Consider a world where human decision-making and thought processes play less of a role in the day-to-day functioning of society. Think now of the implications this would have for the security and defence sector. Over the next few decades, it is likely that Artificial Intelligence (AI) will not only have major implications for most areas of society such as healthcare, communications and transport, but also for security and defence. AI can be broadly defined as systems that display intelligent behaviour and perform cognitive tasks by analysing their environment, taking actions and even sometimes learning from experience. The complex attributes of the human mind are well known, but to replicate most of these abilities in machine or algorithmic form has given policymakers and scholars pause for thought. What is more, much of the concern generated by AI centres on whether such intelligence may eventually lead to post-human systems that can generate decisions and actions that were not originally pre-programmed. Accordingly, optimists argue that AI has the potential to revolutionise the global economy for the better, whereas some pessimists have gone as far as to forecast that AI will mark the end of modern society as we know it.

In the area of defence, it is not too hard to see why the use of AI can represent both an opportunity and a danger. On the one hand, a lack of human oversight on the functioning of AI-enabled weapons systems,
coupled with the non-zero probability that such a system could be compromised, might lead to indiscriminate actions and behaviour that violates international norms on the conduct of war. Such systems are unlikely to respect human dignity, either. Misuse by non-state actors and proliferation are also risks to consider. On the other hand, advocates for AI argue that such intelligence may actually improve military decision-making processes by cutting through the usual fog and friction of the conflict space. Given the high degree of tension and emotion that usually surrounds conflicts, AI-enabled technologies could be deployed to relieve logistical burdens, improve data gathering and interpretation, ensure military-technological superiority and enhance combat reaction times. Irrespective of how AI is viewed, it is clear that its application to the conflict space is likely to raise questions about the future character of warfare and strategic autonomy.

The EU has already started to think about the defence implications of autonomous weapons and AI. For example, on 12 September 2018 the European Parliament passed a resolution calling for ‘meaningful human control over the critical functions of weapon systems’. These discussions and reflections are not only required because there are ongoing discussions within relevant fora such as the Convention on Certain Conventional Weapons (CCW), but also because the US, China and to some extent Russia are taking strides in the area of AI-enabled weapons and surveillance systems. For example, a US project to develop computer algorithms that can make it easier for the US military to interpret satellite and drone surveillance data feeds (nicknamed ‘Project Maven’) has been initiated. These technologies are already being used by the US Africa and Central Commands to mine data provided by drones. As part of its ‘Made in China 2025’ strategy to harness hi-tech sectors for its economic development, Beijing is developing a range of AI research hubs and state-backed research is focussing on cloud computing and facial recognition technologies.

The EU has started to recognise the growing importance of the phenomenon, as can be seen by the signing of a ‘Declaration of Cooperation on AI’ between 25 European countries in April 2018. More specifically on defence, the Preparatory Action on Defence Research’s (PADR) strategic foresight project could include elements of AI in the future and the European Commission’s plan to allocate 5% under the European Defence Fund (EDF) to disruptive technologies echoes the need to invest in AI-relevant research. The Capability Development Plan (CDP) also flags the importance of AI as a future strategic enabler for the EU. In addition, future Permanent Structured Cooperation (PESCO) projects could eventually focus on AI. The European Commission has started to act on AI more strategically with a €1.5 billion investment in AI research and development (R&D) for the period 2018-2020 under the Horizon 2020 programme, a €500 million investment in start-up firms until 2020 under the European Fund for Strategic Investments and specifically on defence, the Preparatory Action on Defence Research’s (PADR) strategic foresight project could eventually focus on AI in the future and the European Commission’s plan to allocate 5% under the European Defence Fund (EDF) to disruptive technologies echoes the need to invest in AI-relevant research. The Capability Development Plan (CDP) also flags the importance of AI as a future strategic enabler for the EU. In addition, future Permanent Structured Cooperation (PESCO) projects could eventually focus on AI. The European Commission has started to act on AI more strategically with a €1.5 billion investment in AI research and development (R&D) for the period 2018-2020 under the Horizon 2020 programme, a €500 million investment in start-up firms until 2020 under the European Fund for Strategic Investments and development (R&D) for the period 2018-2020 under the Horizon 2020 programme, a €500 million investment in start-up firms until 2020 under the European Fund for Strategic Investments and the formation of a Commission-led European AI Alliance and High-Level Expert Group on AI dealing with pertinent ethical questions. It is also notable that on 10 April 2018, 25 European countries signed a declaration of cooperation on AI.

