Integrating Artificial Intelligence in the European Union's Civilian Common Security and Defence Policy Missions:

Reflections on Opportunities and Risks for Trainings and Operational Uses

Drafted by Dr Francesco Paolo Levantino and Dr Marta Stroppa (SSSA)
within the framework of the activities of the EUTI Working Group on Innovation
24 April 2026

Funded by the European Union

This research paper was prepared in the framework of the activities of the Working Group on Innovation established within the European Union Training Initiative (EUTI) project. It presents reflections on the opportunities, challenges, and implications associated with the integration of Artificial Intelligence (AI) into EU Civilian Common Security and Defence Policy (CSDP) Missions, with particular attention to both training activities and operational uses.

The paper aims to contribute to current discussions on the responsible, effective, and human rights-compliant use of AI in civilian crisis management, in line with relevant EU and international legal and policy frameworks. In this respect, the analysis may also contribute to debates concerning the adaptation of training methodologies and approaches, operational practices, and related capability-development processes within the broader EU civilian crisis-management framework.

In light of the thematic relevance of this topic and considering the still limited availability of dedicated resources and research in this field, the paper could be considered not only for internal circulation within the EUTI consortium and its Working Group on Innovation, but also for possible sharing with relevant EU stakeholders engaged in civilian CSDP training, planning, and operational activities, including the Civilian Planning and Conduct Capability (CivOpsHQ), relevant European Union External Action Service (EEAS) units, and the European Security and Defence College (ESDC). Such dissemination could help stimulate further exchanges in this field; moreover, considering the exploratory nature of this paper, direct interaction with relevant stakeholders may provide useful feedback, highlight emerging priorities and operational needs, and support the orientation of further research and dedicated training activities, while also allowing the EUTI consortium and its members to contribute to the next steps in the development of official EU policies, operational practices, and training approaches.

The paper was written by Dr Francesco Paolo Levantino and Dr Marta Stroppa, Postdoctoral Researchers in international and European law at the Institute of Law, Politics, and Development (DIRPOLIS) of the Sant'Anna School of Advanced Studies of Pisa (Pisa, Italy). Their respective research activities focus primarily on the regulation and use of modern and emerging technologies in different domains – particularly from the perspective of international and European human rights law – as well as on the application of international law to cyberspace and on the use of AI in that context. The paper was developed under the supervision and guidance of Prof Francesca Capone and Dr Annalisa Creta, respectively Associate Professor, Pro-Rector for Internationalisation Policies, and Co-Director of the Master's Programme in International Security Studies and Senior Researcher and Project Coordinator at the same institution.[1]

[1] Sant'Anna School of Advanced Studies, Piazza Martiri della Libertà, 33 – 56127 Pisa (Italy) | Contacts: Prof Francesca Capone (f.capone@santannapisa.it); Dr Annalisa Creta (a.creta@santannapisa.it); Dr Francesco Paolo Levantino (f.levantino@santannapisa.it); Dr Marta Stroppa (m.stroppa@santannapisa.it).

Funded by the European Union

Integrating Artificial Intelligence in the European Union's Civilian Common Security and Defence Policy Missions:

Reflections on Opportunities and Risks for Trainings and Operational Uses

Abstract: This research paper examines the opportunities and risks associated with the integration of Artificial Intelligence (AI) systems into the full life cycle of European Union (EU) Civil Common Security and Defence Policy (CSDP) Missions, with a specific focus on both training activities and operational deployment. In a context characterised by increasing geopolitical instability, violations of international and human rights law, democratic backsliding, transnational threats and climate change, AI is emerging as a potentially transformative tool to enhance the EU's capacity to prevent conflicts, stabilise fragile environments, and support sustainable peace. Its integration may contribute to a shift from a reactive to a more anticipatory, precise, efficient, and adaptive approach to crisis management. The paper first explores the potential role of AI in training and capacity-building activities, including scenarios generation, simulations, exercises design, *curriculum* development, and adaptive learning. It then analyses operational applications across the mission life cycle, examining how AI systems may support planning, implementation and evaluation of Civilian CSDP Missions. At the same time, the paper critically assesses the risks and limitations associated with AI deployment in this domain. These include data quality constraints, biases and discrimination, opacity and limited explainability, data protection and security concerns, as well as potential dependency effects such as deskilling. Such risks are further exacerbated by uneven levels of AI literacy among personnel and the inherent complexity of crisis environments. It concludes that the integration of AI must be firmly grounded in relevant international and EU legal and policy frameworks, including international and European human rights law and, when applicable, the AI Act, the GDPR, and the EUDPR, to ensure that technological innovation reinforces, rather than undermines, the legitimacy and effectiveness of EU Civilian CSDP Missions.

Keywords: EU Civilian CSDP Missions; training; civilian crisis management; artificial intelligence.

Table of content:

Funded by the European Union

1. Introduction

Artificial Intelligence (AI) and AI systems are evolving rapidly and are increasingly utilised across numerous sectors by a growing number of actors to perform diverse tasks. In the context of European Union (EU)'s Civilian Common Security and Defence Policy (CSDP) Missions,[2] their use may have the potential to make crisis management more proactive, precise, efficient, and adaptive, ultimately enhancing the EU's ability to prevent conflicts, stabilise fragile settings, and support sustainable peace. In a context marked by increasing violations of international law and human rights law, democratic backslidings, persistent instability, transnational threats, and climate change, the EU's capacity to defend its interests and those of its partners is indeed under growing pressure.[3] Against this background, AI may support a shift from a reactive to an anticipatory approach to crisis management, bringing important benefits both in the training and deployment phases. In this sense, its potential spans across the entire mission life cycle, from planning to implementation and evaluation, while also offering opportunities to better tailor training programmes, *curricula*, and learning experiences.

At the same time, however, the integration of AI into civilian crisis management also gives rise to important risks and challenges that must be taken into account in order to avoid (or at least minimise) any potential detrimental impact on already vulnerable communities or unstable settings and to ensure compliance with international and European standards. For instance, as AI systems' behaviour depends – *inter alia* – on the quality and quantity of the data used to train them, limited availability and accessibility of quality data in crisis situations may compromise the accuracy of AI-generated outputs, undermining the efficacy and effectiveness of such uses. Likewise, incomplete, biased or inadequate datasets may lead to discriminatory or unfair results, with negative consequences for affected communities and deployed personnel. In training and education, the use of and the blind reliance on such systems may create some distortive effects, e.g., by giving the illusion that the uncertainty characterising real missions can be easily "predicted", or again, by progressively generating dependencies on the side of users possibly leading to serious side effects such as deskilling. Furthermore, the ability of AI systems to process and infer from massive volumes of data raises concerns in terms of data privacy and security. Their opacity, limited transparency, and sometimes unpredictable outputs also pose challenges for accountability in case of harm. These risks are often compounded by insufficient expertise or training of personnel on basic AI literacy.

Against this background, this research paper aims at exploring the opportunities and risks of integrating AI across the entire life cycle of EU Civilian CSDP Missions, including both training and operational practice. Importantly, this analysis is grounded in the recognition that the integration of AI into EU Civilian CSDP Missions should not occur in a normative vacuum. Any assessment of its potential benefits and risks must therefore be situated within, and aligned with, applicable international and EU standards and legal frameworks – including, when their respective scope of application is triggered, those set out in Regulation (EU) 2024/1689 (AI Act),[4] Regulation (EU) 2016/679 (GDPR),[5] Regulation (EU) 2018/1725 on the processing of personal data

[2] The EU currently deploys 13 Civilian CSDP Missions in Ukraine, Georgia, Kosovo, Moldova, Armenia, Libya, the Palestinian Territories (Ramallah and Rafah), Mali, Somalia, Iraq and the Central African Republic, as well as a civil-military Security and Defence Initiative in support of West African countries of the Gulf of Guinea. https://www.consilium.europa.eu/en/policies/csdp-missions-operations/.

[3] Cf., e.g., European External Action Service (EEAS), "Civilian CSDP Compact: Towards More Effective Civilian Missions", 22 May 2023, p. 10.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act, AI Act).

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

Funded by the European Union

by EU institutions, bodies, offices and agencies (EUDPR),[6] as well as sectorial sources and policy documents such as the Strategic Compass for Security and Defence, the Civilian CSDP Compact, the EU's Integrated Approach to External Conflicts and Crises and the EU Policy on Training for CSDP – as well as broader systems of fundamental human rights protection. Compliance with these frameworks is indeed fundamental to ensure that technological innovation supports, rather than undermines, the legitimacy, credibility, and effectiveness of Civilian CSDP Missions.

Within this analytical frame, the paper assesses the extent to which AI can enhance the EU's capacity to act across the full spectrum of crisis management activities – from training, early warnings, and strategic planning to operational deployments, and post-deployment assessments – while identifying and critically examining associated limitations and risks. In doing so, this paper adopts a qualitative and exploratory approach, drawing on existing literature and policy discussions on the use of AI in education and training, as well as on lessons learned from its application in related fields such as disaster risk management. By combining existing knowledge and reflections with the peculiarities of EU Civilian CSDP Missions, the paper assesses both the potential benefits and the limitations of AI systems in crisis management, with particular attention to their compliance with international and European standards.

The paper is structured in three main parts. First, it examines key general features of AI systems which are of cross-cutting relevance for their use in all phases of EU Civilian CSDP Missions (including training) and that warrant careful consideration. In particular, these features require that any use is tailored in light of the intrinsic risks associated with AI systems. The paper then develops around two main thematic areas. The first provides a survey of possible uses of AI for the development and delivery of training programmes, *curricula*, and experiences. The second explores how AI systems can be incorporated into the planning, implementation, and evaluation phases of EU Civilian CSDP Missions. Each of these exploratory thematic blocks will also contain an analysis of potential benefits and risks, identified through the use of relevant international and European sources and standards. The paper then concludes with some final reflections and a set of recommendations.

2. Cross-cutting "properties" of AI systems and their implications

For the purposes of this contribution, the term "AI" is used as an 'umbrella term for computational methods that enable machines to perform tasks typically requiring human intelligence such as learning, reasoning, perception, and decision-making',[7] which includes – *inter alia* – techniques such as machine learning (ML).[8] In turn, the expression "AI system" will refer here to 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments' according to the corresponding definition provided in the AI Act.[9]

[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Data Protection Regulation for EU institutions, bodies, offices and agencies, EUDPR).

[7] Cf. Science Advice for Policy by European Academies (SAPEA), "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", SAPEA Rapid Evidence Review Report, Munich, December 2025, p. 18.

[8] The term "machine learning" refers to '[a] subset of Artificial Intelligence (AI) that enables systems to improve performance on tasks through data-driven learning, rather than explicit programming. It includes supervised, unsupervised, and reinforcement learning'. *Ibid.*

[9] See Art. 3(1) AI Act and, for further information, the European Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C (2025) 5053, 29 July 2025. See also Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", CDDH, April 2026, pp. 6-13.

Funded by the European Union

In addition, given the recent diffusion of commercial and readily available generative AI (GenAI) systems,[10] Large Language Models (LLMs) or Large Visual Models (LVMs), this paper will also consider such tools and make reference to them when relevant since, in most cases, their use would allow to perform at least a significant number of the tasks and activities discussed in the present analysis. In fact, for their relatively low cost, user-friendly interfaces, and their 'capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems',[11] general-purpose AI systems (GPAI) have significantly widened access to capabilities that were previously limited to specialised actors. In this respect, they have contributed to turning instruments once reserved to experts into tools now routinely utilised by a growing number of users. While the uses and outputs of AI systems depend in part on the specific characteristics of the systems at issue, GenAI and GPAI distinguish themselves precisely for their versatility, since they can be employed for a broad variety of tasks and generate outputs of different kinds, including *descriptive* outputs aimed at organising or structuring information, *predictive* outputs based on the analysis of existing data in order to "anticipate" future developments, and *prescriptive* outputs designed to suggest possible courses of action.[12] The widespread diffusion of chatbots such as ChatGPT, Gemini, Claude, Copilot, or Perplexity offers a clear illustration of the relevance of these developments. These systems are in fact frequently approached by very different categories of users as if they were authoritative and reliable sources of knowledge; often without sufficient critical scrutiny.[13] In this connection, recent reports indicate that such tools are being adopted even in particularly sensitive and risky domains, including by high-ranking public authorities,[14] for the identification of hostile intent and online propaganda in order to protect military personnel during oversea deployments, or for the planning and conduct of military operations.[15]

Also in the context of humanitarian aid, disaster and crisis management, there are reports on the increasing use of AI systems to support prevention, preparedness, response to, and recovery from emergencies.[16] In particular, AI is being integrated into a growing ecosystem of digital tools and platforms, including crowdsourcing and data collection systems that aggregate real-time information from, e.g., affected populations; conversational tools and systems powered by LLMs that facilitate communication and information dissemination; training and simulation environments and platforms used to prepare responders through realistic scenario modelling; and automated analysis tools designed to process large volumes of heterogeneous data for rapid situational awareness and decision-support.[17] In these contexts too, however, the integration of AI systems may not always

[10] The term "generative models" refers to 'AI models that can create new content based on training data, e.g. producing text, images, code or simulations. Applications include generating scenario narratives or structured protocols'. SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, p. 18.
[11] See Art. 3(66) AI Act.
[12] Cf. M. Roscini, "Assessing the Role of AI in Determining the Necessity and Proportionality of the Exercise of Self-Defense Against an Armed Attack", *International Law Studies*, 2026, Vol. 107, Issue 1, p. 79 and references there.
[13] F. P. Levantino, "Generative and AI-Powered Oracles: 'What Will They Say About You?'", *Computer Law & Security Review*, 2023, Vol. 51, pp. 1-6.
[14] M. Bryant, "'We Didn't Vote for ChatGPT': Swedish PM Under Fire for Using AI in Role'", The Guardian, 05 August 2025, available at https://www.theguardian.com/technology/2025/aug/05/chat-gpt-swedish-pm-ulf-kristersson-under-fire-for-using-ai-in-role; J. Titcomb, "ChatGPT Triggers Surge in MPs Using AI-written Speeches", The Telegraph, 11 September 2025, available at https://www.telegraph.co.uk/business/2025/09/11/chatgpt-triggers-surge-in-mps-using-ai-written-speeches/; A. Taylor, "Albania Appoints World's First AI-Made Minister", Politico, 11 September 2025, available at https://www.politico.eu/article/albania-apppoints-worlds-first-virtual-minister-edi-rama-diella/. All online resources cited in this research paper were last accessed on 24 April 2026.
[15] Cf. J. O'Donnell, "Phase Two of Military AI has Arrived", *MIT Technology Review*, 15 April 2025, available at https://www.technologyreview.com/2025/04/15/1115078/phase-two-of-military-ai-has-arrived/; Ramkumar, K. Hagey and V. Bergengruen, "Pentagon Used Anthropic's Claude in Maduro Venezuela Raid", The Wall Street Journal, 15 February 2026, available at https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17; E. Pilkington, "US Military Reportedly Used Claude in Iran Strike Despite Trump's Ban", The Guardian, 01 March 2026, available at https://www.theguardian.com/technology/2026/mar/01/claude-anthropic-iran-strikes-us-military.
[16] On this, see *inter alia* A. Beduschi, "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks", *International Review of the Red Cross*, 2022, Vol. 104, No. 919, pp. 1149-1169; and SAPEA, "Artificial intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*
[17] *Ibid.*, p. 23.

Funded by the European Union

be the result of formal institutional policies or dedicated decisions to procure and deploy specific tools. In this sense, at this stage, the use of AI tools may frequently depend on individual initiatives by staff members relying on commercial tools, thus risking taking place outside adequate guidance and supervision.[18] Precisely this kind of concerns seems to underpin the development of GPT@EC, through which the European Commission provides its staff with access to different LLMs within a controlled environment, thus limiting the direct reliance on external commercial tools for the processing of internal information.[19]

In this light, AI seems to have the potential of bringing several benefits if integrated both in the training of civilian personnel taking part in EU Civilian CSDP Missions, and in the implementation of the missions themselves (from the planning stage to the conduct and evaluation phases).[20] Yet, AI also presents some important limitations that must be taken into account before delving into specific applications of AI in this context.

