NOTIONES

The EU Framework on Artificial Intelligence

Whitepaper

Authors: Domenico Frascà, Zanasi & Partners, IT

DOI: 10.5281/zenodo.7477224

January 2023 | First presented June 2022

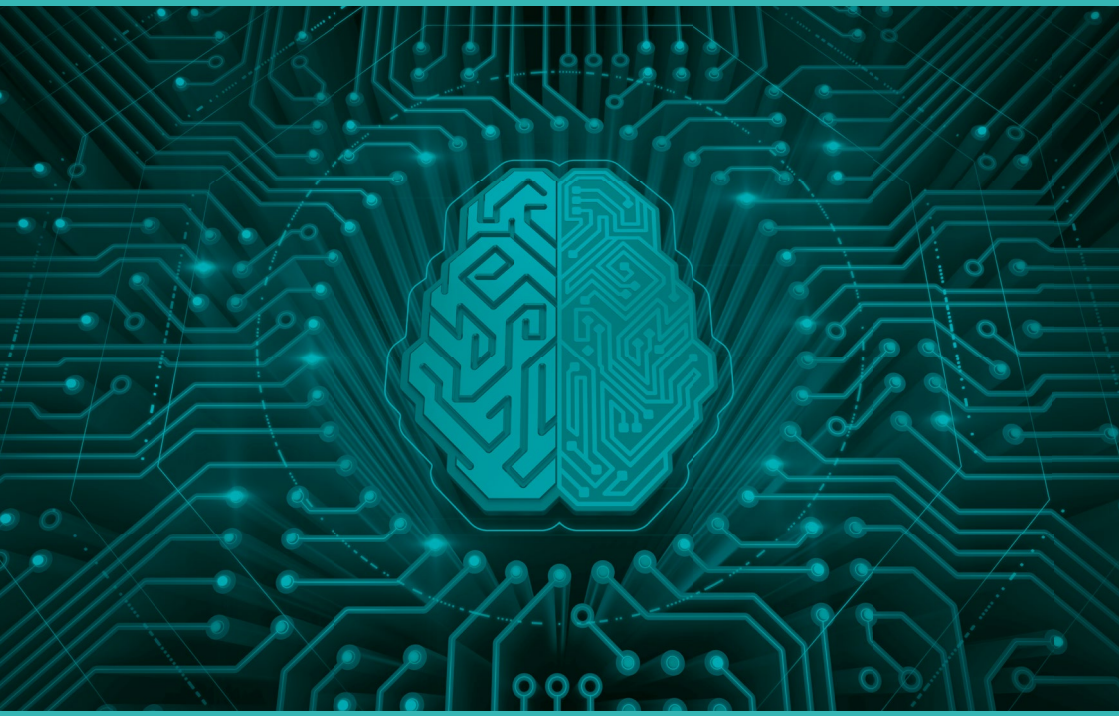


Table of Content

Project introduction 3

The EU Framework on Artificial Intelligence 5

AI for Law Enforcement applications 11

Human-centric AI 13

The NATO approach 15

Conclusions 17

References 18

Disclaimer 24

Project introduction

Novel technologies have presented practitioners with new opportunities to improve the intelligence process, but have also created new challenges and threats. Consequently, the timely identification of emerging technologies and analysis of their potential impact, not only on the intelligence community but also on terrorist or criminal organisations, is crucial.

However, time constraints can prevent intelligence practitioners from being updated on the most recent technologies.

In order to address this challenge NOTIONES will establish a network, connecting researchers and industries with the intelligence community. This network will facilitate exchange on new and emerging technologies but also equip solution providers with insights on the corresponding needs and requirements of practitioners. The so gained findings will be disseminated in periodic reports containing technologic roadmaps and recommendations for future research projects and development activities.