It is for such reasons that there is a need to study the impact that AI might have as a strategic enabler for the EU’s Common Security and Defence Policy (CSDP), especially with regard to military and civilian missions and operations and EU capability.
development. Notwithstanding genuine concerns about defence-related AI, this Brief addresses a question of growing relevance for the EU: in what ways could AI enhance the EU’s ability to tackle security and defence threats and risks? By answering this question, this Brief not only seeks to advance the discussion about AI and security and defence within an EU context, but it also hopes to offer policymakers a few analytical pointers that may be useful when dealing with defence and AI.

Understanding Artificial Intelligence

It is important to be precise about the meaning of AI: it can easily be seen as a stand-alone capability or technology when in reality it should be regarded as a strategic enabler. It is therefore more accurate to speak of AI-enabled cyber-defence, AI-supported supply chain management or AI-ready unmanned and robotic systems. Yet, as a strategic enabler, AI cannot be likened to other enablers such as electricity or fuel because it implies a fundamental paradigm shift in the way decisions are made and taken in the conflict space. It is for this reason that it is also necessary to distinguish between the different branches of AI (see Figure 1).

It is also essential to recall that most AI advances are not being made in the defence sector but by companies such as Amazon, Apple, Google, IBM and Microsoft that are investing billions of dollars in AI technologies and R&D. Additionally, advances in AI sit in parallel to developments in Big Data, distributed ledger technology, data storage capacity, nanotechnology, robotics, the Internet of Things (IoTs) and quantum computing. While data on what countries invest on civil and defence AI R&D is scarce, it is nevertheless possible to gauge how the EU is comparatively performing by looking at the amount of peer-reviewed research that is being produced on civil and defence-relevant AI through the Scopus database (see Figure 2). Of course, such data has its limitations because it is difficult to use research production levels as a reliable indicator of the overall investments made by countries in AI (not least in terms of the applicability of such research for defence). Nevertheless, when searching for the key word ‘Artificial Intelligence’, the database shows that since 2008 research centres in the EU-28 have published 19,051 (or 30.7%) of the global total of 62,000 articles – China 9,671 (or 15.6%) and the US 9,572 (or 15.4%).

European research institutes and academies are therefore responding to AI with fundamental research, but there are question marks over how far this research is being translated into applied research and innovation projects. For example, there are currently over 200 AI-related patents listed on the European Patent Register and many were filed by non-EU manufacturers. This compares to over 450 patents for cloud computing and over 10,000 patents for automobile-related products. However, European governments have understood the importance of innovating in AI and a number of EU member states are developing national AI strategies and investing government funds into AI research.

FIGURE 2 | Peer-reviewed journal articles on AI
2008-2018

Data: Scopus/Elsevier, 2018
France has signalled its intention to invest €1.5 billion in AI research by 2022 as part of the country’s broader innovation plan. On 18 July 2018, the German government announced that as part of its national strategy on AI it would examine its research and innovation funding, develop key infrastructure and skills. France and Germany also plan to work together on AI, and a number of other EU member states have developed or are developing national AI strategies (such as Estonia, Finland, and Sweden). Although data is still imprecise, one estimate of the economic impact of AI and automation calculates that the benefit will be anywhere between €6.5 trillion and €12 trillion annually by 2025.

Despite its paradigm-shifting nature, however, there are still limitations to AI systems and more time and investment are required before these systems reach maturity. At present, AI systems are capable of reading data but there are limits as to how far these systems can interpret data. There is still a gap between reading and reasoning in AI. In this sense, for the time being humans still play a vital role in data interpretation and reasoning. Continued investment in AI is vital if intelligent systems are to be used effectively and responsibly, yet success in developing defence-relevant AI will depend in large part on governments being able to invest enough capital, and having the skills base necessary, for AI R&D and robotics. However, most progress in AI technologies will likely emerge in the civil sector. This highlights a familiar discussion about the importance of dual-use technologies for the EU. If it is accepted that relevant AI R&D will largely emerge from the civil rather than the defence sector, then an emphasis on building relationships with civilian actors such as firms and research institutes is of paramount importance.

**AI and CSDP missions and operations**

There are multiple ways in which AI might serve as a strategic enabler for CSDP missions and operations (see Figure 4 for an overview). These enabling factors can be organised across three broad categories: detection, preparation and protection.