First, it should be considered that AI systems' behaviour largely depends on the data used to train them,[21] as well as on the "input data" used to operate such systems.[22] Following the often quoted "garbage in-garbage out" principle, 'poor data quality leads to equally poor outcomes'.[23] If the datasets used to train these systems are incomplete, outdated, or contain errors, the outcomes might be poor in quality and reproduce such characteristics.[24] This may significantly impair the system's capacity to generate accurate, relevant, timely and meaningful outputs in relation to the system's intended purpose. In this connection, a related issue concerns the presence of biases in the design and development of AI systems. Biases in algorithms (also known as algorithmic bias) may be linked to technological or statistical errors deriving from, e.g., (under)representation of specific groups, contexts or events, or again, to the dominance within training datasets or input data of certain human viewpoints, prejudices and stereotypes that are then reflected in AI systems' performance and corresponding outputs. If left unaddressed, such biases can accumulate and intensify – especially if embedded in feedback loops where the outputs of a given AI system and then feedback as training or input data of other systems – thus reinforcing biases over time and perpetuating risks or discrimination, particularly against vulnerable or underrepresented groups.[25]

Moreover, now moving to the way in which AI systems operate in practice, these systems are often characterised by a high degree of "opacity". In fact, at the current state of technological development, it is particularly difficult to understand how AI systems reach specific outputs due to the complexity of their innerworkings, the scale and heterogeneity of the data involved in their training and operation, and the non-linear nature of their processes through which their outputs are produced – to the extent that AI systems are often described as "black boxes".[26] This lack of interpretability complicates efforts to explain why a particular decision was made, which inputs were decisive, or whether the system behaved in accordance with its intended purpose. In the context of GenAI systems, opacity is further exacerbated by the fact that their outputs are generated on the basis of statistical patterns rather than through deterministic rules or a genuine

[18] See Access Now, "Reinventing Humanitarian Aid Procurement for the Age of AI", March 2026, pp. 2; 7-8.
[19] See European Commission, "Commission Launches a New General-Purpose AI Tool – GPT@EC", Directorate-General for Digital Services (News Article), 22 October 2024, available at https://commission.europa.eu/news-and-media/news/commission-launches-new-general-purpose-ai-tool-gptec-2024-10-22_en.
[20] Respectively discussed in Sections 3 and 4 of the present contribution.
[21] See the definition of "training data" in Art. 3(29) AI Act where this expression refers to 'data used for training an AI system through fitting its learnable parameters'.
[22] See the definition of "input data" in Art. 3(33) AI Act where this expression refers to 'data provided to or directly acquired by an AI system on the basis of which the system produces an output'.
[23] A. Beduschi, "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks", *cit.*, p. 1158.
[24] EU Fundamental Rights Agency (FRA), "Data Quality and Artificial Intelligence - Mitigating Bias and Error to Protect Fundamental Rights", FRA Focus, 2019, p. 2.
[25] EU FRA, "Bias in Algorithms: Artificial Intelligence and Discrimination", Report, 2022.
[26] M. Almada, "Technical AI Transparency: A Legal View of the Black Box", 14 January 2025, available on SSRN.

Funded by the European Union

"understanding" of the content analysed and then produced.[27] As a result, outputs may be contextually plausible yet difficult to trace back to specific data sources or reasoning pathways, or again, they may even appear coherent and plausible while they are factually incorrect or entirely fabricated, leading to so-called "hallucinations".[28]

Beyond these structural limitations, AI systems are also vulnerable to deliberate interferences affecting the integrity of data and datasets. Such integrity breach may occur, for instance, through cyberattacks aimed at poisoning training datasets or adversarial manipulation of trained models. Feeding malicious or manipulated data into AI systems can significantly distort the systems' behaviour, undermining their performance and reliability. [29]

Relevant EU regulatory frameworks have increasingly sought to address these and other challenges through a combination of different legal instruments. The AI Act, for example, sets out a risk-based approach for AI,[30] and envisages a set of rules applicable – *inter alia* – to providers placing on the market or putting into service AI systems in the EU, to deployers of AI systems established or located in the Union, as well as, under certain conditions, to providers and deployers established in a third country, where the output produced by the AI system is used in the EU. In addition, this Regulation may also apply to EU institutions, bodies, offices and agencies when they act as providers or deployers of AI systems.[31]

Within this framework, the AI Act prohibits specific AI practices which would pose unacceptable risks to fundamental rights and EU values as for its Article 5,[32] and regulates "high-risk AI systems" including – *inter alia* – AI systems classified as such under Article 6 AI Act, including certain systems listed in its Annex III that may 'have a significant harmful impact on the health, safety and fundamental rights'.[33] In relation to "high-

[27] V. Barassi, "Toward a Theory of AI Errors: Making Sense of Hallucinations, Catastrophic Failures, and the Fallacy of Generative AI", *Harvard Data Science Review*, Special Issue 5, 2024.
[28] *Ibid*. In this connection, insofar as this contribution also refers to GenAI systems and LLM-based tools, it should be recalled that the AI Act introduces some "transparency obligations" under its Art. 50 and provides a regime for general-purpose AI models under its Chapter V.
[29] S. T. Erukude, V. C. Marella, and S. R. Veluru, "AI-Driven Cybersecurity Threats: A Survey of Emerging Risks and Defensive Strategies", in S. J. Nanda, R. P. Yadav, M. Prasad, and M. Saraswat (Eds.), "Data Science and Applications: Proceedings of ICSDA 2025, Volume 3", 2026, Springer, Cham.
[30] M. Ebers, "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act", *European Journal of Risk Regulation*, Vol. 16, No. 2, 2025, pp. 684-703.
[31] See Art. 2 and the definitions of "providers" and "deployers" in Art. 3(3)-(4) AI Act. In connection to the application of the AI Act to some of the possible uses of AI explored in this paper, this Regulation applies – *inter alia* – to providers placing on the market or putting into service AI systems in the Union, to deployers that have their place of establishment or are located within the Union, and, under certain conditions, to providers and deployers established in a third country where the output produced by the AI system is used in the Union. In this respect, Recitals 22 and 23 clarify, respectively, the rationale of the "output used in the Union" criterion and the application of the Regulation to Union institutions, bodies, offices and agencies when acting as providers or deployers. By contrast, Article 2(3) AI Act, read together with Recital 24, excludes AI systems that are placed on the market, put into service, or used exclusively for military, defence or national security purposes; that exclusion is purpose-based and does not automatically extend to dual-use or otherwise non-exclusively military uses, which may still fall within the scope of the Regulation. On the use of AI in relevant sectors see also, EEAS, "Civilian CSDP Compact: Towards More Effective Civilian Missions", 2023, *cit.*, pp. 22-23.
[32] Prohibited AI systems or practices include: (a) deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm; (b) exploiting vulnerabilities related to age, disability, or socio-economic circumstances to discord behaviour, causing harm; (c) social scoring; (d) assessing the risk of an individual committing criminal offenses solely based on profiling or personal traits; (e) compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage; (f) inferring emotions in workplaces or educational institutions (except for medical or safety reasons); (g) biometric categorisation systems that infer sensitive attributes (except for labelling or filtering lawfully acquired biometric datasets or when law enforcement categorises biometric data); (h) "real-time" remote biometric identification in publicly accessible spaces for law enforcement (with a *numerus clausus* of exceptions). See, in particular, AI Act, Art. 5 and Recitals 28-45.
[33] Cf. Recital 46 of the AI Act. For further information on which AI systems fall in this category, see also Art. 6 AI Act, Recitals 47 ff., and Annex III to the AI Act.

Funded by the European Union

risk systems", the AI Act establishes a set of requirements concerning – *inter alia* – risk management,[34] data management and governance measures,[35] technical documentation,[36] record-keeping through logging systems,[37] transparency and the provision of information to deployers,[38] human oversight,[39] as well as the accuracy, robustness and cybersecurity of such systems.[40] These requirements primarily fall on providers of AI systems who must ensure that "high risk AI systems" comply with the requirements contained in Section 2 of Chapter III of the AI Act. Moreover, the AI Act imposes specific obligations on deployers of such systems. For instance, deployers must take appropriate technical and organisational measures to ensure that uses of "high risk AI systems" intervene in accordance with providers' instructions for use and must assign human oversight to operators who have the necessary training, competence, support, and authority.[41]

However, provisions concerning, e.g., human oversight and other forms of human involvement and/or supervision in the operation of AI systems are often challenged by a lack of expertise on the side of users, thus reducing the effectiveness of such measures irrespective of whether the AI systems concerned qualify as "high risk". Without a clear understanding of how AI systems function, deployers may not be able to understand their outputs, identify their limitations and inherent risks, such as algorithmic bias and manipulation. In this sense, increasingly more diffused are phenomena involving users-AI systems interactions such as "sycophancy" where AI systems, chatbots in particular, tend to accommodate users' views and expectations.[42] In this light, lack of expertise can foster instances of automation bias, leading deployers to trust and follow the recommendations or decisions of automated systems even when those outputs are flawed, incomplete, or when they contradict other available information.[43] Uncritical reliance may thus result in overlooking errors, or diminishing critical judgement, ultimately increasing possibilities for taking harmful or otherwise risky decisions, with potential negative consequences from multiple perspectives. For this reason, the AI Act provides, at its Article 4, an obligation for both providers and deployers of AI systems to 'take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used, and considering the persons or groups of persons on whom the AI systems are to be used'.[44] Adequate AI literacy, in this sense, might not only mitigate risks but also enable more informed and confident uses of AI, thereby supporting the diffusion of greater trust in such technologies, including among the individuals and groups who may – to different extents – be affected by their deployment.

Other relevant regulatory frameworks are those concerning the protection of personal data, including the GDPR and the EUDPR, which establish a comprehensive framework aimed at ensuring that the processing of personal data is carried out in a manner that respects fundamental rights, and in particular the right to respect for private life and that to the protection of personal data.[45] Accordingly, the processing of personal data in the context of EU Civilian CSDP Missions must – where and to the extent it falls within the scope of such regulations – be carried out in compliance with the applicable EU data protection regime. This implies – *inter alia* – that processing should rest on an appropriate legal basis and comply with data protection principles such as those concerning the lawfulness, fairness and transparency of the processing, purpose limitation, data

[34] See Art. 9 AI Act.
[35] See Art. 10 AI Act.
[36] See Art. 11 AI Act.
[37] See Art. 12 AI Act.
[38] See Art. 13 AI Act.
[39] See Art. 14 AI Act.
[40] See Art. 15 AI Act.
[41] Cf. Arts. 26(1)-(2) AI Act; see also Arts. 13(3)(d) and 14.
[42] Cf. R. Mahari and P. Pataranutaporn, "We Need to Prepare for 'Addictive Intelligence'", *MIT Technology Review*, 05 August 2024, available at https://www.technologyreview.com/2024/08/05/1095600/we-need-to-prepare-for-addictive-intelligence/.
[43] M. L. Cummings, "Automation Bias in Intelligent Time Critical Decision Support Systems", *AIAA 1st Intelligent Systems Technical Conference (20-22 September 2004, Chicago, Illinois)*, 2004.
[44] Art. 4 AI Act. See also Recital 20 and the definition in Art. 3(56) AI Act.
[45] See Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR).

Funded by the European Union

minimisation, accuracy, storage limitation, integrity and confidentiality, as well as accountability.[46] In this regard, the GDPR applies, e.g., where personal data is processed by private entities involved in the development, provision, or use of AI systems in Civilian CSDP Missions, and may also apply to data processing by Member State authorities insofar as such processing falls within the scope of the GDPR and does not fall within relevant exclusions in the field of Common Foreign and Security Policy (CFSP) or within the law-enforcement framework established by Directive (EU) 2016/680, when applicable.[47] In this sense, the EUDPR applies when such processing is undertaken by EU institutional actors themselves, including the European External Action Service (EEAS) and, where applicable, other EU institutions, bodies, offices and agencies involved in the mission framework, while processing carried out by CSDP missions remains governed by the specific scope limitations of Regulation (EU) 2018/1725 and by mission-specific data protection regimes.[48] In the context of EU Civilian CSDP Missions, in fact, this framework is also operationalised through mission-specific data protection regimes, including instructions of the Civilian Operations Commander and standard operating procedures on the protection of personal data, as reflected in the privacy statements and data-protection notices of missions such as EUM ARMENIA, EUCAP SOMALIA, and EULEX KOSOVO.[49]

Finally, not secondary are considerations related to the respect of fundamental rights, as enshrined in applicable international and regional instruments, and in particular in the EU Charter of Fundamental Rights (CFR) and in the European Convention on Human Rights (ECHR).[50] This requirement acquires particular significance when AI systems are integrated into both training and operational EU Civilian CSDP Missions' activities. The use of AI, therefore, must be assessed also against its potential impact on fundamental rights, including – *inter alia* – the rights to privacy, data protection, non-discrimination, and that to an effective remedy.[51] This awareness is essential to guarantee that any use of AI systems across the life cycle of Civilian CSDP Missions remains firmly grounded in the EU's fundamental values and does not undermine the protection of individuals affected by mission activities.

3. Exploring possibilities and risks of using AI for the development and implementation of training for EU Civilian CSDP Missions

Among the possible areas in which AI may be integrated across the "life cycle" of EU Civilian CSDP Missions, training activities seem to constitute a particularly relevant and fertile ground. This is not because such uses would be exempt from risks such as e.g., algorithmic or automation biases and hallucinations,[52] but rather because it is precisely in this context that the flexibility, adaptability, as well as the scalability of AI systems

[46] See, in particular, Arts. 5 and 6 GDPR and Arts. 4 and 5 EUDPR.
[47] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
[48] On the applicability of the EUDPR to AI systems, see European Data Protection Supervisor (EDPS), "Guidance for Risk Management of Artificial Intelligence systems", 11 November 2025. See also Arts. 2(1) and 2(4) EUDPR and Arts. 42(1), 43 and 44 TEU.
[49] See, e.g., the privacy and data-protection notices of the European Union Mission in Armenia (EUM ARMENIA), the European Union Capacity Building Mission in Somalia (EUCAP SOMALIA), and the European Union Rule of Law Mission in Kosovo (EULEX KOSOVO). These notices indicate that personal data processing practices in civilian CSDP missions are framed by reference to Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, as well as mission-specific instruments, including Civilian Operations Commander instructions and Standard Operating Procedures on the protection of personal data.
[50] Cf. F. P. Levantino and F. Paolucci "Advancing the Protection of Fundamental Rights Through AI Regulation: How the EU and the Council of Europe are Shaping the Future", in P. Czech, L. Heschl, K. Lukas, M. Nowak and G. Oberleitner (Eds.), "European Yearbook on Human Rights 2024", Brill, 2025, pp. 3-37; see also Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", *cit.*
[51] In this respect see, for instance, the possible obligation for certain deployers of "high-risk" AI systems to carry out a fundamental rights impact assessment under Art. 27 AI Act.
[52] See *supra* Section 2.

