EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

NON-PROLIFERATION AND DISARMAMENT PAPERS

No. 84 July 2023

WEAPONIZING INNOVATION? MAPPING ARTIFICIAL INTELLIGENCE-ENABLED SECURITY AND DEFENCE IN THE EU

RALUCA CSERNATONI

I. INTRODUCTION

Emerging and disruptive technologies (EDTs) such as artificial intelligence (AI) systems are ushering in a new era of high-tech global competition and geopolitical rivalry. AI and most notably advances in machine learning (ML) are already affecting warfare in various ways. Cutting-edge AI systems herald significant strategic advantages as 'ultimate enablers' of key major players such as the United States and China, but also risk unforeseen disruptions in global regulatory and norms-based regimes governing armed conflicts.[1] As an all-purpose and enabling technology, AI is an umbrella term that is often framed as revolutionizing the very ontology of war, and engendering paradigmatic shifts in strategic, operational and tactical military praxis.[2] AI has undeniably become a keystone in both national strategies and military doctrines. Its development for military purposes fuels fears of a new 'arms race' and that adversarial zero-sum thinking will dominate global politics. AI-enabled security and defence applications in particular are prompting heated debates about the technology's weaponization and widespread militarization, as well as ethical and regulatory concerns over the use and deployment of AI technologies on the battlefield.

More critical engagement is needed with the notion of 'military AI', especially since it has been narrowly conflated with militaristic visions of a technologically disrupted future, fuelling related research and

SUMMARY

Emerging and disruptive technologies and their security and defence uses have become central to European Union (EU) initiatives. Artificial intelligence (AI) systems are no exception. As the focus of great power rivalry and increasing weaponization, AI technologies present both risks and opportunities in terms of transforming civil–military relations, due to their dual-use characteristics, and their increasing deployment in the cyber-physical domain. This paper explores recent EU-led efforts, identifying common programmes and projects, and considering the European technological sovereignty discourse, recent strategic initiatives and the key stakeholders involved. In the absence of an EU strategic vision that clearly articulates a position on this emerging technological domain and its responsible military research, development and fielding, such efforts risk becoming scattered pieces of an absent overarching intellectual puzzle. The paper also provides a cautionary tale regarding the mainstreaming of AI-driven technological solutions into security and defence across the EU, noting that this legitimizes a specific geopolitical and militaristic imaginary of innovation that might not be compatible with the EU's promotion of responsible, trustworthy and human-centric visions of such systems.

ABOUT THE AUTHOR

Dr Raluca Csernatoni (Romania/Hungary) is a Research Fellow at Carnegie Europe, where she specializes in European defence with a focus on emerging and disruptive technologies. She is currently a Guest Professor with the Centre for Security, Diplomacy and Strategy at Vrije Universiteit Brussel. Her previous positions include Visiting Faculty at the Department of International Relations, Central European University, Vienna; and Postdoctoral Researcher and Lecturer at the Department of International Relations, Charles University, Prague. Csernatoni holds a PhD and a master's degree in international relations from Central European University.

[1] Horowitz, M. C., 'Artificial Intelligence, international competition, and the balance of power', *Texas National Security Review*, vol. 1, no. 3 (2018), p. 41.

[2] Shaw, I. G. R., 'Robot wars: US empire and geopolitics in the robotic age', *Security Dialogue*, vol. 48, no. 5 (2017); and Holmqvist, C., 'Undoing war: War ontologies and the materiality of drone warfare', *Millennium: Journal of International Studies*, vol. 41, no. 3 (2013).

development (R&D) efforts and the race to deploy lethal autonomous weapon systems (LAWS).[3] Most recently, this notion has been linked to the use of artificially intelligent swarming drones in the application of military force, or 'military swarms'.[4] While efforts to pave the way for the increased delegation of lethal force to such technologies merit substantive reflection, rapid advances in ML are already poised to transform almost all aspects of the business of war, from defence industry supply chains to civil–military dynamics in R&D, military decision making, operations, training, logistics and force protection, among other things.[5] While recent analysis has focused on US and Chinese power dynamics, less attention has been dedicated to the European Union's (EU) efforts or its perspectives on military AI.

Against this backdrop, the geopolitical element of AI systems has attracted more attention at the EU level, where it is seen as a powerful tool of economic, political and military statecraft. This geopolitical dimension has also played out in the context of recent discussions about strengthening European 'strategic autonomy' and 'technological sovereignty', and in line with developments spearheaded by the self-styled 'geopolitical' European Commission of the incumbent president, Ursula von der Leyen.[6] This is not surprising, given the challenges of mainstreaming critical technologies such as military AI into European security and defence practices, principally due to the differing competencies within the EU and among its member states in high-politics fields such as foreign, security and defence affairs. Indeed, security and defence matters, including those related to the technological and industrial domains, as well as their respective strategic R&D initiatives, have traditionally been the exclusive competency of member states. These matters operate under intergovernmental decision making within the EU, rather than become subject to the EU's supranational leadership.[7]

In recent years, however, the European Commission has expanded its competencies in these fields through market-based and industrial initiatives to shape and bolster the competitiveness and innovation of the European Defence Technological and Industrial Base (EDTIB).[8] It has also increasingly linked civilian science, technology and innovation programmes to the emergence of the EU-led security and defence R&D policy areas that benefit from innovation in critical dual-use technologies.[9] Against this background, this paper focuses on recent EU plans for AI-enabled security and defence technologies by exploring projects under EU-led financing programmes such as the European Defence Fund (EDF) and its precursor programmes, as well as projects led by the European Defence Agency (EDA).[10]

First, section II examines R&D trends in AI-enabled security and defence initiatives in the EU. Section III then discusses the unmanned swarm systems programmes under the EU's Pilot Project on Defence Research. Section IV maps AI-related defence research projects under the Preparatory Action on Defence Research (PADR) and section V highlights several defence industrial projects supported by AI as part of the European Defence Industrial Development Programme (EDIDP). Section VI assesses the role of the EDF as a game changer for AI defence technologies. Finally, section VII looks at several AI defence initiatives and applications spearheaded by the EDA, before the paper ends with recommendations and overarching conclusions in sections VIII and IX.

As a realpolitik vision of technological solutionism gains increasing strategic traction in Brussels and EU member state capitals, it is important to note that this equally legitimizes a specific geopolitical and militaristic imaginary that might not always

[3] Bo, M., Bruun L. and Boulanin, V., *Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS*, SIPRI Report (SIPRI: Stockholm, Oct. 2022); and Boulanin, V. and Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems*, SIPRI Report (SIPRI: Stockholm, Nov. 2017).

[4] Verbruggen, M., 'The question of swarms control: Challenges to ensuring human control over military swarms', EU Non-Proliferation and Disarmament Papers no. 65, Dec. 2019.

[5] Goldfarb, A. and Lindsay, J. R., 'Prediction and judgment: Why artificial intelligence increases the importance of humans in war', *International Security*, vol. 46, no. 3 (2022).

[6] Csernatoni, R., 'The EU's hegemonic imaginaries: From European strategic autonomy in defence to technological sovereignty', *European Security*, vol. 31, no. 3 (2022).