**Detection**

AI could be used by the EU to enhance its surveillance and intelligence capacities for CSDP deployments. Specifically, it could allow the EU to gather data from large-scale geographical areas without having to increase staffing levels. In essence, AI-enabled systems could assist the EU’s ‘Integrated Approach’ by not only mining multiple data sources, but also interpreting data in such a way that a clearer picture of conflict and/or crisis dynamics in a country or region emerge. Although the causes and characteristics of conflict are largely multifaceted and unpredictable, AI-enhanced software could help EU bodies such as PRISM and the Single Intelligence Analysis Capacity (SIAC) within the European External Action Service mine open-source data to better detect and monitor fragility in specific countries and regions. Early AI-assisted big data conflict and crisis analysis and intelligence could close the gap between detection and early action. Other EU capabilities could benefit from AI-enabled systems. For example, the EU Satellite Centre (EU SatCen) already use AI-tools to assist with data gathering from their round-the-clock earth surface scanning (see Figure 3 below). The potential of using a constellation of sensors to build up a predicative analysis of ground-level conditions is also being considered.

Furthermore, AI could improve the EU’s detection capacities at the tactical level. For example, counter-piracy maritime operations such as EUNAVFOR Atalanta could in the future leverage AI-enabled platforms to monitor a specific geographic area. As Figure 3 shows, the EU SatCen is already using AI systems to monitor open water areas through a mixture of systems. Deep learning techniques could allow such operations to predict and/or detect erratic or abnormal maritime behaviour based on a blend of satellite imagery, high-altitude platform stations (HAPS), unmanned system footage/images and sensors, when such technologies are available and permitted. Even the EU’s peacebuilding and humanitarian initiatives could benefit from AI-enabled technologies, especially in post-conflict and/or fragile situations. If AI leads to enhanced situational awareness, this could support the choice of locations for the provision of humanitarian assistance, thereby potentially making it easier to identify secure locations for setting up refugee camps (i.e. by identifying water supplies and optimal aid delivery routes). Keeping in mind important issues such as privacy and data security, the EU’s border assistance missions might also benefit from AI-supported technologies such as biometrics and facial recognition to deal with customs checks and monitoring.

**Preparation**

AI could well play a larger role in decision-making processes under the CSDP, and crisis management planners could use AI-enabled systems to compress the ‘planning-decision-action loop’. Interestingly, AI may be used to categorise and/or rank policy options according to pre-programmed criteria which could provide policymakers with a more precise understanding of deployment factors such as costs, required staffing and equipment levels, the impact of operational footprints on local communities and, in the extreme, likely casualty numbers. Of course, relying on existing or past data to assist with detection or prediction for such variables is easier than situations where data is scarce or unavailable. Nevertheless, AI could alter the way mission and
operation planners and commanders draft crisis management concepts (CMC), concept of operations (CONOPS) and operational plans (OPLANs) for CSDP deployments. AI-backed systems could lead to a more efficient allocation of resources and capabilities during missions and operations and they could provide the Political and Security Committee (PSC) with a more complete picture of the crisis scenario and context. Finally, given the creation of the Military Planning and Conduct Capability (MPCC), EU command and control could benefit from AI-enabled technologies to better coordinate multiple missions and operations that are characterised by varying degrees of intensity, geography, unknown contingencies and strategic objectives.

The possibilities of using AI-enabled systems for training and exercises should not be overlooked, either, especially given that the EU runs exercises of a dual civilian and military nature (the CMX and PACE exercises, for example). AI may be leveraged in CSDP table top exercises to assist with the identification of possible policy options and to enhance the learning experience by confronting policy planners with more realistic crisis scenarios. In this sense, AI-enabled training platforms could more accurately mimic the actions of individual adversaries and terrorist groups based on data from their past actions, doctrines and strategies even if AI-enabled systems may not be able to fully recreate the element of surprise usually associated with terrorist attacks. Concerning operational training, already in 2016, a Raspberry Pi computer enabled with AI was able to beat a fighter pilot in a simulated environment. Additionally, AI-enabled systems could greatly enhance the work of the European Security and Defence College (ESDC) in areas such as CSDP pre-deployment training. While there can be no replacement for humans in communicating the psychological and emotional aspects of crisis management, AI-assisted learning tools could provide trainees with a more holistic understanding of the crisis situation they will be deployed to.