Funded by the European Union

may be leveraged to improve the way in which mission staff are prepared for the wide range of different tasks, challenges, needs, and environments they may be called to face during deployment. In this respect, the rationale for exploring the possibilities AI may offer in this field seems to find connections with the current EU framework on CSDP training. For instance, the 2024 EU Policy on Training for CSDP emphasises that training activities should be learner-centred, interactive, measurable through learning outcomes, and delivered through diverse formats and methods, including e-learning, blended learning, practical exercises and simulations, as well as other state-of-the-art techniques.[53] In a similar direction, reflections on the fact that traditional training produces only limited returns if not complemented by experiential learning, practical exercises, the creation of "communities of practice", and the systematic integration of lessons learned seem to provide elements to consider AI as a promising tool.[54] Likewise, the corresponding 2024 Implementing Guidelines for the EU Policy on Training for CSDP identify among the key elements and features for suggested training methodologies the fact that these should be 'dynamic and adaptable and include organised self-reflection for the participants to support the learning'.[55] In the same context, the acquisition of knowledge through the use of modern and emerging technologies is described as 'an integral part of the educational framework' capable of offering 'unique benefits including flexibility, accessibility, and a vast array of learning opportunities'.[56] These elements seem here particularly relevant not only because they may be easily linked to the possible use of AI in this field, but also because they can be further articulated thanks to similar reflections in the broader field of "AI in education" which frequently push in the direction of considering how the potential added value of AI does not lie simply in automation, but rather in its capacity to *support* more personalised, iterative, interactive and responsive forms of learning, provided that users retain the capacity to review, challenge, adapt and adjust AI-supported outputs. For instance, recent reports by the Organization for Economic Co-operation and Development (OECD) underlie that AI systems may indeed support personalised learning and help reducing tedious or burdensome tasks,[57] while both the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Council of Europe (CoE) warn on the fact that their performance and the effectiveness of their use is not undisputed and remains dependent on the ability of both educators and learners to critically verify and adapt the outputs of such systems before using them.[58] UNESCO, in particular, further underlines that AI-based tools may facilitate access to and support personalised learning and facilitate more innovative educational experiences, while also stressing that such opportunities should always be "filtered" through human-centred and rights-based lenses and that given the high number of issues associated with the blind reliance on these tools, available evidence does not support uncritical or generalised uses.[59] In a similar manner, sector-specific reflections on training for crisis management suggest that AI may help in addressing some structural limitations of traditional approaches by supporting greater adaptability, for example through scenarios generation, while simultaneously warning that positive results of training activities cannot be presumed merely from the use of technologically advanced tools.[60]

In light of these considerations, the use of AI in training for EU CSDP Missions might offer a series of possibilities to be critically examined in light of both the specific functions that each stage of the training "life

[53] See diffusely Council of the EU, "EU Policy on Training for CSDP", 11362/24, 19 June 2024, p. 6 in particular.
[54] *Ibid.*
[55] EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", 15973/2024, EEAS(2024)1450, p. 11.
[56] *Ibid*.
[57] See, in particular, the section "Opportunities of AI and Digital Technology" in Organization for Economic Co-operation and Development (OECD), "Opportunities, Guidelines and Guardrails for Effective and Equitable Use of AI in Education", 2023, see also pp. 6 ff.
[58] See UNESCO, "AI and Education: Protecting the Rights of Learners", 2025; CoE, "Artificial Intelligence and Education: A Critical View Through the Lens of Human Rights, Democracy and the Rule of Law", 2022. See also Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", *cit.*, pp. 83-91.
[59] UNESCO, "AI and Education: Protecting the Rights of Learners", *cit.*, pp. 29 ff.; UNESCO, "AI Competency Framework for Teachers", 2024, pp. 17 ff.
[60] See K. L. Eide, I. Lund-Kordahl and B. Tallak Bakken, "How Artificial Intelligence (AI) Fundamentally Changes Crisis Management Training and Exercises", in M. Sarfraz (Ed.), "Crisis Management Dynamics - Strategies, Challenges, and Best Practices", IntechOpen, 2025, pp. 127-142.

Funded by the European Union

cycle" is expected to perform and the corresponding risks that may follow from the use of such systems. Therefore, in the following pages, reports and studies by international organisations such as the UNESCO, the OECD, the CoE, or the EU will offer the chance to consider the opportunities and risks of using AI in training activities on grounds that are more solid than mere speculation. The next sub-sections will thus reflect on the opportunities and risks of integrating AI across the various phases through which training activities are conceived and designed, delivered, evaluated, and refined.

3.1. AI in the identification of training needs and learning objectives

From the perspective advanced thus far, a first and rather immediate area in which AI could be integrated concerns the very stage at which training priorities, needs, and objectives are identified. This may be considered as a particularly sensitive phase, since it is the one that through preliminary analysis inevitably orients the planning and implementation of further activities. In this respect, the 2024 Implementing Guidelines for the EU Policy on Training for CSDP clearly define the identification of training needs and objectives as a key starting point for the training "life cycle". This approach largely reflects the Analysis, Design, Development, Implementation and Evaluation (ADDIE) instructional design model, in which the analysis phase provides the basis for the subsequent design, development, implementation and evaluation of training activities.[61] More specifically, at this earlier stage the Guidelines frame this process through a requirement-driven logic linked to a Training Requirements Analysis (TRA). In particular, training activities are required to align with a number of elements such as – *inter alia* – policy developments, the lines of operations' mandates, lessons identified in the field, operational requirements and shortfalls, emerging trends, previous training analyses and evaluations.[62] In this field, AI capabilities may be particularly useful insofar as they can support the processing, comparison, and structuring of dispersed information – here intended as information or data scattered across multiple sources and/or formats, and that are often difficult to analyse in a timely and effective manner.[63]

In this direction, AI systems may be used for their capacity to assist those responsible for training design in the identification of recurring observations and themes/topics across large volumes of material, including, e.g., previous evaluations, mission feedback, lessons learned, after-action reviews, training reports, or other forms of documentation produced before, during, and after trainings and deployments. In this context, AI systems could operate as "diagnostic" support tools. Indeed, reports in the field of AI and education highlight that AI systems may be used to identify patterns, generate structured representations of extensive datasets, and support those involved in teaching/planning activities by making more easily detectable possible existing bottlenecks, recurrent trends, challenges or areas in which adapting existing standards and/or practices may be required.[64] Transposed to the context of training activities for EU Civilian CSDP Missions, such capabilities could

[61] See – *inter alia* – R. M. Branch, "Instructional Design: The ADDIE Approach", Springer, 2009.
[62] Cf. EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit.*, p. 6.
[63] With respect to similar uses, however, whenever the documentary basis used for such analyses contains personal data as defined e.g., in Arts. 4(1) GDPR and 3(1) EUDPR, and when such frameworks are applicable, data shall be processed in accordance with relevant provisions, including – *inter alia* – the principles contained in Arts. 5 GDPR and 4 EUDPR, as well as in light of the requirement for an adequate legal basis under Art. 6 GDPR. Moreover, also in relation to the purpose limitation principle, when personal data are collected from data subjects or obtained for purposes related to the uses of AI exemplified here, corresponding information duties as contained in Arts. 13 ff. GDPR and 15-16 EUDPR should also be respected. In addition, where such AI-supported processing is likely to result in a high risk to the rights and freedoms of natural persons, Art. 35 GDPR and, where applicable, Art. 39 EUDPR may require the carrying out of a data protection impact assessment, particularly in cases involving new technologies, systematic and extensive evaluation of personal aspects, or other forms of processing capable of significantly affecting the persons concerned. See also European Data Protection Supervisor (EDPS), "Generative AI and EUDPR. Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems", 28 October 2025.
[64] Cf., *inter alia*, European Commission, "Guidelines on the Ethical Use of Artificial Intelligence and Data in Teaching and Learning for Educators", 2026, pp. 12 ff.; I. Tuomi, "The Impact of Artificial Intelligence on Learning, Teaching, and Education", Joint Research Centre (JRC) Science for Policy Report, 2018, pp. 28 ff.

Funded by the European Union

facilitate the comparison between existing training offers and *curricula* with emerging operational needs or priorities thus supporting the detection of possible overlaps between courses or content areas. Similarly, AI could assist in mapping how newly identified or emerging priorities, needs, and developments relate to existing training offers and structures, potentially enabling more tailored, responsive, and differentiated training content.

At the same time, however, the possible benefits of using AI at this stage of the training lifecycle – as just sketched – should not obscure the ambiguities inherent in the very logic behind such uses of AI. In this sense, the very ability of AI systems to process large quantities of information and identify recurrent patterns may in fact induce excessive confidence in the identification of what for such systems is actually, e.g., most easily retrievable, quantifiable, or repeatedly formulated, at the expense of what the real aims of the training need and objectives identification phase should be *vis-à-vis* context-specific or dependent, more "weakly articulated", politically sensitive, otherwise variable, or simply less visible content. In this connection, recent EU and international guidelines and reports in the field of education repeatedly warn against the blind assumption that the way in which AI performance and outputs support human decision-making processes are neutral or "objective". On the contrary, AI tools' outputs – as such – tend to reflect and reproduce the assumptions, gaps and values represented the most in the data they have been trained with, and therefore may reinforce existing biases or misinterpret needs.[65] In this sense, limiting the identification of training needs and learning objectives to a technical and AI-performed exercise of "pattern recognition" would be reductive. In fact, if left insufficiently scrutinised and/or supervised, the performance of such analyses by AI systems could privilege what has been most frequently reported over what is most significant in that specific case, thus privileging "*quantitative visibility*" over "*qualitative relevance*". This kind of considerations seem particularly problematic in fields such as civilian crisis management, where adaptation is precisely what is required and often depends on (human) capacities and judgments to recognise also through experience what is relevant and urgent in light of mission-specific factors, as well as to orient action through legal and ethical considerations and a precise vision on the distinction between what is already known and "codified" from what seems necessary or desirable.

A similar ambiguity emerges when moving from the identification of training needs to the formulation of learning objectives. Here again, AI may prove useful in supporting trainers or course designers in identifying and drafting measurable objectives and related indicators, organising them into coherent clusters, aligning them with identified requirements, or adapting them to different groups of participants. In this field, however, the Implementing Guidelines expressly refer to the so-called "Bloom's Taxonomy" as a model through which educational objectives may be structured according to a progression of increasingly complex and interconnected cognitive levels – from remembering and understanding to applying, analysing, evaluating, and creating – so as to promote intellectual growth, the development of critical thinking abilities and the capacity to meaningful engage with materials.[66] From this perspective, the formulation of learning objectives does not emerge as a merely formalistic task but already presupposes a judgment concerning the kind of cognitive and professional development that the training aims to foster. In this connection, sectorial reports and guidelines stress that those using AI in educational settings should be able to evaluate whether AI systems effectively support learning objectives, whether these remain sustainable in the long term, and whether their use actually contributes to the common good.[67] In particular, rather than treating AI as a tool capable of autonomously defining what objectives are relevant in any given context, the Guidelines specify that AI use should be subordinated to the pedagogical priorities identified by educators. In this sense, AI may assist in organising learning objectives, activities and resources, or in mapping such elements against the relevant *curriculum*; however, the decisive criterion should remain whether the *suggestions* produced by the system make

[65] See e.g., European Commission, "Guidelines on the Ethical Use of Artificial Intelligence and Data in Teaching and Learning for Educators", *cit.*, p. 10; UNESCO, "AI Competency Framework for Teachers", *cit.*, p. 15; CoE, "Artificial Intelligence and Education: A Critical View Through the Lens of Human Rights, Democracy and the Rule of Law", *cit.*, pp. 37 ff., 67 ff.
[66] See Annex 1 in EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit.*, p. 19.
[67] Cf. European Commission, "Guidelines on the Ethical Use of Artificial Intelligence and Data in Teaching and Learning for Educators", *cit.*, pp. 6-7.

Funded by the European Union

pedagogical sense in the context at hand and effectively support pre-identified learning objectives.[68] AI may indeed *assist* in translating identified needs into more clearly articulated and "cognitively differentiated" objectives, for instance, by helping in distinguishing whether, e.g., a given module or activity is primarily functional to consolidate knowledge, support the practical application of theoretical knowledge, stimulate comparative or other analytical approaches, structure judgments, and so on. In fact, here too it is important not to lose sight of the centrality of this step within the "training lifecycle".

In this sense, the identification of learning objectives does not simply describe expected outputs but already orients training activities towards certain identified and expected forms of professional conducts, behaviours, and competences – therefore influencing how mission staff will be trained. From this perspective, if the use of AI to assist in, e.g., identifying and drafting learning objectives, categorising competencies, or mapping goals against existing *curricula* may indeed render these activities more efficient and more easily standardised, it is this same standardisation process that may become problematic by excessively limiting or automating mechanically existing practices rather than helping to revise and improve them, thus narrowing rather than supporting more reflexive and context-sensitive approaches to the achievement of desirable objectives. Indeed, if simplistic and uncritical uses of AI reduce the formulation of learning objectives to an excessively automated exercise of "taxonomical ordering", linguistic, or other kinds of optimisation, results may emerge as a set of objectives that is formally well written and/or structured but pedagogically weak or deprived of actual possibilities for adaptation. In the case of training for EU Civilian CSDP Missions, such a risk would be especially significant where the capacity to act appropriately depends not only on theoretical knowledge or predefined technical skills but most of all on how these are put to good use in practice through contextual sensitivity and awareness in relation to specific and variable circumstances of each case. In fact, the latter may well require the ability to act in dynamic – and at times unpredictable – socio-political and economical contexts or to consider ethical and legal consequences of the actions taken. In other words, if it is true that, on the one hand, AI may facilitate the translation of identified training needs into defined objectives; on the other hand, it may also foster an overly formalised understanding of such objectives – related competencies and skills – privileging once more what AI can more easily measure and classify over what must instead remain open to human and professional assessments, judgments, reflections, experiences and human-to-human exchanges.

3.2. AI for course conception, curriculum design, and the preparation of training materials

Once training requirements and objectives have been identified, the next phase of the training "life cycle" concerns the actual conception of the course, that is activities functional to – *inter alia* – the definition of the overall course concept, its structuring into a *curriculum* containing specific modules and sessions, their progressive, logical, and pedagogical sequencing, the preparation of classes and materials, as well as the selection of methodologies through which identified objectives are to be pursued. In this respect, AI systems may be integrated in each of these activities bearing in mind their respective specificities.

With respect to course conception, following the identification of training needs and requirements, AI may be useful to further and more specifically convert them into a well-structured learning path. In this sense, AI's flexibility and adaptability may support the drafting or updating process of course concepts, the modular articulation of courses and sessions content and the adaptation of existing courses and their components to different mission and staff profiles, or to different categories of participants. In this regard, also relevant reports and guidelines seem to suggest possibilities for similar uses of AI in the context of education. Yet, they also insist on the fact that the relevant starting point for the integration of such activities should remain the actual

[68] *Ibid*, p. 27. See also, UNESCO, "AI Competency Framework for Teachers", *cit.,* pp. 28 ff.

Funded by the European Union

teaching/training needs and AI integration should be considered only in as far as it is relevant, appropriate, and adds value in relation to the specific needs each time identified.[69]

Transposed to the context of training for EU Civilian CSDP Missions, the 2024 Implementing Guidelines for the EU Policy on Training for CSDP offer useful starting points to explore how AI can support *curriculum* design and lesson planning activities. This is because Annex 2 makes clear reference to the "BOPPPS Model" as a structured framework aimed at ensuring – *inter alia* – lessons' relevance, the active participation of trainees, their continuous assessment as well as continuous adaptation to their needs and characteristics.[70] By encompassing six main elements – Bridge-in, Objective, Pre-assessment, Participatory learning, Post-assessment, and Summary – this model provides a precise idea of how lessons' planning and design is way more than the mere arrangement of content, but a real way of shaping the learning experience through the design and use of specific content to effectively catch the attention of the audience at the opening of classes, clarifying their specific objectives and how learning outcomes will be verified, "activating" prior knowledge and experiences, making them engaging for participants throughout the process and consolidating key messages and content.[71] In light of the "BOPPPS Model", the potential relevance of AI could be discussed in connection to its capacity to support the performance of the pedagogical functions that each of those components is meant to reflect.

For instance, within the "BOPPPS Model" the "Bridge-in" moment is conceived as an introductory moment to establish a connection with the participants' interests in the course/lesson, as well as with their prior experiences and expectations.[72] In the context of training for EU Civilian CSDP Missions, AI may support trainers in generating captivating "prompts" or visual inputs for the audience, in identifying recurring dilemmas, perspectives, curiosities or misconceptions emerging from the interaction with participants, thus making that learning context and experience particularly relevant to that specific audience. In turn, moving to the "Objective" component of the "Bloom's Taxonomy" while the specification of learning objectives for each session is aimed at helping both trainers and participants in orienting their focus and the overall direction of the session towards specific knowledge and skills and, as seen above, this is partly the result of the prior translation of training needs and requirements into training objectives, in this case, AI might actually support the explanation and formulation of lessons' objectives in a way that is functional and consistent to understanding what both their pedagogical and practical value is.