[7] Csernatoni, R., *The EU's Defense Ambitions: Understanding the Emergence of a European Defense Technological and Industrial Complex*, Carnegie Europe Working Paper (Carnegie Europe: Brussels, Dec. 2021).

[8] Wilkinson, B., 'The EU's defence technological and industrial base', In-depth analysis requested by the European Parliament Sub-Committee on Security and Defence, Jan. 2020.

[9] European Commission, 'Action Plan on Synergies between Civil, Defence, and Space Industries', COM(2021) 70 final, 22 Feb. 2021.

[10] The European Defence Fund (EDF) supports competitive and collaborative projects throughout the entire cycle of research and development for a bigger impact on the European defence capability and industrial landscape. European Commission, Defence Industry and Space, 'European Defence Fund', accessed 23 June 2023.

be compatible with the EU's identity as a normative and civilian power.[11] Sociotechnical imaginaries are group achievements and collectively held visions, where certain visions and aspirations take hold and gain collective force as key stakeholders mobilize the resources to make their visions more durable and desirable over time.[12] The move towards this militaristic vision contributes to the creation of a collective imaginary of Europe as a strategically independent global power and technologically sovereign imagined space. At the same time, however, attention should be drawn to how the EU can contribute to a rules-based international order and military AI arms control regime, thereby mitigating the growing normalization of military AI and autonomous systems use in warfare, as well as their widespread deployment on the battlefield.

To achieve this, both EU-funded programmes and EDA initiatives should take the relevant steps to develop best practices and address the potential risks, challenges and undesired outcomes that stem from military AI, from establishing standards of human oversight over AI-enabled technologies to considering the unpredictability and safety of certain systems, and recognizing the increased chances for conflict escalation and infringement of international law, and of ethical principles.[13] Sceptics have argued against overly hyping the disruptive effects of AI systems as heralding a new 'revolution in military affairs'.[14] Nonetheless, it should be noted that AI presents a host of new challenges and risks, since human agency is at stake.[15] This paper aims to critically engage with EU-led efforts by identifying common projects with elements of AI-driven security and defence technologies. The focus is on EU-level supranational and intergovernmental defence cooperation.

II. RESEARCH AND DEVELOPMENT TRENDS IN AI-ENABLED DEFENCE

For the past two decades, there has been a growing global belief among major powers such as the USA and China that more autonomous weapon systems, which are seen as the culmination of algorithmic war, are needed to mitigate the impact of AI-enabled warfighting on human cognition, speed of reaction and scale of attack.[16] In line with a circular logic, they promote an imaginary by which the apparent solution to problems generated by the increased automation of weapon systems is to be found in *more* AI-enabled autonomous weapon systems.

When a new technology promises enhanced intelligence, speed, accuracy and efficiency, this exerts disruptive effects on military power projection in global politics.[17] Nonetheless, this logic also rests on an instrumentalist and deterministic view of military AI and autonomous weapon systems, whereby such technologies are neutral tools or technological solutions in the hands of states and human agents, and only a technological solution can mitigate the challenges they trigger.[18] This is reflected in ongoing discussions within the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems, especially in relation to the convergence of new technologies in the case of LAWS or when states seek to establish definitions of LAWS as neutral technological tools that serve their aims and interests.

When it comes to the EU, from a policy perspective, experts, policymakers and political leaders are increasingly embracing the instrumentalist and solutionist view outlined above, in the light of an increasingly volatile geopolitical landscape and increasing technological competition between the great powers.[19] This has paved the way for the rise of imaginaries of European strategic autonomy and technological sovereignty in EU security and defence matters.[20] To illustrate, in his opening speech at the

[11] Csernatoni (note 6).

[12] Jasanoff, S., 'Future imperfect: Science, technology, and the imaginations of modernity', eds S. Jasanoff and S. H. Kim, *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (University of Chicago Press: Chicago, 2022).

[13] Boulanin, V. et al., *Responsible Military Use of Artificial Intelligence: Can the European Union Lead the Way in Developing Best Practice?*, SIPRI Report (SIPRI: Stockholm, Nov. 2020).

[14] Horowitz, M. C., 'Do emerging military technologies matter for international politics?', *Annual Review of Political Science*, vol. 23 (May 2020); and Gilli, A. and Gilli, M., 'Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage', International Security, vol. 43, no. 3 (2018/19).

[15] Hoijtink, M. and Leese, M. (eds), *Technology and Agency in International Relations* (Routledge: Abingdon/New York, 2019).

[16] Amoore, L., 'Algorithmic war: Everyday geographies of the war on terror', *Antipode*, vol. 41 (2009).

[17] Suchman, L., 'Algorithmic warfare and the reinvention of accuracy', *Critical Studies on Security*, vol. 8, no. 2 (2020).

[18] Schwarz, E., 'Autonomous weapons systems, artificial intelligence, and the problem of meaningful control', *Philosophical Journal of Conflict and Violence*, vol. 5, no. 1 (2021).

[19] Brattberg, E., Csernatoni, R. and Rugova, V., 'Europe and AI: Leading, lagging behind, or carving its own way?', Carnegie Endowment for International Peace, 9 July 2020.

[20] Csernatoni (note 6), p. 398.

EDA Annual Conference 2022, High Representative/Vice President Josep Borrell noted that 'EDTs—such as artificial intelligence—have the potential to alter the character of warfare' and that the 'Great Powers around the world', including the USA, China and Russia, are developing and operationalizing these for military purposes.[21] This indicates how EDTs are increasingly being framed, and that dual-use AI is being given increased emphasis.

In this respect, the European Commission has instigated significant action to contribute to European security and defence innovation by boosting R&D, and by addressing strategic dependencies in critical technological domains. Specifically, the Commission's 'Roadmap on critical technologies for security and defence' aims to boost and promote synergies between civilian and defence R&D in order to enhance the competitiveness and resilience of EU security and defence sectors.[22] The 2022 Roadmap highlights that more mapping and analysis need to be done to understand the EU's strategic dependencies, vulnerabilities, associated risks and capacities, by providing in-depth reviews of sensitive technological ecosystems such as AI systems.

The Commission carried out two preliminary case studies of defence technology areas: one on autonomous systems and the other on semiconductors, due to their cross-cutting relevance for military capabilities in different domains. The autonomous systems study comprised analytical work on autonomous systems for defence, paying specific attention to AI and ML. It identified relevant critical technologies and the four main areas where the EU is lagging behind: skills, data, hardware and testing.[23] Exploring synergies between various EU-led innovation programmes such as Horizon Europe and the Digital Europe Programme (DEP) was also emphasized, with a view to fostering coordination in priority areas such as cybersecurity, AI and supercomputing.