Finally, AI technologies could support the logistical aspects of CSDP military and civilian deployments. AI-supported analysis could help identify safe locations for basing, suitable transport infrastructure, landing tracks, proper evacuation routes and/or proximity to local and regional supply chains. AI could aid CSDP logistical planners with environmental management, too. Such intelligence could also greatly assist with the maintenance of transport capabilities and aid with inventory management. As far as the components and replacement parts of military and civil platforms are concerned, AI could play a role in identifying anticipatory needs and supply (AI controlled sensors under the IoTs could detect engine or weapons systems faults before they occur and signal to suppliers that a replacement part should be shipped to theatre in time, for instance). What is more, AI-enabled (semi-)autonomous vehicles could assist with supply and transportation of military and civil equipment and sentry systems could even be deployed to protect supply lines and lines of communication for CSDP missions and operations. The use of robots for the purposes of explosive ordnance disposal and medical treatment are well documented, but AI-systems could also be used to protect EU convoys when deployed in non-permissive environments. This is particularly important given that a host of non-combative actors (NGOs, aid workers, diplomats, etc.) also use EU lines of communication.

FIGURE 3 | Example of AI use at the EU Satellite Centre
Fully automatic ship detection with feature extraction (here: length in metres)
FIGURE 4 | CSDP tasks and AI applicability

Data: Scopus/Elsevier, 2018

Protection

CSDP military and civilian missions and operations take on a variety of tasks (see Figure 3 for specific examples). Given the different levels of intensity of each task, AI could contribute to helping the EU protect its personnel and improve its force endurance in the field. For example, a military CSDP deployment at the highest end of the intensity spectrum such as the separation of enemy forces could employ autonomous (person out-of-the-loop) and near-autonomous (person-on-the-loop) air, naval and land systems to engage in rescue and evacuation tasks. Relatedly, AI-enabled loitering munitions might be envisioned to boost the capabilities of troops operating in non-permissive environments characterised by hybrid threats and/or anti-access area denial (A2/AD) capabilities or in response to a terrorist attack. While CSDP personnel are unlikely to operate under such circumstances for an extended period of time, the example of the deployment of the Quick Reaction Force (QRF) EUTM Mali is instructive of the hostile environments CSDP personnel can find themselves operating in.\(^\text{23}\)

Current research into AI-enabled technologies touches on a wide range of areas including image sensing in dark or hostile environments and medical guidance for human and robot medics. These technologies are applicable to CSDP deployments and the combination of AI and (near) autonomous swarm systems could be invaluable for helping EU forces with situational awareness in the field, especially in densely populated urban areas. AI-enabled systems could also protect EU personnel from in-theatre risks such as disinformation campaigns and cyber defence. Given that some governments and criminal networks are developing AI-enabled technologies to mimic the behaviour of legitimate organisations and individuals, the EU could counter such tactics with AI-supported capabilities to reveal fake images, videos and/or audio files. AI could therefore be used for the swift and effective dissemination of EU messaging. Relatedly, AI could help CSDP personnel accurately distinguish between hostile military forces and innocent civilians when cloaking or hostage tactics are employed. In relation to cyber defence, AI-enhanced protective software might boost capabilities to protect communication information systems (CIS) through more precise traffic analysis, enabling the identification of unusual or unauthorised behaviour on EU networks.

Developing capabilities with AI

Despite the potential operational effects of AI, it could impact EU capability development processes, too. More broadly, AI may have implications for the European Defence Technological and Industrial Base (EDTIB), not least in terms of defence R&d, supply chain management and production. AI-enabled technologies could help with the prototyping phase of defence projects by modelling expected performance and maintenance, repair and overhaul (MRO) cost projections. In production, AI-enabled robotics and additive manufacturing systems could make up the shortfall in skilled labour entering the defence industry. When defence contracts are awarded, AI-management systems could help firms avoid delivery delays and reduce overhead costs. Standardisation might be easier as AI-ready systems trawl, identify and apply standards databases from the civil and defence sectors. Enhanced use of
sensors and data management could also allow AI systems to model and control material usage during production, especially with regard to production factors such as the tensile strength and/or blast resistance of materials and components. Additionally, AI could assist with supply chain management by scouting for new technologies and components on a European and global basis while factoring in security of supply concerns.

It is for such reasons that AI-related technologies could increasingly inform the work of the PADR and any future European Defence Research Programme (EDRP) after 2020. While PADR/EDRP projects are subject to an ‘ethical, legal and societal review’ (ELSA review), it is clear that there is room for AI to help improve the competitiveness of Europe’s defence industry. Indeed, even projects that are already supported by the PADR could eventually lead to AI-inspired follow on projects. For example, the EU’s ‘Ocean2020’ defence research project focuses on maritime situational awareness and its core task of fusing multiple data sources and demonstrating the interaction of unmanned systems and sensors could be amplified with AI technologies in the future. Given that an important logic of the EDF and the CDP is about investing in the EU’s future defence technologies, AI could greatly enhance the EU’s ability to detect and analyse defence technology and capability trends.