In this connection, AI systems may also support trainers in better and more efficiently designing and structuring so-called "pre-assessment" tasks and activities to determine what the entry level of the audience is, thus granting the modulation of pre-identified possibilities to adjust the lesson's development and its activities accordingly. Similar considerations can also be extended to the "post-assessment" phase of the "BOPPPS Model" which aims at 'measur[ing] the extent to which participants have achieved the learning objectives or gained the intended knowledge and skills from the training' through – *inter alia* – 'quizzes, tests, practical demonstrations, or performance evaluations' depending on the nature and content of the training.[73] In fact, in this case too, AI may assist trainers not only in preparing such tools, but also in calibrating them more closely to the nature of the training, the profile of the participants, and the specific type of, e.g., competences that are expected to be acquired or improved from each specific session. In the context of training for EU Civilian CSDP Missions, this may prove particularly useful where what is to be assessed is not merely the retention of information and knowledge, but the corresponding ability to concretely apply them. In this sense, AI could support the preparation of differentiated forms of knowledge verification aimed, for instance, at testing whether participants are able, e.g., to identify the most suitable legal or ethical frameworks to address a given situation,

[69] See UNESCO, "AI Competency Framework for Teachers", pp. 25, 31, 41; UNESCO, "AI and Education: Protecting the Rights of Learners", *cit.*, p. 35; European Commission, "Guidelines on the Ethical Use of Artificial Intelligence and Data in Teaching and Learning for Educators", *cit.*, p. 27.
[70] See Annex 2 in EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit*., pp. 19-20.
[71] *Ibid.*
[72] *Ibid.*
[73] *Ibid.*

Funded by the European Union

to prioritise competing operational considerations, or to justify a certain course of action in light of mission-specific constraints. In a similar manner, while the statutory function of the "summary component" is to 'reinforce learning, clarify any remaining questions, and solidify understanding' of a given topic,[74] AI may offer support for example by assisting trainers in extracting key takeaways from the lesson/session, in reformulating them according to the specific audience addressed, or in generating concise recapitulations that connect the lesson's content back to the expected learning objectives. In the case of training for civilian CSDP personnel, this may be particularly valuable if one considers how the discussed material/content may well be dense, interdisciplinary or characterised by the integration of different components, sources, and materials. This seems highly relevant if the consolidation of learning requires participants not only to remember what has been read and/or discussed, but also to understand how different elements – of legal, operational, institutional, cultural, or again political nature – have interacted throughout a given exercise or lesson. Yet, precisely because summarisation is also the moment in which the trainer gives final "directions" to the meaning of what has been taught/learned, the use of AI should remain strictly subordinate to the trainers' conscious judgements and choices. Otherwise, even a formally efficient summary may risk flattening or obscuring relevant nuances, over-simplifying tensions that are instead worth preserving (or actually part of the learning process), or conveying a false or illusionary sense of closure in relation to questions that should instead remain open to further reflection.

To conclude this exploration of possible uses of AI in relation to the components of the "BOPPPS Model", the integration of AI systems for "participatory learning" purposes seems among the most promising possibilities thus deserving dedicated attention. On this point, while the objective of this component of the "BOPPPS Model" is to '[a]ctively engaging participants throughout the lesson encourages deeper understanding and retention' of information through, e.g., exercises and simulations,[75] AI may not only support the design and drafting of relevant materials but also enhance possibilities for more tailored and dynamic experiences. In fact, in relation to trainings aimed, e.g., at preparing civilian personnel to operate in complex environments, other than to stimulate the engagement of participants, participatory learning constitutes an added value in so far as it enables them to confront – in a controlled setting – with the constraints, challenges, and specificities that may characterise missions; thus practically, albeit fictionally, helping the audience in familiarising with them. From this perspective, AI may prove useful to support the construction of scenarios that are not only more realistic and detailed but also more adaptive to variations in the profiles, functions, and likely theatres of deployment of the participants. For instance, rather than limiting the use of AI systems to the generic generation of "case studies", instruments such as GenAI could facilitate the creation or improvement of tailored exercises and materials involving variations specific to the role of, e.g., Human Rights, Police, Strategic, Communication, or other Advisors and the operational, legal, ethical, cultural, or other dilemmas that they may be called to face during deployment. In this light, the potential added value of AI could precisely rest in making it easier to improve pedagogical outcomes through the introduction of variables, such as injections, thus allowing participants to confront a broader variety of situations.

In this connection, those reflections on participatory learning also offer the chance to more closely link them to the broader topic of the use of AI systems for the preparation of training materials. In this sense, training materials relevant from the perspective of participatory learning such as scenario briefs, role-play instructions, simulated operational updates, press statements, social-media feeds, incident reports, transcripts of meetings with local counterparts, draft policy or legal texts, or maps are just part of a broader cluster of resources used for the planning, delivery, support and assessment of training activities. In fact, slides shows, infographics, audio-visual materials, self-assessment sheets, handouts and compilations of legal or policy sources, etc., all contribute to the training and learning processes. Here too, AI may support the preparation of more accessible and flexible resources, including multilingual, simplified, or otherwise differentiated versions of the same materials.

[74] *Ibid.*
[75] *Ibid.*

Funded by the European Union

At the same time, however, and in continuity with the observations already formulated in relation to the use of AI for the identification of training needs and objectives, the use of AI – Gen AI, in particular – risks influencing the quality of the training materials used. In fact, as it frequently happens with the use of similar tools in different sectors, the materials produced may appear formally and stylistically convincing and/or coherent while being substantively inaccurate or erroneous, affected by an excessive degree of generalisation, or otherwise questionable. If one of the objectives of participatory learning approaches is that of allowing participants to experiment in view of real-life situations, these issues are particularly problematic whenever such systems not only fabricate or distort relevant information – through so-called "hallucinations" – but also reproduce dominant assumptions, generic narratives, or culturally flattened representations – i.e., biased results – that fail to reflect the actual variables characterising operational environments. It is precisely for these reasons that recent thematic guidelines insist, on the one hand, on the potential of AI to assist in the preparation or update of inclusive and accessible curricular resources and, on the other hand, on the need for human-accountable validation mechanisms and for continuous pedagogical review of whether AI-generated suggestions and materials genuinely contribute to improving the overall quality and effectiveness of materials. Finally, a further issue concerns the provenance/origins and reusability of AI-produced materials. From this perspective, considering how such resources may be later circulated, adapted by other trainers, archived, or reused across training cycles, uncertainty as to the legal status – e.g., in relation to copyright – traceability, or reliability of their underlying content may undermine not only the opportunity of their use in official training contexts, but also the credibility of their providers.[76]

3.3. AI in training evaluation and refinement

The final phases of the training "life cycle" involve the training evaluation and the identification of possible areas for refinement. In this sense, the result of this activity constitutes the final stage of a training cycle and the starting point for the identification of lessons learned and possibilities for improvement to be used for the planning, design and implementation of future training activities. On these points, already the EU Policy on Training for CSDP put a strong emphasis on the relevance of similar reflections,[77] which are further complemented into the 2024 Implementing Guidelines with respect to the explicit mention of the "Kirkpatrick Model" for training evaluation. Structured around four sequential and progressive levels – Reaction, Learning, Behaviour, and Result – this approach prevents evaluation from being reduced to immediate participants' satisfaction and instead invites a broader inquiry into whether training has actually generated learning, whether what has been learned is later applied in professional practice, and whether this in turn contributes to more general and sustainable effects.[78]

The first level of this model, i.e., "Reaction", measures participants' immediate reactions to the training course, focusing on their satisfaction, their perception of the training's relevance, and whether they found the whole experience worthwhile. In this sense, this assessment concerns not only the learners' response to the training process as such, but also their feelings and perceptions about the materials and the trainers they interacted with.[79] In this context, AI may support the processing of the feedback from participants, helping training providers in organising and comparing responses concerning the perceived relevance of the course, the quality of delivery, the usefulness of materials, or the degree of engagement generated by the methodologies adopted. In the case of CSDP-related training, where participants may come from very different professional backgrounds, mission settings, and cultures, such support may be useful in distinguishing whether positive or negative reactions concerned the training as a whole or rather specific dimensions of it – for instance, its degree of perceived relevance, the appropriateness of the level targeted, or the balance between traditional and more

[76] Cf. European Commission, "Guidelines on the Ethical Use of Artificial Intelligence and Data in Teaching and Learning for Educators", *cit.*, pp. 9, 33 ff.; UNESCO, "AI and Education: Protecting the Rights of Learners", *cit.*, pp. 72 ff.
[77] See diffusely Council of the EU, "EU Policy on Training for CSDP", *cit.*
[78] See Annex 3 in EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit.*, pp. 20-21.
[79] *Ibid.*

Funded by the European Union

participatory teaching/learning components. However, if AI systems may indeed facilitate the aggregation and comparison of large volumes of qualitative and quantitative feedback, the use of such outputs and their AI-based assessment or clustering as a self-sufficient indicator of quality and/or success of the training – and of its components – may render that evaluation excessively responsive to what participants found immediately appealing, clear, or efficient, at the expense of what may instead have been willingly calibrated as more demanding, disorienting, or difficult precisely in view of the achievement of certain pedagogical objectives. As it has been already highlighted in different parts of this analysis, in this case too, the risk is that of having AI systems amplifying what is the most readily/easily capturable from feedback rather than what is or might actually be more relevant in this phase.

Moving to the level of the "Learning" component of the "Kirkpatrick Model", the focus shifts more specifically to the extent to which participants have actually acquired and/or consolidated knowledge/skills/competences that the training was expected to develop/provide, as may be assessed, e.g., by comparing pre- and post-training tests. In this respect, if this logic seems to recall the that of pre-assessment and post-assessment stages within the "BOPPPS Model", with respect to the verification of learning at the level of lessons/sessions, this component of the "Kirkpatrick Model" is no longer concerned with whether participants have understood or retained the content of a specific session/lesson, but whether the training activity, considered more broadly, has actually led to the intended learning objectives and, therefore, whether its design, methodology, materials, and delivery have proved effective in relation to the objectives pursued.[80] In this connection, AI may assist in comparing pre- and post-training assessments, in identifying recurring gaps, or in analysing patterns across different cohorts of participants, thus enabling training providers to refine future training activities more rapidly and effectively.[81]

This may prove particularly useful in those courses where learning outcomes combine factual knowledge with the capacity to recognise and handle implications of different nature, such as legal and/or ethical consequences of the way in which concrete situations are addressed. In the context of training for EU Civilian CSDP Missions, for instance, AI-supported analysis could help in detecting whether participants have consistently improved – throughout the training – in identifying, e.g., the human rights implications of a policing measure, in understanding the relationship between a mission mandate and local constraints given by interactions with domestic stakeholders, or in distinguishing between forms of action that are technically efficient but problematic in light of relevant legal or policy frameworks. Yet, even at this level, a certain degree of caution is necessary. The possibility of tracking learning gains through AI-supported forms of assessment does not remove the more fundamental question of whether what is being measured corresponds to what should actually count as learning in this field.

As already suggested in relation to learning objectives, there is always a risk that the use of AI privileges what can be more easily codified, compared, or scored over what remains more difficult to objectify, such as contextual sensitivity, professional judgment, or the capacity to understand and address nuances in complex situations. In this sense, AI may undoubtedly support this more comprehensive part of training evaluation; however, it may not identify and/or resolve the pedagogical questions and issues concerning, for instance, what a meaningful learning gain should consist of within civilian crisis management training.

Moving now to the level of "Behaviour", the latter aims at examining the extent to which participants apply what they have learned once they return to their work environment; in the formulation used in Annex 3 of the

[80] Cf. *Ibid*.

[81] In connection with these possible uses, see however Article 6(2) and Annex III point 3(b) AI Act, which classify as "high-risk" AI systems intended to be used to evaluate learning outcomes, including where those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels. In the context considered here, this classification may become relevant where AI-supported pre- and post-training assessments, scoring, feedback, or learning analytics are used to evaluate identifiable participants' learning outcomes or to influence their subsequent learning pathway, rather than merely to produce aggregated and non-individualised evidence for course improvement. See also Recital 56 AI Act, which links this high-risk classification to the potential impact of such systems on a person's educational and professional trajectory.

Funded by the European Union

Implementing Guidelines, this level concerns changes in behaviour, such as the adoption of new approaches or the practical use of newly acquired knowledge/skills/competences "back on the job".[82] This level is arguably one of the most interesting for possible uses of AI, but also one of the most potentially problematic. It is particularly important in CSDP-related training, since the value of such activities lies not only in the transmission of knowledge but also in the improvement of relevant conducts, decision-making, communication and advising practices, and other forms of professional action in complex settings. Here too AI may appear useful, for example, by helping training providers compare follow-up feedback, mission reports, supervisors' observations, or other forms of post-training documentation in order to identify whether certain skills or approaches seem to recur more consistently after specific training.[83] It may also support the identification of patterns indicating whether what was taught has later influenced, even indirectly, the way in which participants frame problems, communicate within their missions or with relevant stakeholders, or handle recurring or emerging issues. Yet, it is precisely at this stage that the limitations of AI-supported practices show significant shortcomings. Given the specificities of civilian crisis management, behaviour is shaped by a multitude of variables relating to, e.g., mission mandates, institutional and local culture, political constraints, available resources, and the different responsibilities attached to each professional role that no training activity, however well designed, can fully account for. Accordingly, attributing later behavioural developments to a specific training intervention should perhaps be intended as an interpretative task that cannot be reduced to AI-based mechanical "inferences". If AI is used here without adequate caution, the risk is that it may encourage erroneous or excessive reliance on unverifiable causal connections, as if later professional conduct on the ground could be neatly traced back to the training received, whereas in reality what is being observed is the outcome of far more layered and contingent processes, which also have to do with other factors, including, e.g., the characteristic specific to each beneficiary of any given training activity.

Before concluding this exploration of possible uses of AI in relation to each of the main components of the training "life cycle", it is time to discuss the fourth and final level of the "Kirkpatrick Model", namely that concerning "Results". In the logic of this model, this component of the training assessment phase concerns reflections on the broader outcomes achieved as a consequence of the training and aims at determining its longer-term impact through the consideration of improvements in, e.g., organisational processes, overall increased productivity or higher-quality outputs.[84] More specifically, the results of similar considerations might include greater consistency in missions' practices, better alignment between actual requirements on the field and training outcomes or more effective implementation of mission mandates *vis-à-vis* diverse specificities and constraints. In this respect, the Implementing Guidelines themselves make clear that the results of training evaluation should feed into *curricula* revision, updated course concepts, and the preparation of training programmes, while the annual reporting cycle should analyse how the training provided met identified requirements and contributed to broader capability development needs.[85] Also from this standpoint, AI may assist in identifying medium- and long-term patterns across repeated evaluation reports, training cycles, or sets of mission-related observations, thus helping reveal where certain training activities appear to generate more stable and observable benefits and value, where gaps persist, and where, e.g., resources may need to be reallocated or training may need to be differently structured or filled in with targeted content and materials. Nevertheless, it is still the possibility offered by the AI-supported searches for "results" that most clearly reproduces the ambiguity of similar uses of AI as discussed thus far. In this sense, the broader the level of impact considered is, the more difficult it becomes to isolate what can be linked to training activities and

[82] Cf. Annex 3 in EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit.*, pp. 20-21.
[83] If the use of AI in relation to the "Behaviour" level of the "Kirkpatrick Model" is not aimed at merely supporting aggregated training evaluation, but at monitoring, assessing or drawing conclusions about the post-training conduct, performance or professional behaviour of identifiable mission personnel, the assessment may fall under the classification offered for "high-risk" AI systems of Annex III, point 4(b) AI Act, concerning AI systems intended to make decisions affecting work-related relationships, to allocate tasks on the basis of individual behaviour or personal traits or characteristics, or to monitor and evaluate the performance and behaviour of persons in such relationships. See also Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", *cit.*, pp. 92 ff.
[84] Annex 3 in EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit.*, pp. 20-21.
[85] See diffusely EEAS, "Implementing Guidelines for the EU Policy on Training for CSDP", *cit.*

Funded by the European Union

their outputs from what depends on wider, e.g., institutional, operational, or political developments. In such settings, the attraction of AI lies partly in its promise to identify "meaningful" correlations across complex and fragmented bodies of information; yet, the danger is that those correlations may then be treated as stronger evidence of impact than they actually are. This is particularly problematic in contexts such as CSDP missions, where results can be difficult to be isolated from highly variable and dynamic elements of operational environments. Some of them will more clearly emerge in the following section, which with the considerations intervened thus far in mind will explore possibilities and risks of integrating AI into EU Civilian CSDP Missions.

4. Opportunities and challenges of integrating AI in the planning, implementation and evaluation of EU Civilian CSDP Missions

As anticipated above, EU Civilian CSDP Missions pursue a range of objectives aimed at supporting, e.g., peace-keeping, conflict prevention, crisis management, post-conflict stabilisation and reconstruction efforts.[86] In this sense, they represent the EU's flagship instrument for promoting stability, strengthening resilience, and supporting partner countries through non-military means, particularly in contexts marked by instability, emerging threats, or that are affected by ongoing crises. As the context of each host country is unique, every mission operates on the basis of a tailored mandate, which may encompass a broad variety of tasks, including – *inter alia* – advising on institutional reforms, monitoring the implementation of peace agreements, strengthening border management and customs control, supporting law enforcement or armed forces in countering hybrid or other threats, and enhancing the capabilities of local stakeholders through training and capacity-building activities. Against this background, the following sections of this research paper explore the possibilities and risks of integrating AI across the different phases of EU Civilian CSDP Missions – from the initial strategic and operational planning stage to implementation and evaluation phases – with a view to understanding whether, and under what conditions, such technologies may contribute to enhancing their effectiveness, responsiveness, and adaptability to different and ever-evolving challenges. The hypothesis explored here is that AI may further emerge as a technical support tool capable of strengthening the EU's ability to prevent, manage, and respond to crises in a more timely, effective, context-sensitive, and informed manner. At the same time, however, and also in light of the considerations already developed and discussed in the previous sections of this paper, the potential risks that its integration may imply should not be underestimated.