Notwithstanding these analytical and mapping efforts by the Commission, critical voices have pointed out that the EU has been slow to think about the dual-use, military and geopolitical implications of AI, as the focus has primarily been on the social, economic and normative implications of high-risk uses.[24] Indeed, the EU's Artificial Intelligence Act recognizes such risks by proposing the first-ever horizontal law on safeguarding that AI applications and systems are trustworthy and human-centred.[25] However, the act specifically excludes AI systems developed or used exclusively for military purposes from its regulatory scope. Nonetheless, dual-use AI technologies pose regulatory challenges, as they create 'yet another layer of uncertainty, as one cannot know whether any given item has been created with civilian or military purposes'.[26]

The European Commission notes in its 2021 'Action Plan on synergies between civil, defence and space industries' that many emerging and digital technologies offer substantial potential for defence, including AI.[27] Disruptive technologies such as AI are defined as technologies 'inducing a disruption or a paradigm shift, i.e. a radical rather than an incremental change'.[28] Furthermore, it finds: 'Development of such a technology is "high risk, high potential impact", and the concept applies equally to the civil, defence and space sectors. Disruptive technologies for defence can be based on concepts or ideas originating from non-traditional defence actors and find their origins in spin-ins from the civil domain.'[29]

The EDF envisages that up to 8 per cent of its budget should support EDTs and defence projects on innovative applications, including AI technologies. This raises further questions about the power dynamics within the emerging European defence innovation field and regarding EDTs such as AI, as well as the Commission's role in reorganizing the EU's

[21] European External Action Service (EEAS), 'European Defence Agency: Opening remarks by High Representative/Vice-President Josep Borrell during the annual conference', EEAS Press team, 8 Dec. 2022.

[22] European Commission, 'Roadmap on critical technologies for security and defence', COM(2022) 61 final (2022), 15 Feb. 2022; and European Commission, 'Commission unveils significant actions to contribute to European Defence, boost innovation and address strategic dependencies', Press release, 15 Feb. 2022.

[23] European Commission (note 22), pp. 4, 7.

[24] Christie, E. H., 'Defence cooperation in Artificial Intelligence: Bridging the transatlantic gap for a stronger Europe', *European View*, vol. 21, no. 1 (2022); and Sahin, K. and Barker, T., 'Europe's capacity to act in the global tech race: Charting a path for Europe in times of major technological disruption', DGAP Report no. 6, 22 Apr. 2021.

[25] European Commission, 'Regulation of the European Parliament and of the Council, Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', COM(2021) 206 FINAL, 221/0106 (COD).

[26] Carrozza, I., Marsh, N. and Reichberg, G. M., *Dual-use AI Technology in China, the US and the EU: Strategic Implications for the Balance of Power*, PRIO Paper (PRIO: Oslo: 2022), p. 9.

[27] European Commission (note 9), pp. 2, 13.

[28] European Commission (note 9), pp. 2, 13.

[29] European Commission (note 9), pp. 2, 13.

innovation imaginary around the notion of 'disruption' in defence.

The EDF also represents an unprecedented change for the EU. It is the first financial instrument to fund the R&D of defence technologies as part of the EU budget and the 2021–27 Multiannual Financial Framework.[30] The goal with operationalizing the EDF is to foster home-grown innovation and European defence industrial cooperation so that Europe can benefit from cutting-edge, interoperable defence technology and equipment, including in novel areas such as AI and drone technology. Nonetheless, ethical concerns were raised during the 2019 discussions on the partial political agreement on the EDF. The Greens/European Free Alliance group in the European Parliament pushed to ensure that funding from the EDF would not be allocated to LAWS.[31]

Moreover, in line with the EDF regulation, any research project involving autonomous weapons should require meaningful human control. Indeed, this should be a vital benchmark in any coherent EU policy approach to military AI, with the potential to shape all EU-funded security and defence projects. The EDF regulation states that the eligibility of projects related to new defence technologies should be subject to developments in international law.[32] Thus, the development of LAWS with no possibility for meaningful control over selection and engagement decisions when carrying out strikes against people should not be eligible for funding, 'without prejudice to the possibility of providing funding for actions for the development of early warning systems and countermeasures for defensive purposes'.[33] However, the precise definition of meaningful human control and the notion of military AI have both been the subject of substantial international political and academic debate and are highly contested.

It remains unclear how human oversight and control can be 'meaningful', in terms of how such oversight could be implemented in practice, given the complexity and black-boxed nature of most of AI-enabled systems. There is equally little agreement on what exactly 'military AI' involves. This umbrella term comprises technologies ranging from certain types of autonomous weapon systems used in algorithmic warfare, their research, development and fielding, to the ecosystem of civil and military stakeholders involved in their innovation and production, as well as more mundane applications of the technology in the cyber-physical domain, military structures and operations. Most frequently, the correlative concepts of disruption and meaningful human control are associated with discussions related to the legal, normative, ethical and cybersecurity challenges such systems raise in the cyber-physical domain.[34] This is due to the fact that 'the emergence of new weapons systems with autonomous features can shape the way force is used and affects our understanding of what is appropriate' in human–machine teaming and oversight.[35]

When it comes to the R&D of AI-enabled defence technologies beyond the case of LAWS, various initiatives indicate that progress has been made at the EU-level and among member states to capitalize on their advantages as critical strategic enablers. Several key EU defence technological and industrial projects now contain AI elements. The EU and in particular the European Commission and the EDA have recognized the need for strong public–private partnerships and investments in home-grown and cutting-edge AI-enabled defence technologies, notably by promoting civil–military synergies across dual-use and high-tech innovation ecosystems in the EU. Priority has been given to mobilizing civil security R&D programmes for defence purposes. There is already substantial evidence from the EDF's precursor programmes of which technology areas and projects are prioritized. The following sections dive deeper into such programmes by mapping key AI-enabled defence projects and their framing.

III. UNMANNED SWARM SYSTEMS AND THE PILOT PROJECT ON DEFENCE RESEARCH

The Pilot Project on Defence Research, which ran from November 2015 to November 2018, was a critical step in the EU's defence integration. It was set up in partnership by the European Commission and the

[30] Csernatoni, R. and Oliveira Martins, B., 'The European Defence Fund: Key issues and controversies', PRIO Policy Brief no. 3, 2019.

[31] Brzozowski, A., 'European Defence Fund agreed amid ethics concerns', EURACTIV, 22 Feb. 2019.

[32] EDF, Regulation (EU) 2021/697 of the European Parliament and of the Council, establishing the European Defence Fund, 29 Apr. 2021, Article 10, 'Eligible actions', para. 6.

[33] EDF (note 32), para. 6.

[34] Csernatoni, R. and Mavrona, K., 'The artificial intelligence and cybersecurity nexus: Taking stock of the European Union's approach', Carnegie Europe, 15 Sep. 2022.

[35] Bode, I. and Huells, H., *Autonomous Weapons Systems and International Norms* (McGill-Queen's University Press: Montreal/Kingston, 2022), p. 8.

European Parliament, with the participation of EU member states, and was the first time the EU tested the conditions for funding collaborative defence research within an EU framework and budget. The Pilot Project was run and managed by the EDA on behalf of the Commission. It spearheaded the European Commission's 2017 PADR, which in turn led to the creation of a fully fledged EDF.