Finally, AI-supported databases could allow the EU to better track capability inventories and redundancies. Presently, the EU has a range of databases and catalogues that are designed to list European military capabilities and facilitate exchange of information, including: the Collaborative Database (CODABA) and the force, requirement and progress catalogues used as part of the EU’s Capability Development Mechanism. The Coordinated Annual Review on Defence (CARD), PESCO and the CDP benefit from these databases. Although human military expertise is invaluable to capability development processes, AI-enabled data systems could assist capability development planners with the management of such databases, as well as extract potentially valuable information from them. For example, planners could use AI to get a better idea of the expected performance of the listed capabilities and associated usage and MRO costs, as well as manage overall capability inventories. This is of growing importance given the increasing sophistication of defence technologies and the sheer level of data involved in managing defence capabilities and their support packages.

‘Deep learning’ for EU defence

This Brief has focussed on the ways in which AI could enhance the EU’s ability to tackle and prevent security and defence threats and risks. It has been suggested that AI-enabled technologies and systems could enhance the EU’s capacity to detect threats and risks by enhancing its situational awareness and analytical tools, prepare for CSDP missions and operations by improving training and decision-making techniques and protect military and civilian personnel when deployed by the EU. It has also been shown that AI-enabled technologies could play a significant role in the defence capabilities developed in the EU and they may enhance the EDTIB, too. This Brief has provided evidence to suggest that AI could enhance the Union’s ability to act faster, decisively and effectively under the CSDP, although greater technological advances are required to collect and marshal relevant data. Also, it is likely that AI will need to operate alongside humans for quite some time before reaching a substantial degree of autonomy. Given the growing abundance of data and the types of sophisticated military technologies being rapidly developed, the question is: can the EU really afford to miss out on the so-called ‘AI revolution’?

Of course, the adoption of AI-enabled systems in support of CSDP operations and missions may also result in unintended consequences. Two in particular are worth noting. First, there are a host of legal and moral dimensions that emerge out of the discussion – dimensions already recognised by the European Parliament and the European Commission. These include the ethics of using AI-enabled autonomous (or near-autonomous) systems for the identification, tracking and targeted killing of individuals during military CSDP operations and missions and/or AI-supported facial recognition technologies as part of the EU’s civilian CSDP border monitoring and capacity building missions. Related to this ethical discussion are questions about the level of control humans exert over AI systems. Should AI-systems eventually act beyond the intended boundaries set by humans, the issue of accountability would emerge and conflict situations might deteriorate even further as a result. Second, as with the development of any new defence technology there is the potential danger of proliferation and AI-enhanced systems being used by non-state actors.

The EU has already begun to think about the possible implications of AI and any future EU strategy will likely stress the importance of promoting multilateral responses to the use of AI for military purposes. Yet initiatives such as the EDF already provide the Union with an opportunity to think through the possible applications of AI to defence and to what degree the EU should invest in defence-relevant AI technologies. The European Defence Agency (EDA) has also begun to promote the importance of AI for defence with studies, workshops and stakeholder meetings and the
recently revised CDP invokes the importance of AI as a cross-domain capability priority for the future. Furthermore, joint reflection with NATO under the EU-NATO Joint Declarations could aid the EUs efforts, too, especially given that AI-backed technologies will be used by the alliance during its Trident Juncture exercise from October-December 2018.

Ultimately, however, it is important for the Union to grasp the game-changing attributes of AI. As a potential enabler for EU military and civilian missions and operations and capability development, AI represents another technological domain that – if mobilised effectively and appropriately – could enhance the EU’s strategic autonomy.

Daniel Fiott is the Security and Defence Editor at the EUISS.

Gustav Lindstrom is the Director of the EUISS.

Endnotes

1) Such a definition of AI is quoted in the European Commission’s Communication on ‘Artificial Intelligence for Europe’, COM(2018) 237 final, April 25, 2018


12) Scopus allows users to track and catalogue academic publications released around the world in multiple scientific areas of study. See https://www.scopus.com/solutions/scopus


19) SIAC is an arrangement that integrates the analytical capacities of the EU Intelligence and Situation Centre (EU IntCen) with the EU Military Staff’s intelligence directorate.


22) For example, see Peter W. Singer, “Wired for War: The Future of Military Robots”, Brookings Institute, August 28, 2009 https://www.brookings.edu/opinions/wired-for-war-the-future-of-military-robots/


24) The ELSA review brings together a group of international experts to discuss military ethics issues and compliance with international law.