4.1. Strategic and operational planning phases

The planning phase of a Civilian CSDP Mission is a structured and multi-step political, strategic, and operational process, which requires the ability to process vast amounts of data in order to identify an emerging or ongoing crisis warranting prompt action, as well as to decide what measures to adopt in order to address it. It begins as soon as a crisis is identified by the EU at the political and strategic level and is normally based on the Political Framework for a Crisis Approach (PFCA) – i.e., the conceptual framework describing the EU's comprehensive approach to managing a specific crisis, including possible lines of engagement, as well as objectives and expected effects of EU action in the short, medium and long-term. The PFCA informs the development of the Crisis Management Concept (CMC), which provides the basis for subsequent planning by defining the overall end-state, key and *interim* objectives, the means to achieve them, and the principles for measuring success. Depending on the type of intervention outlined in the CMC – whether military or civilian – strategic options may be developed by either the EU Military Staff (EUMS) or by the Civilian Planning and

[86] See *supra* Section 1.

Funded by the European Union

Conduct Capability (CPCC).[87] The latter, in particular, is responsible for the operational planning of Civilian CSDP Missions – namely, for translating the strategic orientation into mission objectives, related mission tasks and expected outputs, as well as the means required to achieve them, including personnel to be deployed and budgetary implications.[88]

In this respect, AI can play a significant role in both the strategic and operational planning of civilian crisis management. While crisis management still tends to be activated primarily in response to ongoing crises, making it inherently reactive, the Civilian CSDP Compact has emphasised the importance for Civilian CSDP Missions to be able to respond 'effectively, flexibly, rapidly and efficiently to evolving external conflicts and crisis'.[89] In other words, if it is true that such measures remain linked to the existence of a crisis, they must nevertheless be capable of addressing emerging and evolving threats, before they fully escalate or consolidate. In this context, AI could contribute to a gradual shift from a primarily *reactive* to a more *anticipatory approach* to crisis management. The use of AI could in fact assist human analysts in processing and analysing large volumes of heterogeneous data. By identifying patterns of instability – such as rising social tensions, disinformation trends, or irregular migration movements – AI could help anticipate crises before their further escalation. This, in turn, could enable earlier and more targeted preventive actions, potentially reducing both human and financial costs associated with large-scale operations.[90] Far from being just science fiction, AI systems are already in use in crisis and disaster risk management to anticipate emergencies. For example, the United Nations Development Programme (UNDP) employs AI-powered tools such as the Crisis Risk Dashboard to analyse historical and near real-time data and identify emerging risks. Similar tools have reportedly been used in Sri Lanka to monitor hate speech, religious violence and macroeconomic issues, as well as in Ecuador to track displacement and migration.[91] The EU Joint Research Centre (JRC) similarly uses AI-enabled tools to analyse satellite data from earth observation systems such as Copernicus, thus supporting early warning mechanisms and evidence-based risk management.[92]

In addition, AI can also strengthen strategic foresight through predictive modelling by simulating the potential consequences of different response options and enabling planners to test alternative intervention strategies

[87] For a comprehensive overview of the different phases comprising the EU crisis management and planning process, see S. Sönmez, E. Dikici, and M. Durak, "EU Crisis Management and Planning Process", *Journal of Military and Information Science*, Vol. 2, No. 4, 2014. See also, EEAS, "CSDP Structure, Instruments and Agencies: Peace, Partnership and Crisis Management Directorate (PCM)", 12 December 2023, available at https://www.eeas.europa.eu/eeas/peace-partnerships-and-crisis-management-directorate-%E2%80%93-pcm_en.

[88] On the operational planning of Civilian CSDP Missions, see B. Loeser, "How to Plan", in G. Faleg (Ed.), "The EU's Civilian Headquarters: Inside the Control Room of Civilian Crisis Management", Chaillot Paper 175, European Union Institute for Security Studies, May 2022, pp. 16-23.

[89] EEAS, "Civilian CSDP Compact: Towards More Effective Civilian Missions", 2023, *cit.*, p. 12.

[90] On the shift from reactive to anticipatory approach in crisis management and humanitarian aid, see M. Lowcock, "Anticipation Saves Lives: How Data and Innovative Financing Can Help Improve the World's Response to Humanitarian Crises", Speech delivery at the London School of Economics, 2 December 2019, available at https://www.unocha.org/publications/report/world/mark-lowcock-under-secretary-general-humanitarian-affairs-and-emergency-relief.

[91] UNDP, "5 Ways AI Can Help Crisis Response Around the World", available at https://www.undp.org/5-ways-ai-can-help-crisis-response-around-world.

[92] European Commission, "AI Approaches for Disaster Risk Management", Science for Policy Brief, JRC142778, June 2025, p. 2. The Global Disaster Awareness and Coordination System, for instance, processes meteorological bulletins to detect early signs of tropic cyclone formation, enabling civil protection authorities to obtain earlier situational awareness and consequently to prioritise mitigation and preparedness actions. Likewise, the Global Human Settlement Layer relies on AI to analyse satellite images and map built-up areas, informal settlements, refugee camps or critical infrastructures, contributing in this way to the assessment of human exposure and vulnerabilities, estimate potential damage from natural hazards and planning of targeted preparedness measures. Destination Earth (DestinE), a digital twin – i.e. a high-fidelity digital replica of the Earth – is currently used to monitor and predict natural and human-induced phenomena with unprecedented precision. It was used during the flash floods that recently occurred in Nigeria in May 2025. For more information on these tools, see, respectively, A. M. Gonçalves, "AI in Action: How the Joint Research Centre Supports Disaster Risk Management", Union Civil Protection Knowledge Network, Newsletter, Issue 17, March 2026, p. 4; D. Barantiev and M. Mastronunzio, "How the Digital Twin Destination Earth Transforms EU Crisis Response", Union Civil Protection Knowledge Network, Newsletter, Issue 17, March 2026, p. 8.

Funded by the European Union

under varying assumptions.[93] This is particularly relevant for crisis management, where planning processes depend on comprehensive situational awareness and forward-looking analysis in highly dynamic, conflict and/or disasters-affected environments. By integrating data from multiple sources, such models can help assess different risk scenarios and support more informed planning of mitigation and response measures. A relevant example is Singapore's "Virtual Singapore", a digital twin that integrates real-time data and advanced 3D modelling to simulate urban dynamics and support operations planning and disaster management.[94]

However, such applications are subject to significant limitations that must be carefully considered. When the degree of availability and accessibility of quality data is affected by an ongoing crisis, instability, weak institutional infrastructures, or limited capacity for systematic data collection, this may compromise the accuracy of AI-generated results.[95] In this sense, incomplete or outdated datasets might fail to capture shifting dynamics on the ground, such as emerging security threats or political instability. In addition, AI systems often struggle when confronted with new situations that fall outside the scope and context of their training datasets. Consequently, there is a concrete risk that they may fail to identify patterns for unprecedented threats or for low-probability and high-impact events.[96] This risk is further compounded when AI systems are trained with data from one context – for example, a specific geographical region – and are then deployed in different operational environments.[97] Taken together, these limitations create a concrete risk that AI-generated outputs may reflect an inaccurate representation of reality, which could lead to responses that are poorly planned, targeted, or untimely. For this reason, it is crucial that human analysts, operators, and decision-makers subject such outputs to different forms of verification including with respect to their contextual relevance.[98] At the same time, however, these limitations do not exhaust the possible relevance of AI during the "planning stage". In fact, even when its contribution to anticipatory analysis and predictive modelling remains circumscribed, AI systems may still offer a more concrete added value in other dimensions of mission design, for instance, in relation to logistical planning and resource allocation.

In this respect, a second area in which AI can meaningfully support the design of Civilian CSDP Missions concerns the optimisation of the deployment of personnel, equipment, and support assets to meet mission requirements and objectives more efficiently.[99] By analysing operational needs and other constraints – such as the availability or lack of personnel and material resources, as well as deployment timelines – AI systems can indeed support more effective allocation strategies. This may help in ensuring that resources are deployed where and when they are most needed.[100] A comparable approach is already employed by UNDP through EVA.ai-powered platform, which matches skilled personnel to field needs by considering expertise, availability, proximity to location, languages and previous experiences.[101] In the context of Civilian CSDP Missions, such possibilities appear particularly relevant since AI systems could support their modularity,

[93] On a study on how AI is used in the field of strategic foresight, albeit not connected to Civilian CSDP Missions, see The World Economic Forum and OECD, "AI in Strategic Foresight: Reshaping Anticipatory Governance", White Paper, November 2025.
[94] OECD, "Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions", OECD Publishing, Paris, 2025, pp. 258-259.
[95] A. Beduschi, "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks", *cit.,* p. 1159;
[96] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, p. 30.
[97] M. Pizzi, M. Romanoff, and T. Engelhardt, "AI for humanitarian action: Human rights and ethics", *International Review of the Red Cross*, 2020, Vol. 102, No. 913, p. 155.
[98] A. Beduschi, "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks", *cit.,* p. 1159;
[99] On how logistical planning and resource allocation work in Civilian CSDP Missions in general, see E. Bellocchi and M. Tabit, "How to Support", in G. Faleg (Ed.), "The EU's Civilian Headquarters: Inside the Control Room of Civilian Crisis Management", Chaillot Paper 175, European Union Institute for Security Studies, May 2022, pp. 31-36.
[100] B. Rajalakshmi, P. Aswini, H. P. Thethi, H. R. Goyal, J. Sravanthi and A. A. Hameed, "Utilizing Artificial Intelligence for Efficient Resource Allocation and Logistics in Humanitarian Aid", *2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI)*, 2024.
[101] UNDP, "5 Ways AI Can Help Crisis Response Around the World", *cit.*

Funded by the European Union

scalability, and adaptability to changing needs on the grounds, in line with the indications in the Civilian CSDP Compact, thus facilitating timely adjustments in mission size and assets.[102]

Also in this case, however, any adoption of AI systems to enhance the operational planning of Civilian CSDP Missions in terms of logistics and resource allocation must take into consideration some inherent limits of AI. Not only can the lack of quality and representative data on operational needs lead to flawed outcomes and reinforce existing biases, resulting in, e.g., unequal resources allocation, but the limited transparency of AI tools can also make it difficult for decision-makers to fully understand or justify allocation choices, particularly in operationally sensitive contexts.[103] These observations are all the more relevant if one considers that, in practice, planning and resources allocation in civilian crisis management rarely concern the internal organisation of missions alone. On the contrary, they are frequently dependent on the capacity of the different actors involved to exchange information, align assessments, and priorities. From this perspective, the potential relevance of AI extends beyond the "merely internal" optimisation of planning choices and also concerns possibilities concerning coordination and interoperability within the EU system and with external partners.

This seems particularly relevant for instance in the framework of civil-military missions, such as the EU SDI GoG,[104] and, in relation to external partners, such as local authorities, other international or regional organisations, or private entities (including, e.g., social media platforms and satellite data providers). In this sense, AI-enabled platforms can indeed facilitate real-time information sharing, harmonise planning and reporting processes, and support joint situational awareness.[105] At the same time, however, the more such forms of coordination come to rely on AI systems, the more evident some underlying issues become. In fact, in crisis-management settings, the collection, and further processing of data rarely occur within a single legal framework. On the contrary, they typically raise complex challenges due to the frequent cross-border nature of crisis management and the fragmentation of legal frameworks across jurisdictions, as different actors may operate under different rules concerning, e.g., respective mandates and data protection regimes.[106] From this perspective, the issue is not only whether AI may facilitate coordination and interoperability, as it also encompasses considerations as to what conditions may facilitate this process through fully lawful practices. In this respect, several guidelines may offer useful practical reference points. For instance, this is the case of the Handbook on Data Protection in Humanitarian Action, an initiative developed under the auspices of the International Committee of the Red Cross (ICRC) which explores – *inter alia* – data protection challenges associated with the use of AI in the humanitarian sector.[107] Similarly, the UN Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data has issued detailed Data Responsibility Guidelines, which were recently updated.[108] In contexts where relevant EU legal frameworks (e.g., the AI Act and the GDPR) may not equally apply for all the actors involved, these documents may provide operational benchmarks capable of orienting more responsible practices in contexts where multiple actors interact under frequently different regimes.[109] A further difficulty, however, lies in the uneven distribution of AI capabilities

[102] EEAS, "Civilian CSDP Compact: Towards More Effective Civilian Missions", 2023, *cit.*, p. 12.
[103] E. X. Wood, "AI and Big Data in Disaster Response: Ethical and Practical Challenges", *Journal of Dynamic Disasters*, Vol. 1, No. 4, December 2025, pp. 3-4, and 7.
[104] The European Union Security and Defence Initiative in support of West African countries of the Gulf of Guinea (EU SDI GoG) is a civilian and military initiative established in 2023 in partnership with Côte d'Ivoire, Ghana, Togo and Benin. It provides tailor support combining military and civilian expertise, based on the needs identified and articulated by the four partner countries. Further information on the mission is available at https://www.eeas.europa.eu/eu-sdi-gulf-guinea_en.
[105] F. E. Öcal and S. Torun, "Leveraging Artificial Intelligence for Enhanced Disaster Response Coordination", *International Journal of Disaster Risk Management*, Vol. 7, No. 1, 2025, p. 240; SAPEA, "Artificial intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, p. 52.
[106] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, p. 52.
[107] Massimo Marelli (Ed.), "Handbook on Data Protection in Humanitarian Action", Third Edition, Cambridge University Press, Cambridge, 2024.
[108] UN OCHA, "Data Responsibility Guidelines", October 2021, revised in January 2025.
[109] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, pp. 45-46.

Funded by the European Union

among those same actors. In this sense, while some entities may rely on advanced AI systems, others may lack comparable tools, and this asymmetry may itself become an obstacle to achieve effective interoperability.[110]

4.2. Implementation phase

AI systems also have the potential to affect in significant ways the manner in which Civilian CSDP Missions are implemented. Since some applications of AI are cross-cutting and therefore potentially relevant across very different kinds of missions, while some others might be more closely dependent on the mission's mandate, operational context, and strategic objectives, the following sections will explore and discuss the possible integration of AI precisely from this perspective. In doing so, the analysis will move from more general uses to progressively more specific tasks, by exploring both potential benefits and risks deriving from the integration of AI into the implementation of Civilian CSDP Missions.

4.2.1. Cross-cutting application of AI to Civilian CSDP Missions

AI may bring several cross-cutting benefits to the implementation of Civilian CSDP Missions in at least three closely related aspects, namely enhancing situational awareness, supporting decision-making and communication processes. AI can indeed significantly enhance operational effectiveness and situational awareness, particularly in complex and fast-changing environments characterised by fragmented information and rapidly evolving conditions. As already noted above, AI systems may assist in analysing data from multiple sources – e.g., from satellites to social media – to generate near-real-time insights, condense large volumes of information into more readily intelligible formats for decision-makers, and detect patterns or signals that may escape human observation.[111]

For instance, image recognition systems and computer vision tools can identify changes in terrain, infrastructure damage, or atypical movements of people and vehicles, potentially indicating security incidents or humanitarian needs that require prompt intervention.[112] In the field of disaster risk management, comparable AI applications have already been deployed with promising results. In Haiti and in the Turkey and Syria earthquakes, AI-enabled open-source tools were used to analyse social media in real-time and identify priority needs.[113] If adapted to Civilian CSDP Missions, similar tools could support closer monitoring of the operational environment and enable faster responses to emerging threats. For instance, AI may be used in monitoring missions to integrate data from different sources to analyse, e.g., movements, potential ceasefire violations, and emerging threats. At the same time, however, the possible contribution of AI at this level remains strictly dependent on the quality, completeness, and timeliness of the data available. As already observed in the previous sections, obtaining high-quality data in contexts affected by ongoing crises, instability, and/or weak institutional infrastructures may be particularly challenging. This problem is further accentuated where reliance is placed on crowdsourced or open-source data, such as content shared through social media, which may be fabricated or contain errors and inaccuracies. People may report incomplete or incorrect information and, in some cases, misleading or unverified content can spread quickly. For this reason, it is essential to adopt robust data validation mechanisms, cross-check information from multiple sources, and combine crowdsourced data with official information whenever possible.[114] Likewise, algorithmic bias may distort

[110] *Ibid*, pp. 52-53.
[111] OECD, "Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions", *cit.,* p. 259-260.
[112] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, pp. 31-33.
[113] A. M. Gonçalves, "AI in Action: How the Joint Research Centre Supports Disaster Management", Union Civil Protection Knowledge Network, Newsletter, Issue 17, March 2026, p. 4; EC, "Artificial Intelligence Approaches for Disaster Risk Management", *cit.*, p. 3.
[114] A. Beduschi, "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks", *cit.,* pp. 1158-1159.