The signing of Pilot Project grant agreements worth €1.4 million marked the beginning of the EuroSWARM, SPIDER and TRAWA projects.[36] While this sum might seem trivial compared to the immense budgets of other states, it marked a resolute step in the EU's defence research integration and its prioritization of specific technological domains. Beyond the clear focus on technologies that enable remotely piloted aircraft systems, by giving prominence to swarm research on defence and human detection algorithms in mobile robots to achieve situational awareness, the EU set a precedent when setting EuroSWARM's main objectives—to develop key techniques for adaptive, informative and reconfigurable operations by unmanned heterogeneous swarm systems.

The project was expected to deliver a command-and-control architecture for autonomous and heterogeneous swarms of sensors. While weaponry was excluded from the system, using aerial unmanned swarm-based autonomous systems such as EuroSWARM could be a pilot for large-scale use to deal with both internal and external security and defence challenges, such as border management and surveillance. These technologies raise questions regarding human–swarm relations, agency and oversight, not to mention the ethical, regulatory and strategic implications related to fielding them as part of security and defence practice.[37] The EU should therefore consider the long-term implications of developing such technologies and ensure that they are used only in compliance with international law and regulations. The development and deployment of these technologies should also be subject to ethical considerations, in line with the principles of transparency, accountability and respect for human dignity, civil liberties, privacy and autonomy. There should be careful consideration of the potential risks associated with swarming drones, including the potential for loss of human life, property damage and other unintended consequences.

Dual-use research on swarms has also been conducted under the EU's Framework Programmes for Research and Technological Development. For instance, the European Commission's Horizon 2020 project, Roborder, is designed to respond to the needs of border authorities and law enforcement agencies across Europe, by 'developing and demonstrating a fully functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles which will incorporate multimodal sensors as part of an interoperable network'.[38] The intention is to implement a heterogenous robot system and boost it with detection capabilities for early identification of criminal activity in border and coastal areas. The EU's funding for the development of dual-use AI-powered drones that can autonomously patrol Europe's borders cannot be easily ignored, due to their potential for military use. These drones also contribute to the militarization of borders.

Major European defence companies have become central beneficiaries of numerous EU research projects involving AI technologies.[39] This has had a notable impact on shaping the EU's imaginary for security- and defence-related R&D. Complex challenges such as irregular migration are being managed through technocratic policy initiatives and defence industry-driven lobbying to invest more in the R&D of cutting-edge technologies for border security.[40]

A 2021 in-depth overview of AI use at EU borders by the European Parliamentary Research Service notes that the EU has been actively exploring how AI technologies can be developed and adopted in order to improve border control and security, and that 'applications for biometric identification, emotion detection, risk assessment and migration monitoring have already been deployed or tested at EU borders'.[41] The report underlines that these 'powerful

[36] Information compiled by the author based on project descriptions and European Defence Agency (EDA), 'First EU Pilot Project in the field of defence research sees grant agreements signed for €1.4 million', 28 Oct. 2016.

[37] Verbruggen (note 4).

[38] Roborder, Project homepage, accessed 23 June 2023.

[39] Csernatoni, R., 'Between rhetoric and practice: Technological efficiency and defence cooperation in the European drone sector', *Critical Military Studies*, vol. 7, no. 2 (2021).

[40] Csernatoni, R., 'Constructing the EU's high-tech borders: FRONTEX and dual-use drones for border management', *European Security*, vol. 27, no. 2 (2018).

[41] Dumbrava, C., *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*, European Parliamentary Research Service (EPRS) In-depth Analysis (EPRS: Brussels, July 2021).

technologies' also pose considerable risks, specifically linked to 'their insufficient or varying accuracy and the multiple fundamental rights risks they entail (including bias and discrimination risks, data protection and privacy risks, and the risk of unlawful profiling)'.[42] For example, the analysis flagged the project iBorderCtrl (Intelligent Portable Control System), which ran between 2013 and 2019 and received €4.5 million in EU funding.[43] It aimed to develop a decision support system for border checks that included an automated deception detection tool. The project carried out pilot tests at several land border crossing points in Hungary, Greece and Latvia, aiming to develop a deception detection tool to identify 'biomarkers of deceit', such as 'left eye blink', increased face redness and 'head movement directions'.[44]

The research, development and results of such projects have been strongly criticized, given their contribution to normalizing algorithmic profiling.[45] In addition, details are scarce for many projects about the exact nature of the research conducted and whether ethical concerns and human rights protections played any role in their design and testing. There is also the risk of a false sense of objectivity and neutrality towards technologies, where technological progress becomes a priori desirable and, more worryingly, detached from broader ethical, legal and social questions.

Overall, swarm research has been increasingly spotlighted in EU-funded programmes and has been a priority for the EDF and its precursor programmes, as evidenced by the prominent positions of EuroSWARM and the PADR flagship project, OCEAN2020. The latter is a €35 million, large-scale technology demonstration project, funded by the PADR under the leadership of Italian arms manufacturer Leonardo and implemented by the EDA to improve interoperability between manned and unmanned systems, for example, by increasing the autonomy of swarms.[46]

IV. AI-ENABLED DEFENCE PROJECTS UNDER THE PREPARATORY ACTION ON DEFENCE RESEARCH

Within the research strand of the EDF, the European Commission earmarked €90 million for the PADR between 2017 and 2019. PADR implementation is run by the EDA. Envisaged as a concrete step in assessing and demonstrating the added value of EU-led defence research and technology and fostering further cooperation between EU member states' ministries of defence and EU defence industries, the PADR was a preliminary phase in the launch of a substantial defence research programme in 2021 by the EDF.

Noteworthy also is the fact that, among other things, the 2019 PADR work programme targeted research on 'future disruptive defence technologies', or those that challenge the future or are emerging game-changers.[47] The call for proposals on emerging game-changers highlighted 'cutting-edge high-risk/high-reward research projects that aim to demonstrate a new technological paradigm within the scope of one or more of the areas, including autonomous positioning, navigation and timing; AI for defence; quantum technologies for defence applications; long-range effects and augmenting soldier capacity', while proposals on challenging the future prioritized 'cutting-edge, high-risk/high-impact research leading to game-changing impact in a defence context'.[48] Unsurprisingly, several projects with AI elements were funded under the 2019 PADR call. However, what exactly 'high-risk/high-reward/high-impact' entails in interpreting the different shades of risk in a security and defence context remains unclear.

In another project, AIDED (Artificial Intelligence for Detection of Explosive Devices), the description states that it aims to use swarming robots and AI algorithms 'able to identify unconventional (Improvised Explosive Devices – IEDs) and conventional (Buried Mines) to autonomously plan offline and run-time mission plans and to provide positioning, navigation and mapping to control a fleet of robots that cooperate quickly to identify a safe passage in a high-risk area'.[49]

A further project with a focus on swarms, ARTUS (Autonomous Rough-terrain Transport UGV Swarm),

[42] Dumbrava (note 41), p. 33.

[43] Intelligent Portable Control System (iBorderCtrl), 'Project summary', accessed 23 June 2023.

[44] Dumbrava (note 41), pp. 17–18.

[45] Statewatch, 'EU: Secrecy of border control "lie detector" research project examined in court', 5 Feb. 2021.

