taken to develop and maintain domestic expertise in advanced data processing.

AI skills key to Sweden's national security

For the total defence to be able to benefit from the opportunities offered by AI technology, and to address the challenges, the AI expertise within relevant organisations needs to increase. Securing maintenance of competence in a field that is evolving rapidly, and that is widely exposed to international competition, is a significant but important challenge for Sweden. Another major challenge for the total defence and society in general is learning how to respond to the new vulnerabilities inherent in AI. Sweden is in a strong position to address these challenges, but relying too heavily on industry and private research initiatives taking responsibility for issues of national interest is a risky strategy.