Funded by the European Union

assessments where datasets on which AI systems rely on are not sufficiently representative of local populations or vulnerable groups, potentially leading to instances of discrimination.[115] Finally, in absence of robust cyber-security measures, the reliability of AI outputs can also be compromised by deliberate manipulation, such as poisoning of data or adversarial attacks designed to deceive AI systems (such as image recognition systems) with misleading inputs.[116]

Beyond situational awareness, AI can also support decision-making processes by helping in detecting anomalies, prioritising incidents according to assessed risk levels, and suggesting potential courses of action. This can help mitigate cognitive overload for human operators and promote more timely and informed decisions – provided that these systems rely on high-quality data and are designed to assist, rather than replace, human judgement.[117] In turn, however, decision-makers that rely on AI systems must have appropriate levels of AI literacy to understand/verify the AI-generated output without falling into the trap of automation bias or becoming victims of "hallucinations".[118] The final authority must indeed remain with human decision-makers, especially in high-stakes contexts where decisions can have significant political, legal, or humanitarian consequences.[119] Also in this case, similar AI applications have already been successfully deployed in the field of disaster management. During the 2015 Nepal earthquake, for example, AI systems were used to structure and process vast amounts of unverified and heterogeneous data, enabling the filtering, classification, and geo-location of real-time reports, thereby substantially reducing the cognitive – and informational – burden on human operators. This allowed humanitarian responders to pinpoint critical needs with greater precision and timeliness than traditional methods.[120]

Finally, in operations where communication challenges are frequently pronounced, AI can further contribute through real-time translation, speech recognition, and conversational agents (such as chatbots) capable of facilitating interactions among international staff, local stakeholders and populations. Such tools may arguably reduce the risk of misunderstandings and support the rapid dissemination of alerts and key information to local communities in accessible formats, provided that adequate connectivity and digital infrastructures are available.[121] In Estonia, for example, the PwinPlan project uses AI to deliver EE-ALARM alerts in each recipient's preferred language – based on linguistic data from mobile operators – resulting in a reduction of calls to national emergency numbers and improving both public awareness and efficiency.[122] Similarly, in Australia and New Zealand, the Emergency Situation Awareness platform monitors content on social media to provide its users with real-time information about the impact and scope of an occurring natural disaster.[123] Similar tools could be deployed in Civilian CSDP Missions to facilitate a rapid and effective communication of real-time information in different languages. This, in turn, may also assist to counter and mitigate the spread of misinformation.[124] Precautions shall be adopted, however, to ensure representativeness of local communities (including, e.g., different dialects) and reduce any risk of inaccuracies in automated translation or speech recognition, especially in high-stakes or culturally sensitive contexts.

4.2.2. Specific application of AI tailored to the Civilian CSDP Missions' mandates

[115] *Ibid*, pp. 1159-1161;
[116] M. Pizzi, M. Romanoff, and T. Engelhardt, "AI for Humanitarian Action: Human Rights and Ethics", *cit.*, pp. 155-156.
[117] *Ibid,* pp. 155-157.
[118] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, pp. 31-33.
[119] *Ibid,* p. 46.
[120] *Ibid*, pp. 68-70.
[121] OECD, "Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions", *cit.*, p. 259.
[122] J.-A. Van Vlaenderen, "Clearer, Faster Emergency Warnings: Lessons From Estonia's PwinPLan Project", Union Civil Protection Knowledge Network, Newsletter, Issue 17, March 2026, p. 21.
[123] Further information is available at https://www.csiro.au/en/research/technology-space/ai/Emergency-Situation-Awareness.
[124] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, p. 23.

Funded by the European Union

As mentioned before, AI can also be configured and applied in distinct ways depending on the mission's mandate, operational context, and strategic goals. Whether in crisis response, conflict prevention, rule-of-law support, investigations of different nature, border management, or security sector reforms, AI may assume an enabling and support function. The examples that follow are meant to illustrate AI-based tools may assume different roles depending on the mission type, its specific mandate, and the specificities of the environments in which they are deployed.

(a) Promoting institutional reforms

Civilian CSDP Missions generally act under a specific mandate to facilitate institutional reforms – as in the case of EUAM IRAQ,[125] EUAM RCA,[126] EUAM UKRAINE,[127] and EUPOL COPPS,[128] which have been established to support security and/or justice sector reforms, or EULEX KOSOVO,[129] which was originally tasked to support the re-establishment of governmental functions in a post-conflict setting. In such contexts, AI may bring significant benefits, by supporting, e.g., institutional reforms while also helping rebuild trust between local populations and national institutions.

Institutional reforms aimed at strengthening effectiveness and accountability can benefit significantly from the integration of AI, provided that its use remains consistent with missions' mandates and relevant EU and international standards on human rights, democracy, and the rule of law. In contexts where institutional structures are weak or fragmented, including those in the security and justice sectors, AI can – other than support more efficient allocation of personnel and resources – improve coordination among agencies or other institutions, and contribute to the development of more coherent and resilient administrative systems. In this sense, it could also support benchmarking activities to identify indicators to more concretely assess progresses at the local level. At the same time, AI-driven tools can enhance oversight capacities by identifying irregularities, detecting risks of, e.g., corruption, and flagging potential abuses of power through the analysis of large and complex dataset and the assessment of integrity risks.[130] This can play a key role in reinforcing institutional integrity and rebuilding public trust, particularly in fragile or transitional settings. At the same time, however, such uses also entail risks related to false positive or inaccurate flagging of suspicious activities,

[125] The European Union Advisory Mission in Support of Security Sector Reform in Iraq (EUAM Iraq) was launched in October 2017 in response to a request by the Iraqi government to support the achievement of lasting peace, stability and security in the region following the defeat of Da'esh in 2015. The mission is tasked with offering strategic advice to the Iraqi security sector. Further information is available at https://www.euam-iraq.eu.

[126] The European Union Advisory Mission in Central African Republic (EUAM RCA) was established in 2019 with the mandate to provide strategic advice to the Central African Republic Ministry of Interior and Public Security and to the Internal Security Forces to support the establishment of coherent and accountable security providers under full national ownership. Further information is available at https://www.eeas.europa.eu/euam-rca_en.

[127] The European Union Advisory Mission for Civilian Security Sector Reform in Ukraine (EUAM UKRAINE) was originally deployed in 2014 to advise State security bodies on security, police, judiciary, prosecution, anti-corruption and human rights. Since 2022, the Mission provides support to law enforcement agencies to facilitate the flow of refugees from Ukraine to the neighbouring Member States, the entry of humanitarian aid into Ukraine, and the investigation and prosecution of international crimes. Further information is available at https://www.euam-ukraine.eu/.

[128] Initially established in 2006 as a Police Advisory Mission, the European Union Coordinating Office for Palestinian Police Support (EUPOL COPPS) has the mandate to assist the Palestinian Authority in building its institutions with a focus on security and justice sector reforms. Further information is available at https://eupolcopps.eu.

[129] The European Union Rule of Law Mission in Kosovo (EULEX KOSOVO) was launched in 2008 with the mandate to support the relevant rule of law institutions in Kosovo in their path towards increased effectiveness, sustainability, multi-ethnicity and accountability, free from political interference and in full compliance with international human rights standards and best European practices. Currently EULEX KOSOVO is still active, with the mandate to monitor activities and exercise limited executive functions, including second tier security responder. Further information is available at https://www.eulex-kosovo.eu.

[130] OECD, "Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions", *cit.*, pp. 213-217.

Funded by the European Union

which may unjustly target individuals or institutions, undermine due process, or erode trust if not accompanied by robust human oversight and verification mechanisms.[131]

By enabling evidence-based assessments, AI can also support reform processes that are better tailored to the needs of different population groups, including vulnerable or marginalised communities. Particularly relevant, in this sense, are the studies conducted by the OECD, which highlight how AI is increasingly used in the exercise of governmental functions worldwide, delivering tangible benefits across multiple domains.[132] AI has in fact the potential to facilitate the automation and personalisation of internal processes and public services, improve decision-making and forecasting, strengthen fraud detection, and enhance the skills and productivity of public servants. More broadly, it can act as a strategic enabler of more effective, innovative, participatory, and trustworthy governance. Through advanced data analytic capabilities, AI allows governments to design more responsive policies, optimise service delivery, and continuously monitor performance, thereby addressing evolving societal needs with greater precision.[133] In the context of Civilian CSDP Missions, AI-enabled tools could assist missions and local stakeholders in analysing large volumes of administrative, policy, legislative and judicial data and identify gaps in service delivery, recurrent inefficiencies, or areas where current practices remain inconsistent with reform objectives. Of course, also in this respect, the quality and representativeness of data remain critical, since incomplete, outdated, or biased datasets may lead to distorted assessments or policy recommendations potentially reinforcing existing inequalities or institutional weaknesses rather than addressing them.[134] Furthermore, risks related to opacity in AI systems may limit transparency and accountability in public decision-making, especially where automated or semi-automated processes are not sufficiently explainable.[135]

Finally, Civilian CSDP Missions should also provide specific training on how to integrate AI in different institutions in compliance with international human rights – or other – standards and the rule of law, with the view of gradually introducing AI solutions that may further increase the effectiveness, efficiency and accountability of such institutions in the long run. For example, in the field of the justice sector reform, where AI tools have proved to be useful to assist in digitalising and organising legal documents, enabling faster case processing and improved access to justice,[136] Civilian CSDP Missions could integrate AI in their capacity building activities, by providing training to national officers, judges, and prosecutors on how to effectively use AI in their work in full compliance with international, regional and domestic law. Similar training activities have already been provided by UNESCO.[137] In the security sector, where AI may bring some important benefits in, e.g., resource allocation and strategic planning, data analytics and digital forensics,[138] *ad hoc* training courses should be organised in order to ensure that security personnel not only acquire the technical skills to operate AI systems, but also develop a critical understanding of their limitations. Training should particularly address key technical, ethical and social issues associated with AI – including, e.g., algorithmic

[131] *Ibid*, pp. 217-218. From the perspective of the AI Act, similar uses should be considered with caution and only as preliminary indicators. In this sense, they may fall within the category of "high-risk" systems under Art. 6 and Annex III AI Act or, in the most problematic configurations, even under that of "prohibited practices" as per Art. 5 AI Act. See also Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", *cit.*, pp. 37-45.
[132] OECD, "Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions", *cit.,* pp. 26-27.
[133] *Ibid*. On the use of AI in policy evaluation, see also pp. 221-227.
[134] *Ibid*, pp. 35-37.
[135] *Ibid*, p. 37.
[136] The University of Bologna, together with other partners, has launched Project ADELE – Analytics for Decision of Legal cases – an EU funded project which relies on data science, ML and natural language processing techniques to analyse datasets of judgement and develop methods to extract knowledge from judicial decisions and engage in outcomes predictions, supporting legal research and decision making processes in the judiciary.
Further information is available at https://site.unibo.it/adele/en/project.
[137] See, for instance, UNESCO, "Global Toolkit on AI and the Rule of Law for the Judiciary", 2023; and UNESCO, "Guidelines for the Use of AI Systems in Courts and Tribunals", 2025.
[138] Cf. EUROPOL, "AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement", Observatory Report, 2024.

Funded by the European Union

bias and opacity – to prevent misuse or overreliance on automated systems in sensitive decision-making processes.[139] These risks are especially relevant in operational contexts where inaccurate or incomplete AI-generated insights may directly affect security decisions on the ground. Moreover, such training should be tailored to the specific needs of the host countries. Some applications of AI in law enforcement – e.g., predictive policing and the use of biometric technologies – raise important concerns *vis-à-vis* human rights, particularly with regard to privacy and data protection, the risk of mass surveillance, potential biases and discrimination.[140] These systems may produce false positives or false negatives, leading to unjust profiling, misidentification of individuals, or disproportionate targeting of specific groups, thereby undermining procedural fairness and public trust in law enforcement agencies. Moreover, AI opacity further complicates the situation by making it difficult to understand or challenge how decisions are reached.[141] Where the host country relies – or intends to rely – on AI systems for such purposes, Civilian CSDP Missions should carefully train law enforcement agencies in order to ensure that any potential use of – *inter alia* – "high-risk" AI systems that do not fall under the category of "prohibited practices" is aligned with relevant legal frameworks.[142]

(b) Monitoring the enforcement of peace agreements

In missions tasked with the monitoring of boundary lines and the enforcement of peace agreements, such as EUM ARMENIA[143] and EUMM GEORGIA,[144]AI can further enhance situational awareness on the ground and existing early warning systems.[145] As mentioned above, AI can predict, to some extent, the likelihood of an emerging crisis or risks of escalation – e.g., by monitoring and analysing online and local news – allowing Civilian CSDP Missions to focus on preventive measures, while bearing in mind the limitations already highlighted with respect to data quality, potential bias, and the risk of inaccurate or misleading predictions. Likewise, in post-conflict situations, AI may help predict whether there is the risk of breaches of peace agreements – although such assessments should always be complemented by human expertise.[146] Similar initiatives already exist. In this sense, the Armed Conflict Location & Event Data (ACLED), for instance, is an independent and impartial global monitoring project that collects, analyses and maps data on conflict and protests to identify, understand and track patterns and trends in conflict and crisis situations around the globe.[147]

In Civilian CSDP Missions, AI can be used to integrate real-time data from, e.g., drones, satellites, sensors, and open-source intelligence, to provide timely analysis of movements or unusual activities along ceasefire

[139] *Ibid*, pp. 31-36.
[140] See, e.g., F. P. Levantino, "Assessing the Risks of Emotion Recognition Technology in Domestic Security Settings: What Safeguards Against the Rise of 'Emotional Dominance'?", in E. Kosta, D. Hallinan, P. De Hert and S. Nusselder (Eds.), "Data Protection and Privacy (Vol. 17): To Govern or to Be Governed, That is the Question", Hart Publishing, 2025, pp. 225-257.On the legal, ethical and societal implications of predictive policing, see also R. Van Brakel, "Legal, Ethical, and Social Issues of AI and Law Enforcement in Europe: The Case of Predictive Policing", in N. A. Smuha, "The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence", Cambridge University Press, Cambridge, 2025, pp. 367-382.
[141] OECD, "Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions", *cit.,* pp. 261-263.
[142] More broadly, see also Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", *cit.*, pp. 46-53.
[143] The European Union Mission in Armenia (EUM ARMENIA) was launched in 2023 with the mandate to observe and report the situation on the ground, contributing to human security in conflict-affected areas and supporting confidence building between Armenia and Azerbaijan. Further information is available at https://www.eeas.europa.eu/euma_en?s=410283.
[144] The European Union Monitoring Mission in Georgia was launched in 2008 to monitor compliance by Georgia and Russia with the peace agreement. It patrols in areas adjacent to the South Ossetian and Abkhazian Administrative Boundary Lines in order to observe the situation on the ground, report incidents, and contribute with its presence to improving the security situations. Further information is available at https://www.eumm.eu.
[145] G. Schvitz, C. Corbane, C. Gentile, A. Bergmaier and A. Vivancos, "The Future of Conflict Early Warning: New Technologies and Policy Impact", *European Commission JRC Workshop Proceedings*, 2025.
[146] O. B. Olaide, A. K. Ojo, "A Model for Conflicts' Prediction using Deep Neural Network", *International Journal of Computer Applications*, Vol. 183, No.29, 2021.
[147] Further information on ACLED is available at https://acleddata.com/about-acled.