[46] Open Cooperation for European mAritime awareNess (OCEAN2020), 'About the project', accessed 23 June 2023.

[47] EDA, 'Pilot Project and Preparatory Action on Defence Research', accessed 23 June 2023.

[48] EDA (note 47).

[49] EDA, 'Artificial Intelligence for Detection of Explosive Devices (AIDED)', [n.d.].

intends to demonstrate the feasibility of an intelligent small swarm of 3 to 12 unmanned ground vehicles (UGVs) that will closely follow a platoon in various difficult terrains.[50] According to ARTUS, the 'supporting swarm will significantly augment their capacity by: providing substantially added payload for the entire equipment through harsh environments . . . [and] reacting autonomously to unexpected developments'. However, the project does not describe how the intelligent swarm would increase a 'unit's mobility and flexibility; and . . . the overall protection level of the troops'. Nor does it provide details about the intended dynamics of human–swarm interactions.

It is arguable that these framings of the PADR calls contribute to the creation of a certain imaginary surrounding 'the future' and of defence research on emerging, 'game-changing' or disruptive technologies such as AI-enabled swarming robots. The notion of disruption, which is synonymous with several of the framings in the PADR calls such as 'a new technological paradigm', 'cutting-edge' and game-changers, is indeed becoming increasingly central to various EU policy areas. This indicates that these narratives and research framings seek to mitigate the EU's dependence on these technologies, but that they also ensure the legitimization of EDTs and AI systems in EU priorities.

This non-linear way of thinking behind disruption, which aims to permanently break up lines of continuity, has also long been observed in the military domain. Technological revolution and innovation have been equally important topics in security and defence praxis, culminating in the crystallization of concepts such as the revolution in military affairs in the 1970s and 1980s. In the case of the EU, the importance given to disruptive technologies seen as silver bullets for the EU's strategic autonomy is illustrative of how stakeholders frame current conversations on AI in security and defence.

V. DEFENCE TECHNOLOGIES SUPPORTED BY AI IN THE EUROPEAN DEFENCE INDUSTRIAL DEVELOPMENT PROGRAMME

The EDIDP was a two-year industrial programme in 2019–20 to boost the competitiveness and innovation capacity of the EU's defence industry.[51] The aim was to support the efforts of the EU defence industry to develop defence equipment and technologies by providing co-financing from the EU budget. The EDIDP had a budget of €500 million over two years and was the second precursor programme of the EDF alongside the PADR.

The EDIDP allocated €158.3 million to 26 projects as a result of its 2020 calls, while in 2019 it had a total budget of €196.6 million for 16 selected projects. A cursory examination of the 2019 and 2020 EDIDP projects identifies several examples worthy of note with regard to AI. In the 2019 call for proposals, three projects integrate algorithms with increased autonomy and automation in space, ground and sea environments: (*a*) iMUGS (Integrated Modular Unmanned Ground System); (*b*) OPTISSE (Very High Resolution Optical Payload for Small Satellites for Defence Applications); and (*c*) SEA DEFENCE (Survivability, Electrification, Automation, Detectability, Enabling Foresight of European Naval Capabilities in Extreme Conditions).[52]

The ambitiously named 2020 EDIDP project AI4DEF (Artificial Intelligence for Defence) aims to 'demonstrate the benefits of AI for better situation awareness, decision making and planning'.[53] In addition, to 'illustrate the transversal and scalable approach of AI4DEF as a cloud service platform, it will be implemented in multiple domains such as UAV (unmanned aerial vehicle) missions with means-of-effect optimization, enhanced Joint ISR (intelligence, surveillance and reconnaissance) analysis, tactical situation awareness and decision making'.[54] Noteworthy here is the decision to frame the project as delivering on the promise of European sovereignty.

This harnesses the promise of technology as a source of the EU's geopolitical identity building and power projection. Within the technological sovereignty imaginary, there is a palpable urgency-driven imperative and a permanent state of emergency against structural forces that call for reduced dependencies and a 'made-in-Europe' AI for security and defence. Similarly, seeking to reduce such dependencies in the space context, the 2020 EDIDP project INTEGRAL (Innovative and Interoperable Technologies for Space Global Recognition and Alert) aims to develop a space intelligence capability, through a European

[50] EDA, 'Autonomous Rough-terrain Transport UGV Swarm (ARTUS)', [n.d.].

[51] European Commission, 'European Defence Industrial Development Programme (EDIDP)', accessed 23 June 2023.

[52] European Commission (note 51).

[53] European Commission and Council of the EU, 'AI4DEF: Artificial Intelligence for Defence—Selected Projects European Defence Industrial Development Programme (EDIDP) 2020', 2021.

[54] European Commission and Council of the EU (note 53).

military space situational awareness (SSA) command-and-control system.[55] The project will 'study, design, prototype and test an advanced space command and control (C2) flexible and modular architecture to process and exploit SSA data generated from sensors in order to provide a complete military space picture'.[56] According to the project description, the project will rely on innovative algorithms based on AI/ML to overcome the limitations of current SSA command-and-control systems, paving the way for the achievement of European independence with regard to military SSA. Here, the stated goal is also that of strategic autonomy and 'European independence' with regard to space situational awareness.[57] Coordinated by the Italian company Vitrociset, a subsidiary of Leonardo, the project is a close collaboration with another 2020 EDIDP project, SAURON (Sensors for Advanced Usage and Reconnaissance of Outerspace Situation), to form the two facets of a future European space surveillance network.[58]

Other 2020 EDIDP projects merit a mention, such as MIRICLE (Mine Risk Clearance for Europe), the air combat capability project MUSHER and the advanced design of the HERMES data exchange platform, which supports the cyber defence of autonomous military systems.[59]

Nonetheless, various commonalities connect all of these projects. First, there is little public information about the projects themselves and it is relatively difficult to obtain further details on specific AI elements or how ethical considerations feature in their development and prototyping. In addition, given the range of functions envisaged, EDIDP activities demonstrate how cross-cutting AI for defence is. However, given the absence of a common EU strategic vision that clearly articulates a position on this emerging technology and its military research, development and use, the risk is that such projects become scattered pieces of an absent intellectual and strategic puzzle.

VI. THE EUROPEAN DEFENCE FUND AND AI DEFENCE TECHNOLOGIES

Through its total budget of close to €8 billion for the period 2021–27, the EDF seeks to promote cooperation among EU defence industries and research actors of all sizes and geographic origins across the EU. In the category of disruptive technologies, it has signalled various potential research topics, including AI for defence.

Thus, within its selected projects, the EDF supports high-end defence capability projects such as the next generation of fighter aircraft, tanks and ships, as well as critical defence technologies such as military cloud, AI, semiconductors, and space, cyber or medical countermeasures. It will spearhead disruptive technologies, most notably quantum technologies and new materials, and tap into promising small and medium-sized enterprises and start-ups. In addition, €13.5 million has been earmarked for improving research on cyber defence and on using AI for incident management.[60] The 2022 EDF call for proposals has a budget of approximately €924 million. Eight calls will address 16 categories on 33 topics, ranging from adapting cyber situational awareness to building shared databases for image recognition, medium-sized semi-autonomous vessels, underwater manned/unmanned teaming and swarms, and adaptive camouflage.[61]

Several successful individual project proposals that were awarded funds under the 2021 EDF call contain AI elements, from use in cyber defence operations to intelligent automation, knowledge extraction, frugal learning (developing high-performing machine learning algorithms with little data and with energy efficiency) for rapid adaptation of AI systems,

[55] European Commission and Council of the EU, 'INTEGRAL: Innovative and Interoperable Technologies for Space Global Recognition and Alert—Selected Projects European Defence Industrial Development Programme (EDIDP) 2020', 2021.

[56] European Commission and Council of the EU (note 55).

[57] EU Agency for the Space Programme (EUSPA), 'Space Situational Awareness', 10 Dec. 2022; and Fiott, D., *The European Space Sector as an Enabler of EU Strategic Autonomy*, In-depth analysis requested by the SEDE Subcommittee (European Parliament: 16 Dec. 2020).

[58] European Commission and Council of the EU, 'SAURON: Sensor for Advanced Usage and Reconnaissance of Outerspace Situation—Selected Projects European Defence Industrial Development Programme (EDIDP) 2020', 2021.

[59] European Commission and Council of the EU, 'MIRICLE: Mine Risk Clearance for Europe—Selected Projects European Defence Industrial Development Programme (EDIDP) 2020', 2021; European Commission and Council of the EU, 'MUSHER: Development of a Generic European Manned Unmanned Teaming (e-MUMT) system— Selected Projects European Defence Industrial Development Programme (EDIDP) 2020', 2021; and European Commission and Council of the EU, 'HERMES: Advanced Design of the HERMES Data Exchange Platform Supporting the Cyber Defence of Autonomous Military Systems—Selected Projects European Defence Industrial Development Programme (EDIDP) 2020', 2021.

[60] European Commission, 'European Defence Fund (EDF) calls 2021', 30 June 2021.

[61] EDF, 'EDF calls for proposals 2022', 2022.

Table 1. Projects selected from the European Defence Fund 2021 call for proposals

Project abbreviation	Project in full
AInception	AI framework for improving cyber defence operations
EU-GUARDIAN	European framework and proof-of-concept for the intelligent automation of cyber defence incident management
KOIOS	Knowledge extraction, machine learning and other artificial intelligence approaches for secure, robust, frugal, resilient and explainable solutions in defence applications
FaRADAI	Frugal and robust AI for defence advanced intelligence
COMMANDS	Convoy operations with manned–unmanned systems
ALADAN	AI-based language technology development framework for defence applications
HYBRID	Hydrogen battlefield reconnaissance and intelligence drone
ALTISS	Highly automated swarm of affordable ISR long endurance UAVs for force protection
IntSen2	Proactive automatic imagery intelligence powered by artificial intelligence exploiting European space assets
SEAWINGS	Sea/air interphasic wing-in-ground effect autonomous drones

AI = artificial intelligence; ISR = intelligence, surveillance and reconnaissance; UAV = unmanned aerial vehicle.

Sources: Information compiled by the author; and European Commission, 'European Defence Fund 2021: Calls for proposals, results', 20 July 2022.

intelligent and cooperative manned and unmanned land systems, AI-based language solutions and innovative automated video detection algorithms (see table 1).

The projects in table 1 fall broadly into the topics of developing innovative and future-oriented defence solutions, and research contributing to disruptive technologies for defence. Moreover, such projects are expected be used in sensitive and high-risk security and defence scenarios. It is important to note that these systems are 'black boxed' to non-expert communities, which impedes proper ethical assessment, including democratic oversight. AI systems are often referred to as 'black boxes' because they are opaque and difficult to interpret, meaning that even experts might not fully understand how these systems make decisions or operate. When decision-making processes are opaque, it becomes extremely challenging to understand how ethical or oversight considerations are factored into them. It can also be difficult to identify potential bias and errors, or to assess the accuracy and reliability of systems. Furthermore, it can become extremely problematic to hold organizations or individuals accountable for any ethical violations that might occur.

More broadly, from a democratic oversight perspective, the secrecy surrounding AI systems can limit the ability of policymakers and civil society representatives to properly scrutinize and influence the decisions that are made on use of these technologies. This can lead to a loss of trust in the policy- and decision-making process and make it difficult for political leaders and policymakers to make informed decisions about the fielding of such technologies. The heavy use of military and technical terminology to describe the above projects is a perfect illustration of both technical and non-technical opacity. This raises critical questions about the epistemic divide between certain high-tech defence expert communities and the broader public, as well as how or whether such projects will (ever) be fielded.

VII. AI INITIATIVES FOR DEFENCE SPEARHEADED BY THE EDA

The EDA has also recognized the need to bring high-tech civilian innovation into defence R&D across the EU. According to the EDA, European armies need to harness new civilian high-tech applications as these have evolved at such speed in the past decade that militaries must now factor 'innovative resilience' into their systems.[62] This demands agile capabilities that can absorb new technologies throughout their lifecycle, thereby avoiding obsolescence. The EDA states that these EDTs are 'significantly changing the rules or conduct of conflict within one or two generations', leading the EU member states' armed forces to adapt their future planning and long-term goals.[63] Further, AI is identified as a key strategic enabler in the EDA's

[62] EDA, 'Pushing limits: Defence innovation in a high-tech world', *European Defence Matters*, no. 22 (2021), p. 6.

[63] EDA, 'Driven by global threats, shaped by civil high-tech', *European Defence Matters*, no. 22 (2021).

Capability Development Plan.[64] In the research and technology domain, more than 50 technology building blocks are flagged as relevant to AI. Other key EDA contributions are the AI in Defence Action Plan and Strategic Research Agenda, which builds on the preceding 'AI in defence definition, taxonomy and glossary', as well as an 'AI in defence narrative', and aims to produce a clear vocabulary on AI for everyone within the EDA.[65] Such efforts try to address the many discrepancies or divergent interpretations among member state experts about what AI actually means.

The EDA believes that combining AI with other technologies and functions will yield new military capabilities that will enable fast decision making and real-time situational awareness, improve operational efficiency and military supply lines, and boost predictive battlefield assessments. In this respect, the EDA has emphasized the need for an EU-wide pool of defence data, as well as rules on data governance and interoperability. The EDA has also emphasized the need for defence-trusted AI in terms of human oversight and trustworthiness, and a more unified EU framework for validating and certifying military AI-based systems.[66] The EDA has highlighted that, with the possible exception of big data analytics, no other EDT has more cross-cutting implications for military operations than AI.[67] The EDA has further positioned itself to manage European expectations on military AI, aiming to lay the groundwork for Europe's armies to exploit AI in many operational areas.