Funded by the European Union

lines, potential violations, or emerging threats, enabling faster response and de-escalation.[148] AI systems can detect early signals of instability also by analysing news data on the media and predict internal turmoil or coups – though they may remain susceptible to manipulation, disinformation, and context-related misinterpretation.[149] In addition, AI can also be used to identify and notify instances of hate speech online or the presence of violent language, thereby preventing possible escalations, provided that adequate standards are in place to avoid disproportionate interferences with freedom of expression and to ensure transparency in content moderation.[150]

(c) Enhancing border management and customs control

In missions focused on improving border management systems, such as EUBAM LIBYA[151] or EUBAM RAFAH,[152] if used in compliance with the relevant international framework and in particular with human rights standards, AI can improve both efficiency and security while supporting humanitarian objectives.[153] The EU and its Member States have already employed some AI tools in their efforts to strengthen border control and mitigate security risks related to transnational crimes – including terrorism and illicit trafficking. At the same time, several of these applications require particular caution from the perspective of, e.g., the AI Act, since, depending on their intended purpose and use, they may fall within the category of "high-risk" AI systems, or, in more problematic cases be affected by the prohibitions laid down in Article 5 AI Act. Notably, certain AI tools may be relevant for border control and border security in four main areas: (a) biometric verification and/or identification (through automated fingerprint and face verification or recognition);[154] (b)

[148] A. W. K. Mandokhail, "The Transformative Role of Artificial Intelligence in Conflict Resolution and Peacekeeping", *NUST Journal of International Peace and Stability*, Vol. 7, No. 1, 2024, p. 107.
[149] G. Schvitz, C. Corbane, C. Gentile, A. Bergmaier and A. Vivancos, "The Future of Conflict Early Warning: New Technologies and Policy Impact", *cit.*, p.10.
[150] On the use of AI and machine learning techniques to prevent and counter hate speech, racism and xenophobia online, see M. Finck, "Artificial Intelligence and Online Hate Speech", Centre on Regulation in Europe, Issue Paper, January 2019; and EU FRA, "Online Content Moderation: Current Challenges in Detecting Hate Speech", Report, Vienna, 2023.
[151] The European Union Integrated Border Management Assistance Mission in Libya (EUBAM Libya) was established in 2013 to support the capacity of Libyan authorities to enhance the security of their land, sea and air borders in the short term and to develop a broader Integrated Border Management (IBM) strategy in the long term. Further information is available at https://www.eeas.europa.eu/eubam-libya_en.
[152] The European Union Border Assistance Mission for the Rafah Crossing Point was launched in 2005 to monitor border operations, support coordination among parties, and assist the Palestinian Authority in managing the crossing effectively, contributing to the stability and trust in the region. Further information is available at https://www.eeas.europa.eu/eubam-rafah_en.
[153] More broadly, when uses of AI in the context of Civilian CSDP Mission intersect with humanitarian actions, they should be conceived and implemented bearing in mind and ensuring that they do not undermine the principles of humanity, neutrality, impartiality and independence. Cf., e.g., EEAS, "EU Concept on Effective Civilian-Military Coordination in Support of Humanitarian Assistance and Disaster Relief", EEAS(2018) 1293 Rev. 5, Council doc. 5536/19, 30 January 2019.
[154] The EU's centralised information systems for borders and security are increasingly incorporating biometric technologies for the purpose of identity verification or identification. For example, automated fingerprint identification technology is increasingly being used in numerous information systems (including the Schengen Information System, the European Dactyloscopy Database and the Visa Information System). Cf. C. Dumbrava, "Artificial Intelligence at EU Borders: Overview of Applications and Key Issues", European Parliamentary Research Service, 2021, pp.11-15. From the perspective of the AI Act, it is important to distinguish biometric verification or authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be, from remote biometric identification systems. The latter are included among high-risk AI systems under Annex III, point 1(a), whereas biometric verification systems are expressly excluded from that specific category when used only for identity confirmation – with some exceptions. In addition, AI systems intended to detect, recognise or identify natural persons in the context of migration, asylum or border-control management are listed as high-risk under Annex III, point 7(d), with the exception of verification of travel documents. The possible use of real-time remote biometric identification systems in publicly accessible spaces for law-enforcement purposes is instead subject to the specific prohibition and limited exceptions set out in Article 5 AI Act.

Funded by the European Union

emotion recognition;[155] (c) algorithmic risk assessment;[156] (d) migration monitoring, analysis and forecasting.[157] Similar applications could be adopted also within the framework of Civilian CSDP Missions to support States in border management, provided that such applications are in compliance with international human rights law and other relevant standards.[158] AI can also be used to optimise the allocation of border personnel and surveillance assets, ensuring coverage in high-risk areas. Finally, AI can also be applied in customs control, for instance in the field of goods inspections and screening of cargo, containers, parcels and luggage. This is particularly relevant also in the fight against illicit trafficking.[159]

Whereas there are important benefits from relying on AI systems in the context of border control – e.g., increased capacity to detect fraud and abuses, better and timely access to relevant information for decision-makers – it should be kept in mind that some of these AI applications – notably, biometric identification systems[160] – have already raised several concerns, especially in relation to accuracy, potential bias, and the risk of disproportionate interference with fundamental rights. Despite significant advances in biometric identification tools, indeed, their accuracy remains uneven and highly dependent on both the specific technology used and the context in which it is deployed. Even well-established methods of identity verification face limitations, particularly during data collection, where factors like age or environmental conditions may

[155] Emotion recognition technologies represent one of the most controversial uses of AI. Whereas there are currently no emotion-detection systems deployed at EU borders, a number of EU-funded projects are exploring such technologies for the purpose of enhancing border control. C. Dumbrava, "Artificial intelligence at EU Borders: Overview of Applications and Key Issues", *cit.*, pp.16-18. On some of the risks associated with the use of this technology in law enforcement, see F. P. Levantino, "From Identity to Emotional Dominance? 'Early Warnings' on Emotion Recognition Uses by Police Forces", in N. Menéndez González and G. Mobilio (Eds.), "Next Democratic Frontiers for Facial Recognition Technology (FRT)", Springer, 2025, pp. 126-157; F. P. Levantino, "Assessing the Risks of Emotion Recognition Technology", *cit*. Under the AI Act, AI systems intended to be used for emotion recognition are listed among high-risk AI systems under Annex III, point 1(c), insofar as their use is permitted under Union or national law. Article 5 AI Act prohibits emotion-recognition systems in the areas of workplace and educational institutions, except where their use is intended for medical or safety reasons. Although this prohibition does not specifically target border management, the classification of emotion recognition as high-risk confirms the need for particular caution in contexts involving migrants, asylum seekers or other persons in vulnerable situations, especially in light of the contested scientific reliability of such tools and their potential impact on dignity, privacy and non-discrimination.

[156] AI algorithms are also used to identify unknown persons of interest through "algorithmic profiling" on the basis of specific data-based risk profiles. Algorithmic profiling for assessing individual risks of security and irregular migration is currently being developed in the context of the Visa Information System and the European Travel Information Authorisation Systems. C. Dumbrava, "Artificial Intelligence at EU Borders: Overview of Applications and Key Issues", *cit.*, pp.18-20. It should be noted, however, that the use of algorithmic profiling may lead to unlawful profiling, if not done in compliance with the relevant international standards. *Ibid*, pp. 29-30. In Annex III point 7(b) of the AI Act AI systems used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, to assess risks posed by natural persons who intend to enter or have entered the territory of a Member State – including security risks, risks of irregular migration or health risks – qualify as high-risk AI systems, in so far as their use is permitted under Union or national law. Moreover, Article 5 AI Act prohibits AI systems used to make risk assessments of natural persons in order to assess or predict the risk of committing a criminal offence where such assessment is based solely on profiling or on personality traits and characteristics, while allowing systems that support human assessment where this is already based on objective and verifiable facts directly linked to criminal activity.

[157] The European Asylum Support Office is currently using an early warning and forecasting system to predict the number of asylum applications. The European Commission and other EU Agencies are currently exploring other applications in this field, including in the context of the development of the Frontex EUROSUR system and the Europol Innovation Hub. Cf. C. Dumbrava, "Artificial Intelligence at EU Borders: Overview of Applications and Key Issues", *cit.*, pp. 20-22.

[158] See Council of Europe (Steering Committee for Human Rights), "Handbook on Human Rights and Artificial Intelligence", *cit.*, pp. 54-58.

[159] See N. Jaccard, T.W. Rogers, E.J. Morton, L.D. Griffin, "Automated Detection of Smuggled High-Risk Security Threats Using Deep Learning", *7th International Conference on Imaging for Crime Detection and Prevention (ICDP 2016)*, Madrid, 2016; I. Mademlis, M. Mancuso, C. Paternoster, S. Evangelatos, E. Finlay and J. Hughes *et al.*, "The Invisible Arms Race: Digital Trends in Illicit Goods Trafficking and AI-Enabled Responses", *IEEE Transactions on Technology and Society*, Vol. 6, No. 2, 2025.

[160] Currently, automated biometric systems in this field can be used for two main purposes: (1) biometric verification (or authentication) of identity; (2) biometric identification. C. Dumbrava, "Artificial Intelligence at EU Borders: Overview of Applications and Key Issues", *cit.,* pp. 11-16. See also the considerations in footnotes nn. 153 ff., *supra*.

Funded by the European Union

affect their reliability over time.[161] Similarly, the performance of facial recognition systems in real-world settings is closely dependent on image quality and the effectiveness of matching capabilities, which in turn depend on the quality and representativeness of training datasets.[162] In this sense, relying on AI systems for facial recognition raises significant concerns particularly in relation to algorithmic bias, discrimination,[163] as well as for the data protection and privacy implications of their training and use.[164] Moreover, even technically accurate systems may still pose significant risks, especially since biometric data may reveal sensitive data such as the ethnic origin of the identified person.[165] Finally, concerns also persist regarding the scientific validity of emotion recognition systems, and their potential adverse impact on fundamental rights.[166]

(d) Countering new and emerging threats

The increasing use of hybrid strategies and operations by both States and non-State actors poses increasing threats to security and shared democratic values. This has led the EU to progressively develop a framework on countering hybrid threats: initially based on the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, and later reinforced through the Strategic Compass, which called for the development of the EU Hybrid Toolbox and the EU Hybrid Rapid Response Team.[167] Within this framework, these last two initiatives, in particular, are meant to support coordinated and cross-sectoral responses to complex hybrid campaigns through preventive, cooperative, stability-building, restrictive, and other measures. It is no surprise, therefore, that the EU has included countering hybrid threats among the tasks of Civilian CSDP Missions. So far, EUPM MOLDOVA appears as the only Civilian CSDP Mission with an explicit mandate to support reforms in civilian security sector governance, with a strong emphasis on building resilience against hybrid threats like disinformation, cyberattacks and foreign interferences.[168] It may be expected that other missions will be tasked with a similar mandate.[169]

In order to support host countries in tackling hybrid threats, here too, Civilian CSDP Missions can rely on AI tools to analyse vast volumes of data and spot patterns indicative of hybrid attacks, while being aware of the challenges associated with the interpretation of complex and often ambiguous data and the possibility of false

[161] *Ibid,* pp. 23-24.
[162] *Ibid,* pp. 24-25.
[163] *Ibid,* pp. 26-28. See also M. Forti, "Addressing Algorithmic Errors in Data-Driven Border Control Procedures", *German Law Journal*, Vol. 25, 2024.
[164] For a comprehensive analysis of several concerns associated with the use of facial recognition technology see – *inter alia* – Pete Fussey and Daragh Murray, "Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence", Oxford University Press, 2025.
[165] C. Dumbrava, "Artificial Intelligence at EU Borders: Overview of Applications and Key Issues", *cit.,* pp. 28-31.
[166] *Ibid,* pp. 25-26.
[167] See, respectively, European Commission-High Representative of the Union for Foreign Affairs and Security Policy, "Joint Framework on Countering Hybrid Threats: A European Union Response", JOIN(2016) 18 final, 6 April 2016; European Commission-High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats", JOIN(2018) 16 final, 13 June 2018; Council of the EU, "A Strategic Compact for Security and Defence", March 2022; Council of the EU, "Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns", 10016/2022, 21 June 2022; Council of the EU, "Hybrid Threats: Council Paves the Way for Deploying Hybrid Response Teams", Press Release, 21 May 2024. See also, Council of the EU, "Council Adopts Conclusion on Advancing the EU's Capacity to Counter Hybrid Threats", Press Release, 16 March 2026.
[168] The EU Partnership Mission in Moldova was inaugurated in 2023 with the mandate to contribute to the consolidation of the resilience of the country, through strategic advice and operational support to consolidate the internal security sector of the Republic of Moldova. EUPM Moldova is the first EU Civilian CSDP Mission focused on the field of fighting hybrid threats, cyber attacks, foreign informational manipulation and interference.
Additional information is available at https://www.eeas.europa.eu/eupm-moldova_en.
[169] K. Mustasilta, T. Karjalainen and T. Tammikko, "The European Union's Crisis Management Efforts: Evolution Amid a Shifting International Order and the War in Ukraine", Briefing Paper 427, Finnish Institute of International Affairs, December 2025.

Funded by the European Union

correlations. For example, to enhance the detection of hybrid threats, the European Commission's JRC is currently leveraging AI and existing open-source intelligence to compile a dataset of hybrid threat incidents, which may in turn help to identify adversary patterns and connect seemingly unrelated events.[170] In a similar manner, AI also offers important opportunities for mitigating and countering disinformation: by analysing online content, AI systems can help Civilian CSDP Missions to detect and respond to narratives that may undermine the legitimacy of institutions or exacerbate tensions on the ground.[171] In this respect, however, great caution should guide any follow-up initiatives, since in this context the distinction between coordinated manipulation, legitimate political contestation, and ordinary public debate may be difficult to draw – especially in fragile or polarised environments – thus posing risks *vis-à-vis* the right to freedom of expression and its facets related to the freedom to access to information.

(e) Providing training and capacity-building activities

Finally, training and capacity building activities play a crucial role in Civilian CSDP Missions, especially in those tasked to enhance, e.g., law enforcement capabilities, such as the EUCAP SOMALIA[172] and EUPOL COPPS.[173] Also in this context, AI can improve capacity-building efforts. Adaptive learning platforms powered by AI can tailor training programs for law enforcement officers based on individual performance, an adjustable learning pace, and skill gaps identification. In addition, AI-enabled simulation tools, including augmented and virtual reality systems, can create realistic training environments for crisis response, counterterrorism, or crowd control, allowing law enforcement and civilian security personnel to simulate decision-making processes in complex scenarios without real-world risks.[174] At the same time, the use of AI in training and capacity-building activities entails a number of challenges already highlighted above in relation to its integration in the training "life cycle".[175]

4.3. Evaluation phase

One of the persistent challenges in crisis management is assessing whether interventions have achieved their intended objectives and ensuring that lessons are effectively captured and transferred across missions. Currently, evaluations are often hindered by fragmented data, limited information, and the complexity of attributing long-term changes to specific mission activities, particularly in environments characterised by political volatility and weak institutional capacity. Additionally, knowledge transfer and institutional learning practices are unevenly applied across missions, further complicating effective evaluation.[176]

---

[170] See F. Bosso and S. Ruberto, "Ontology Learning for Hybrid Threats", EC(JRC), 2025.
[171] SAPEA, "Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report", *cit.*, pp. 63-65.
[172] The European Union Capacity Building Mission in Somalia (EUCAP SOMALIA) has been assisting Somalia since 2016 in order to support the development of the Somali maritime security and police sectors, as well as promoting the rule of law. Further information is available at https://www.eeas.europa.eu/eucap-som_en.
[173] The European Union Coordinating Office for Palestinian Police Support (EUPOL COPPS) was initially established in 2006 as a Police Mission comprising a Police Advisory Section. Its mandate was further expanded to also include the rule of law section. In 2008 a Rule of Law Section was added. EUPOL COPPS (the EU Coordinating Office for Palestinian Police Support) assists the Palestinian Authority in building its institutions with a focus on security and justice sector reforms. This support is placed under Palestinian ownership and is delivered in accordance with European and international standards. Ultimately, the Mission's objective is to improve the safety and security of the Palestinian people. Further information is available at https://eupolcopps.eu/.
[174] See European Defence Agency, "The 2023 EU Capability Development Priorities: To Be Ready", 2023, p. 27.
[175] See *supra* Section 3.
[176] See V. Savoranta, "End of Mission: Reinventing Closure and Transition Processes in EU Civilian CSDP", SIPRI Research Policy Paper, February 2026.