The EDA awarded its flagship Defence Innovation Prize in 2020 to SWADAR (Swarm Advanced Detection and Tracking), an AI-focused project proposal by the Italian Aerospace Research Centre (Centro Italiano Ricerche Aerospaziali, CIRA).[68] The SWADAR project description suggests a technological solution for AI-enabled drone-swarm tracking that provides military commanders with an operational picture of swarm attacks, using 'automated recognition of the swarm-attack scenario' by facilitating AI-driven 'learning of new swarming behaviours'.[69] The solution aims to mitigate evolving attacks in both the military and the civilian fields. As observed above, this description is notable for the use of 'technological solutionism' and native European solutions in line with 'technological sovereignty' civil–military concerns.

The EDA has been laying the groundwork for Europe's armies to exploit AI in many operational areas. Three major projects spearheaded by the EDA are worthy of note.[70] First, a project exploring the concept and rules for an EU-wide pool of defence data, guided by the principles of sovereignty over data, security and trust, data interoperability and the portability of data and services. Second, a project focused on analysing the requirements for defence-trusted AI, the technical robustness and safety of operational AI, traceability and accountability, and the overall rules of data governance. Third, a project to map the requirements for a unified EU framework to validate and certify military AI-based systems. Developing a European framework for testing, evaluating and certifying military AI systems is therefore seen as an important step towards a more integrated approach.

Given the importance of military AI, the question arises whether the EDA, as an intergovernmental EU agency, will be able to drive and shape the EU's and the member states' agendas in order to purse a more structured approach to the R&D of AI-enabled defence systems in line with an ethical and human-centric approach. The EDA must also seek to engender a focused dialogue with tech and defence industrial players and the wider research community. However, the EDA's increasing role in defence innovation potentially clashes with the European Commission's agenda-setting role through its flagship EDF and other programmes, as any possible allocation of EU funds to AI defence R&D would empower the intergovernmental EDA at the expense of the supranational Commission. The related tensions are signs of structural inter-institutional competition between the European Commission and the EDA over the governance and management of EU funds in this sensitive sector. In reality, the EU still lacks a proper horizontal coordination and harmonization strategy for security and defence industrial and research efforts when it comes to AI systems. This could hamper the design of an overarching EU strategic vision that clearly articulates the EU position on this emerging

[64] EDA, 'Capability development', accessed 23 June 2023.

[65] EDA, 'EDA pursues work on Artificial Intelligence in defence', 29 June 2021.

[66] EDA, 'Artificial Intelligence: Joint quest for future defence applications', 25 Aug. 2020.

[67] EDA (note 62), p. 7.

[68] EDA, 'Winner: EDA Defence Innovation Prize', *European Defence Matters*, no. 20 (2021).

[69] EDA (note 68), p. 41.

[70] EDA (note 62), p. 7.

technology and its responsible military research, development and use.

VIII. RECOMMENDATIONS

There is currently no common EU strategy or vision for the responsible governance and innovation of military AI within the EU and beyond. There is an absence of international or multilateral agreements and there are no formal certification processes, universally applicable standards or governance frameworks for AI in military contexts.

This governance gap means that EU-led and European Commission-funded programmes, as well as EDA initiatives, should take steps to identify best practices and address the potential risks, challenges and undesirable outcomes that stem from military uses of AI, such as establishing standards of human oversight over AI-enabled technologies, considering the unpredictability and safety of certain systems, and recognizing the increased chances of conflict escalation and infringement of international law and ethical principles.

First, given the risk of a race to the bottom among international players when it comes to military AI, it is equally important for the EU to engage internationally and with like-minded states to avoid being an isolated voice promoting ethical accountability in AI systems. By working with like-minded allies, the EU can promote its vision of ethical accountability and the protection of democratic values and human rights, while also ensuring that these values are mainstreamed into the development and fielding of military AI systems. By actively engaging with international partners and in international and multilateral forums such as UN processes, or with humanitarian organizations such as the International Committee of the Red Cross, the EU can help to promote a consistent approach to and shared vision of the ethical accountability of such systems. A key recommendation is therefore to facilitate this engagement with like-minded states and allies. In particular, meaningful human control should be a vital benchmark in a coherent EU policy approach to military AI, with the potential to shape both EU-funded security and defence projects, and the international debate.

Second, for many projects, details are scarce about the exact nature of the research being carried out and whether ethical concerns and human rights protections played any role in their design and testing. In this regard, the European Parliament should further expand its oversight role, and its role as a platform for democratic exchange and calls for transparency and public engagement vis-à-vis the ethical and fundamental rights issues raised by military AI. The 2021 guidelines for military and non-military use of AI, proposed by the European Parliament, would be a good starting point for best practices and for the EU to substantially engage with the fundamental ethical and legal question of human control.[71] The guidelines call for an EU strategy to prohibit the use of LAWS, while urging the EU to take a leading role, alongside other UN and international community efforts, in creating and promoting a global framework governing the military use of AI systems. If the trend for deep EU-level integration in the field of defence innovation continues, especially under the EDF and when it comes to the R&D of AI technologies, democratic governance concerns must be addressed. This would involve, among other things, giving a greater role to the European Parliament and national legislative bodies. Whereas both the European Parliament and the European Council determine budget allocations by co-decision, the Commission has the right of initiative in terms of defining priorities for EU budget spending under the EDF and plays a key role in implementing and evaluating projects and programmes for financing. A particular concern, however, is the European Parliament’s and national parliaments’ relative lack of in-house expertise in technological matters, especially concerning disruptive technologies such as military AI systems.[72]

Third, it is important to further increase the centrality of the legal, ethical and technical considerations regarding the responsible use of military AI in EU debates, from the review of dual-use technologies to questions related to the application and interpretation of international humanitarian law, ethical considerations and democratic governance. The EDF regulation stipulates that the Commission should implement a process of ethical screening of proposals and evaluate proposals that raise possible ethical concerns with the support of independent experts. The question arises whether the eligibility criteria are tough enough to ensure that the research, development and fielding of military AI is democratically and ethically desirable for the EU and its member states.

[71] European Parliament, ‘Guidelines for military and non-military use of Artificial Intelligence’, Press release, 20 Jan. 2021.

[72] Csernatoni (note 7).

A key priority will be to develop and implement principles on ethical and responsible innovation to democratically govern the R&D of the AI technologies used in weapon systems, and to ensure accountability and compliance with international law, including international humanitarian law and human rights law. In this respect, the EU's position should remain that human control must be retained in decisions on the use of lethal force and built into the full lifecycle of any weapon system. One way ahead would be for the EU to continue to contribute to the work of the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems, which adopted a set of 11 guiding principles in 2019. In addition, it is important that the EU promote participatory and cooperative mechanisms at the international level to promote understanding of the evolving implications of dual-use AI and how best to manage these, while navigating uncertainty and risk in relation to future developments.