Funded by the European Union

The 2023 Civilian CSDP Compact emphasised the need for a more regular and structured performance assessment, as well as for a more systematic approach to knowledge management and organisational learning built on lessons learned from past missions.[177] On this basis, starting from 2024, the EEAS has taken steps to strengthen monitoring and evaluation practices, integrating more consistent performance reviews and reinforcing follow-up mechanisms on recommendations.[178] At the same time, efforts have been made to improve the management of institutional knowledge, notably by revising the lessons learned process. Since the creation of CSDP Missions in 2003, indeed, the EU has recognised the importance of learning from its own experience to improve capacities and the effectiveness of its interventions.[179] However, institutional learning in this field remains only partially systematised, relying not only on formal procedures – e.g., working groups, shared evaluations, workshops and writing reports – but also on informal networks and practices – e.g., personal relationships, corridor talk and information-sharing – which vary across missions.[180] Moreover, the sensitive nature of many CSDP Missions hampers the broad dissemination of lessons within EU structures.[181] Thus, while these recent developments indicate tangible progress, implementation remains uneven across missions and challenges persist in ensuring that identified lessons are effectively translated into operational and strategic adjustments.

CSDP lesson learning practices generally focus on three areas: collecting lessons, knowledge exchange, and training efforts. Lessons from missions and operations are stored in a database to produce annual reports, but contributions are often inconsistent and focus more on successes than failures. Knowledge exchange occurs through conferences, workshops, and seminars, but fragmentation and busy schedules make effective sharing difficult. Moreover, the lessons identified in evaluations are supposed to inform training activities, but the above-mentioned challenges complicate their integration into training programs.[182]

In this respect, AI can be used to provide a more nuanced and evidence-based understanding of mission outcomes. For example, AI systems can track trends in crime rates, judicial efficiency, or public trust in institutions, helping to determine, e.g., whether capacity-building efforts are having a lasting effect. This, in turn, may be used to inform mandate reviews and adjustments, ensuring that missions are adapted to evolving conditions and that resources are used effectively. Furthermore, with the view to ensure sustainability beyond the formal end of a mission, AI can also be used to identify recurring operational patterns, best practices, and structural weaknesses across different missions.[183] This could help address a well-documented limitation in Civilian CSDP Missions practice, namely the difficulty of transferring lessons learned across geographically and contextually diverse missions with different mandates and operating environments. More systematic use of AI-enabled analysis could therefore support a more cumulative approach to institutional learning and improve coherence across different missions. At the same time, any use of AI in this context must take into account the well-known limitations related to data availability and interoperability, as mentioned above, as well as the intrinsic limits of AI systems in capturing the full complexity of local political, social, and cultural dynamics. Indeed, as it has been already stressed, findings and patterns identified through AI are not always accurate nor necessarily valid in different contexts. As a result, AI-generated findings and patterns should be

[177] EEAS, "Civilian CSDP Compact: Towards More Effective Civilian Missions", 2023, *cit.*, p. 21.
[178] *Ibid.*
[179] E. Dari, M. Price, J. Van Der Wal, M. Gottwald, N. Koenig, "CSDP Missions and Operations: Lessons Learned Processes", European Parliament Directorate-General for External Policies (Policy Department), 2012, p. 17.
[180] See, diffusely, E. Dari, M. Price, J. Van Der Wal, M. Gottwald, N. Koenig, "CSDP Missions and Operations: Lessons Learned Processes", *cit.;* and N. Bremberg and E. Hedling, "EU Missions and Operations: Practices of Learning Lessons in the CSDP", in N. Bremberg, A. Danielson, E. Hedling and A. Michalski (Eds), "The Everyday Making of EU Foreign and Security Policy: Practices, Socialization and the Management of Dissent", Edward Elgar, 2022, pp. 131-148.
[181] N. Bremberg and E. Hedling, "EU Missions and Operations: Practices of Learning Lessons in the CSDP", *cit.,* p. 142.
[182] *Ibid*, pp. 142-144.
[183] A. E. Juncos, "How to Learn", in G. Faleg (Ed.), "The EU's Civilian Headquarters: Inside the Control Room of Civilian Crisis Management", Chaillot Paper 175, European Union Institute for Security Studies, May 2022, pp. 51-57.

Funded by the European Union

interpreted with caution and complemented by qualitative analysis and human judgement, particularly when informing strategic decisions or assessing mission success across highly heterogeneous contexts.

5. Concluding remarks and recommendations

In the light of the foregoing analysis, the integration of AI into EU Civilian CSDP Missions emerges neither as an inherently desirable development nor as a possibility to be rejected *a priori*. As illustrated throughout this research paper, indeed, AI systems – including, increasingly diffused general-purpose and generative AI tools – have the potential to substantially enhance the effectiveness, adaptability and responsiveness of civilian crisis management, both in the realm of training and in operational deployment. Their capacity to process large volumes of heterogeneous data, support scenario-building, generate descriptive, predictive, and prescriptive outputs, and enable adaptive learning can contribute to more tailored, realistic, and forward-looking training environments, while also strengthening evidence-based decision-making across the different phases of mission planning, implementation, and evaluation.

In this respect, training activities emerge as a particularly relevant domain for AI integration, given the flexibility, scalability, and adaptability of such systems in supporting more interactive, learner-centred, and experience-based approaches, while still requiring careful human oversight, as well as careful consideration even from a pedagogical perspective in order to critically assess whether the use of AI genuinely improves learning or only renders it more "technological". More broadly, considering that EU Civilian CSDP Missions constitute one of the EU's flagship instruments for promoting stability, strengthening resilience, and supporting partner countries through non-military means, the possible integration of AI in this context must be understood in light of the wide range of objectives they pursue – ranging from conflict prevention and crisis management to post-conflict stabilisation. In this sense, AI may indeed emerge as a technical support tool capable of enhancing the EU's ability to prevent, manage, and respond to crises in a more timely, informed, and context-sensitive manner across the entire mission lifecycle while contributing to its objectives in a flexible and effective manner.

At the same time, however, these opportunities cannot be considered independently from the structural limitations and risks that accompany the use of AI systems in this domain. As highlighted throughout this analysis, their performance is intrinsically dependent on the quality, representativeness, and integrity of the data on which they are trained and operate. In line with the well-known "garbage in, garbage out" principle, incomplete, outdated, or biased datasets may lead to inaccurate or discriminatory outputs, leading to particularly serious consequences. Moreover, the opacity and limited interpretability of many AI systems – often described as "black boxes" – further complicate the ability of users to understand, verify, and contest their outputs. This challenge is further exacerbated in the case of generative AI, whose outputs may appear plausible and coherent while being factually incorrect or entirely fabricated. Additional risks stem from vulnerabilities to manipulation, or from data poisoning or adversarial attacks, which may further undermine the reliability and security of such systems and their use.

Beyond these technical and structural constraints, the way in which AI systems are used in practice raises equally important concerns. Limited levels of AI literacy among personnel or end-users may hinder effective human oversight, thereby increasing the likelihood of phenomena such as automation bias or uncritical reliance on system outputs. In this respect, even where regulatory frameworks (e.g., the AI Act) require human supervision, the absence of adequate expertise may reduce such safeguards to a merely formal requirement. These dynamics are particularly relevant in both training and operational environments, where overreliance on AI tools may distort learning processes, oversimplify complex realities, or negatively affect decision-making, ultimately generating risks for both mission personnel and local populations.

Against this background, the integration of AI into Civilian CSDP Missions should not be understood as a purely technical detail, but as part of a broader transformation requiring appropriate governance frameworks, tailored safeguards, and forms of cultural and organisational adaptation. In fact, ensuring compliance with

Funded by the European Union

existing EU legal and policy frameworks – including the risk-based approach introduced by the AI Act, as well as data protection regimes such as the GDPR and EUDPR – constitutes a necessary, but not sufficient, condition. These frameworks introduce important obligations concerning – *inter alia* – risk management, data governance, transparency, human oversight, and accountability, particularly with regard to high-risk AI systems. However, their effective implementation depends on the capacity of both providers and deployers to operationalise these requirements in practice, something which in the context of Civilian CSDP Missions may be further complicated by their specificities such as the plurality of actors involved and the sensitivity of mission-related information.

In this connection, broader concerns in relation to the growing dependencies and vulnerabilities to which reliance on commercial AI tools and other technological infrastructures exposes EU actors – e.g., in relation to external access to sensitive information – should not be underestimated. In this respect, reflections on AI uptake within EU external action cannot be detached from the wider EU debate on technological and digital sovereignty, and from the Union's efforts to strengthen trusted European AI capabilities and infrastructures.[184]

Nor can these considerations be separated from the centrality of human rights as a framework which should be intended both as a foundation and a limit for legitimate uses of AI. The respect for, protection and promotion of, fundamental rights – including, e.g., human dignity, non-discrimination, privacy, and access to effective remedies – should inform the design, deployment, and evaluation of AI systems, ensuring that technological innovation and application remain firmly anchored in EU values and standards. Integrating human rights impact assessments, due diligence mechanisms, and safeguards against potential infringements of fundamental rights – for instance, due to algorithmic biases – is therefore essential to prevent adverse consequences and reinforce the legitimacy of EU action in external contexts.

In practical terms, this implies investing not only in technological capabilities, but also in human capital. Enhancing AI literacy among personnel, promoting interdisciplinary expertise, and maintaining a central role for human judgement in decision-making processes are essential to mitigate risks such as automation bias and deskilling. Furthermore, mechanisms for continuous monitoring, evaluation, and feedback should be embedded within both training programmes and operational practices, in order to effectively understand when uses of AI should be modified or discontinued in light of their failure to produce meaningful added value or of the generation of risks that cannot be adequately mitigated.

Ultimately, the added value of integrating AI in Civilian CSDP Missions will depend on the extent to which its deployment remains aligned with the EU's foundational principles and strategic objectives. When carefully designed and responsibly deployed, AI systems may indeed contribute to a more anticipatory, coherent, and effective approach to crisis management, enhancing the EU's capacity to respond to increasingly complex and interconnected challenges. However, failures to adequately address AI's associated risks may not only limit these benefits but also generate new vulnerabilities for local communities and staff members.

Recommendations

Considering the findings of this exploratory research paper and that the 2023 Civilian CSDP Compact envisages the development, in 2026, by the EEAS and relevant Commission services, in close consultation with Member States, of a strategy on emerging and disruptive technologies – including AI – in the framework of Civilian CSDP Missions, while, at the time of writing, no finalised and publicly accessible

[184] See, e.g., European Commission, "Cloud Sovereignty Framework", 2025; European Commission, "Apply AI Strategy", COM(2025) 723 final, 8 October 2025; S. Frantini, J. Pohle, D. Di Marco, S. Thabit Gonzalez and G. Sgueo. "Digital Sovereignty as a Geopolitical Strategy: Navigating Dependencies, Power, and Democratic Resilience in a Changing Global Order", JRC Publication Number 146878, 2026. See also European Data Protection Supervisor (EDPS), "Generative AI and EUDPR. Orientations for Ensuring Data Protection Compliance when Using Generative AI Systems", *cit.*, pp. 36-37.

Funded by the European Union

dedicated documents appear to provide specific guidance on the use of AI in this field, the following recommendations may be considered to orient further reflections, research, training and policy-development activities on the integration of AI into EU Civilian CSDP Missions.

- **Embed AI-related initiatives within existing civilian CSDP policies and processes:** Pending the possible development of more specific EU guidance on emerging and disruptive technologies for Civilian CSDP Missions, AI-related initiatives should not develop as isolated or *ad hoc* experiments/initiatives. They should be developed, when relevant, in connection with existing civilian CSDP policies and processes, including those relating to training and missions' life cycles. This would help ensure coherence with the Civilian CSDP Compact and other relevant sectorial policies, thus avoiding uncontrolled developments and duplication of efforts and initiatives, thus supporting a more consistent approach across missions, training and other activities.
- **Use existing EU and international legal frameworks as benchmarks for any relevant use of AI:**
  Any use of AI in connection with Civilian CSDP Missions should be assessed, when applicable, in light of relevant EU legal frameworks, including secondary EU law sources such as the AI Act, the GDPR and the EUDPR, as well as mission-specific arrangements and policies. In this sense, even when these instruments may not apply directly, or may apply only partially, they should still be considered as relevant benchmarks for the development of, e.g., mission-level policies, internal instructions, standard operating procedures, procurement requirements, etc. In any case, such policies as well as any use of AI systems should always remain aligned with relevant international and European human rights law standards. This is particularly important whenever the use of AI systems may affect individuals, local communities, mission personnel, or the exercise of rights and freedoms both in fragile or crisis-affected contexts and in educational/training settings when such use may affect the fundamental rights and freedoms of trainers and training participants.
- **Subject each AI use case to prior relevant impact assessments:**
  AI should not be assessed in the abstract, but in relation to specific intended uses, operational environments and potentially affected persons or groups. Before deployment, use-case-specific assessments should consider legal, human rights, data protection, and other risks and implications descending from the envisioned uses of AI each time considered. While according to relevant secondary EU law sources such as the AI Act, the GDPR and the EUDPR, corresponding types of impact assessments – such as Data Protection Impact Assessments (DPIAs) and Fundamental Rights Impact Assessments (FRIAs) – may not always be mandatory, here too their implementation could be a responsible good practice that could allow to mitigate existing and emerging risks pending the adoption of more specific sectorial guidance in this respect. On this point, also recent developments such as the adoption of the HUDERIA Model and Methodology, as a voluntary and flexible assessment tool to identify and mitigate the impact of the use of AI systems on human rights, democracy and the rule of law in connection to the Council of Europe Framework Convention on AI, human rights, democracy and the rule of law could be considered.
- **Preserve and ensure effective human judgement and oversight through AI literacy:**
  AI systems may *support* the performance of very diverse activities related to Civilian CSDP Missions, but they should never, even indirectly, replace human judgement and human decision-making processes. Human oversight should be intended as a substantive rather than a merely formal safeguard. In this sense, personnel should be able to understand the limits of AI-generated outputs, challenge them, disregard them where appropriate, and document how and why they were used. For this reason, AI literacy should be considered as a basis of cross-cutting competences for staff who design, procure, deploy, supervise or rely on AI systems. From this perspective, training activities should address not only basic technical notions, but also risks such as automation bias, hallucinations, opacity, discriminatory outputs, data protection breaches, cybersecurity

Funded by the European Union

vulnerabilities and the risk of deskilling, with differentiated learning paths and objectives for each relevant category of personnel involved.

- **Ensure that AI-supported training remains pedagogically grounded and subject to quality standards:**
  AI may support training needs analysis, the formulation of learning objectives, *curriculum* design, the preparation of training materials, scenario development, simulations, feedback analysis and evaluation. However, such uses should remain under the control and direction of trainers and subject-matter experts, particularly when AI-generated outputs concern sensitive and important topics such as legal standards, human rights, cultural dynamics, politically sensitive situations or other context-dependent factors. Training quality assurance should include checks on accuracy, contextual relevance, inclusiveness, traceability, pedagogical value and consistency with applicable CSDP training standards. AI should therefore be used to *support*, and not replace, the pedagogical and professional expertise of trainers and educators.
- **Proactively address digital sovereignty and sustainability concerns from the procurement stage:**
  The choices concerning the acquisition or use of AI tools should not be treated as a merely technological or financial matter. Procurement and providers-assessment criteria should consider compliance with EU values and applicable legal standards, including in relation to data protection, cybersecurity, human rights, and environmental sustainability. They should also take into account the risk of technological dependency on foreign actors and the vulnerabilities this may generate, e.g., in relation to access to sensitive information, the continuity of services and the possibility that foreign providers discontinue, modify or restrict access to their services/tools. These considerations seem particularly relevant in light of broader discussions on European digital and technological sovereignty. In this connection, also sustainability should be understood not only in purely environmental terms but also as concerning the long-term viability and usability of the adopted solutions. This includes assessing whether the selected tools can be maintained, updated, audited, explained, and effectively supervised over time; whether the necessary expertise and resources to do so and operate them are available within the relevant institutional framework; and whether their use remains proportionate to the actual added value they provide throughout their life cycle. Solutions that create excessive dependency, cannot be adequately controlled, or require levels of technical, financial, or organisational support that cannot realistically be ensured should therefore be approached with caution.
- **Proceed to the integration of AI through progressive, limited, documented, and reversible pilots:**
  In the absence of consolidated operational guidance, AI should first be tested through carefully delimited and top-down designed pilot activities, preferably in lower-risk settings such as – *inter alia* – training design, scenario development, non-sensitive knowledge management, translation support or feedback analysis. Such pilots should be assessed against pre-identified, clear, and verifiable criteria. Their results, limitations and risks should be documented and shared through appropriate civilian CSDP knowledge-management and sharing channels in order to avoid fragmented experimentation and support the gradual development of common standards, practical guidance and evidence-based policy options.

Funded by the European Union