Fourth, for this to happen, the part of the EDF regulation dedicated to LAWS will need to be operationalized and put into practice. Importantly, it should also be taken up as a benchmark in national capitals. More specifically, when it comes to research, innovation and development in AI security and defence systems, ethical concerns should take centre stage throughout their lifecycle, followed by criteria such as safety, explainability, trustworthiness and transparency. Civilian regulatory frameworks can be an important source of inspiration for the military sector. Building on the Commission's ground-breaking work on the governance of civilian uses of AI and given the dual-use nature of AI systems, the EU and its member states should further explore how the norms, regulations and technical principles proposed for the civilian sector, as in the case of the EU's Artificial Intelligence Act and its risk-based approach, could be translated to the security and defence contexts. For this to happen, EU institutions and agencies, EU member states, private sector stakeholders such as the European defence industry and civilian innovators such as SMEs, as well as the expert military, academic and civil society communities, need to engage in concerted efforts to develop a common vision on responsible military AI. Regardless of how the military sector is regulated in the future, the Artificial Intelligence Act is likely to create beneficial spillover effects.

IX. CONCLUSIONS

A strong and progressive EU in terms of, and the European Parliament's common position on, LAWS and other military use of AI is an important signal to both EU member states and their armed forces, as well as the broader international community. According to the European Parliament's 2021 guidelines, AI-enabled systems must allow humans to exert meaningful control, so they can assume responsibility and accountability for their use in line with the principles of proportionality and necessity. However, while there is little consensus on what exactly meaningful human control is or how it can be achieved, the EU could play a role in providing more clarity by making this definition a priority action. The guidelines also call on the EU to take a leading role in shaping and promoting a global normative framework governing the military use of AI, alongside the efforts of the UN and the international community. However, no such common EU framework is under discussion for the responsible governance and innovation of military AI within the EU and beyond.

One main takeaway from the brief discussion above of former and ongoing projects is that they help to create a specific imaginary surrounding the EU's 'future', premised on defence research on emerging game-changing or disruptive technologies such as AI-enabled swarming robots and other military applications. In this respect, more thinking is required across the EU concerning such developments. There is conceptual uncertainty surrounding discussions on AI disruption and EDTs, as there are parallel concerns about enabling and sustaining technologies in security and defence.

This paper provides an overview of existing initiatives. It has found that under the banner of a geopolitically driven and technological sovereignty imaginary, the EU, and especially the European Commission, has begun to frame the policy discussion in terms of mainstreaming security and defence concerns into the R&D of dual-use EDTs such as AI systems. These narratives highlight the R&D potential of various existing instruments and initiatives. However, the nature of dual-use AI technologies can further complicate the already complex landscape of EU policy and governance processes by raising value-laden societal and normative issues that are not typically prioritized in the military realm. Debates related to international norms, hard regulations, ethics, human rights protections, and the trustworthiness and safety of AI should therefore be a top priority for the EU in both the civil–military and the cyber-physical domains.

While the foundations for an EU-led approach to military AI have been laid by the work of the European Commission and the EDA, and to some degree by the European Parliament, this paper concludes that additional measures must be implemented to crystalize an EU strategic vision that is grounded in responsible, trustworthy and human-centric approaches throughout the research, development and fielding cycle for military AI.

ABBREVIATIONS

AI	Artificial intelligence
EDA	European Defence Agency
EDF	European Defence Fund
EDIDP	European Defence Industrial Development Programme
EDT	Emerging and disruptive technology
EU	European Union
LAWS	Lethal autonomous weapon systems
ML	Machine learning
PADR	Preparatory Action on Defence Research
R&D	Research and development
SSA	Space situational awareness

LIST OF RECENT NON-PROLIFERATION AND DISARMAMENT PAPERS

The EU Space Strategy for Security and Defence: Towards Strategic Autonomy?
Non-Proliferation and Disarmament Paper no. 83
Raúl González Muñoz and Clara Portela
June 2023

Armed Conflict And Nuclear Security: Implications For Europe
Non-Proliferation and Disarmament Paper no. 82
Muhammed Ali Alkiş
April 2023

Opportunities for the European Union to Strengthen Biosecurity in Africa
Non-Proliferation and Disarmament Paper no. 81
Benjamin Wakefield
November 2022

Hypersonic Missile Proliferation: An Emerging European Problem?
Non-Proliferation and Disarmament Paper no. 80
Timothy Wright
May 2022

Balancing the Three Pillars of the NPT: How can Promoting Peaceful Uses Help?
Non-Proliferation and Disarmament Paper no. 79
Ingrid Kirsten and Mara Zarka
May 2022

Navigating Chinese–Russian Nuclear and Space Convergence and Divergence
Non-Proliferation and Disarmament Paper no. 78
Lora Saalman
May 2022

Implementing the 2021 Recast of the EU Dual-use Regulation: Challenges and Opportunities
Non-Proliferation and Disarmament Paper no. 77
Mark Bromley and Kolja Brockmann
September 2021

A Comparison of National Reviews of the Treaty on the Prohibition of Nuclear Weapons
Non-Proliferation and Disarmament Paper no. 76
Michal Onderco and Andrea Farrés Jiménez
June 2021

This document has been produced with the financial assistance of the EU. The contents are the sole responsibility of the EU Non-Proliferation and Disarmament Consortium and can under no circumstances be regarded as reflecting the position of the EU.

A EUROPEAN NETWORK

In July 2010 the Council of the European Union decided to support the creation of a network bringing together foreign policy institutions and research centers from across the EU to encourage political and security-related dialogue and the long-term discussion of measures to combat the proliferation of weapons of mass destruction (WMD) and their delivery systems. The Council of the European Union entrusted the technical implementation of this Decision to the EU Non-Proliferation Consortium. In 2018, in line with the recommendations formulated by the European Parliament the names and the mandate of the network and the Consortium have been adjusted to include the word 'disarmament'.

STRUCTURE

The EU Non-Proliferation and Disarmament Consortium is managed jointly by six institutes: La Fondation pour la recherche stratégique (FRS), the Peace Research Institute Frankfurt (HSFK/ PRIF), the International Affairs Institute in Rome (IAI), the International Institute for Strategic Studies (IISS–Europe), the Stockholm International Peace Research Institute (SIPRI) and the Vienna Center for Disarmament and Non-Proliferation (VCDNP). The Consortium, originally comprised of four institutes, began its work in January 2011 and forms the core of a wider network of European non-proliferation and disarmament think tanks and research centers which are closely associated with the activities of the Consortium.

MISSION

The main aim of the network of independent non-proliferation and disarmament think tanks is to encourage discussion of measures to combat the proliferation of weapons of mass destruction and their delivery systems within civil society, particularly among experts, researchers and academics in the EU and third countries. The scope of activities shall also cover issues related to conventional weapons, including small arms and light weapons (SALW).

www.nonproliferation.eu

EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

FONDATION pour la RECHERCHE STRATÉGIQUE

FOUNDATION FOR STRATEGIC RESEARCH

www.frstrategie.org

PRIF HSFK
Peace Research Institute Frankfurt
Hessische Stiftung Friedens- und Konfliktforschung

PEACE RESEARCH INSTITUTE FRANKFURT

www.hsfk.de

Iai Istituto Affari Internazionali

INTERNATIONAL AFFAIRS INSTITUTE

www.iai.it/en

IISS

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

www.iiss.org/en/iiss-europe/

sipri

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

www.sipri.org

VCDNP
Vienna Center for Disarmament and Non-Proliferation

VIENNA CENTER FOR DISARMAMENT AND NON-PROLIFERATION

www.vcdnp.org