The consortium of NOTIONES includes, among its 30 partners, practitioners from military, civil, financial, judiciary, local, national and international security and intelligence services, coming from 9 EU Members States and 6 Associated Countries. These practitioners, together with the other consortium members, grant a complete coverage of the 4 EU main areas: West Europe (Portugal, Spain, UK, France, Italy, Germany, Austria), North Europe (Finland, Denmark, Sweden, Estonia, Latvia), Mittel Europe (Poland, Slovakia, Ukraine), Middle East (Israel, Turkey, Georgia, Bulgaria, Bosnia Herzegovina, North Macedonia) for a total of 21 countries, including 12 SMEs with diverse and complementary competences.

Project Objectives

GATHER the needs of intelligence and security practitioners related to contemporary intelligence processes and technologies;

PROMOTE interaction of technology providers and academy with intelligence and security practitioners;

IDENTIFY novel technologies of relevance for practitioners through research monitoring;

Project introduction

PUBLISH a periodic report, summarising key findings in order to orientate future research and development;

ENSURE the commitment and involvement of new organisations in the pan-European NOTIONES network.

Project Facts:

Duration: 60 Months **Reference:** 101021853

Programme: Horizon 2020 SU-GM01-2020 Coordination and Support Action

Coordinator: FUNDACION TECNALIA RESERACH & INNOVATION (Spain)

Scientific Technical Coordinator: ZANASI ALESSANDRO SRL (Italy)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101021853.

Coordinator

Scientific Technical Coordinator

Project Security Officer

Academic | Think-Tanks | Research

Technology Providers

Practitioners

The EU Framework on Artificial Intelligence

Artificial Intelligence is a family of technologies that display intelligent behaviour by analysing their environment and taking actions, with some degree of autonomy, to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world – i.e., voice assistants, search engines, or face recognition systems – or AI can be embedded in hardware devices – i.e., advanced robots, autonomous cars, or drones. Many AI technologies require training data to improve their performance. Once they perform well, they can help improve and automate decision-making in their specific domain. In general, AI can optimise existing processes or enable brand-new activities, offering new opportunities and benefits for private and public services - including Law Enforcement - but also serious risks. As first observed by the European Parliament in the Resolution of 16 February 2017 on Civil Law Rules on Robotics, the use of systems regulated by AI involves risks that are different from those linked to the human factor, inevitably posing ethical and legal problems [1]. With regards to privacy, it can be endangered by the unregulated use of facial recognition in public spaces. Furthermore, based on the design and type of data entered, AI systems could reproduce the existing discrimination in the offline world, making decisions influenced by ethnicity, gender, or age class. The so-called "deepfakes" – false but extremely realistic visual and audio contents, which are increasingly used in the field of information warfare – are also created through AI.

Still, the benefits brought by artificial intelligence are enormous. Faced with the rapid technological development determined by the growth of solutions based on artificial intelligence – the number of patent applications published in the last decade has increased by + 400% – and in an international context where the main competitors of the European Union are heavily investing in this technology, the European Commission has adopted a series of initiatives aimed at regulating AI [2].

Fragmentation of national actions with regard to AI applications as a risk to EU global competitiveness and standard setting [3] was the main reason that prompted the EC to launch the European Strategy on Artificial Intelligence in April 2018 [4]. The main assumption at the basis of the European strategy is that the EU "can lead the way in developing and using AI for good and for all, building on its values and its strengths". These strengths include the following: world-class researchers, labs, and start-ups; the Digital Single Market; a wealth of industrial, research and public sector data which can be unlocked to feed AI systems. Within its strategy, the European Commission then identified three distinct but complementary commitments: (a) increase investments in research and innovation of AI technologies to a level that corresponds to the economic weight of

the European Union in the world; (b) leave no one behind – especially in the education field – and ensure a smooth transition to the era of artificial intelligence in the workplace; (c) ensure that new technologies reflect European values and principles. With respect to this last commitment, the EC made explicit reference to the General Data Protection Regulation (GDPR) of 2016 on data protection and privacy in the European space [5] – and to Article 2 of the Treaty on European Union (TEU), which lists the founding values of the European political community: "respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities" [6].

In the aforementioned Communication, the European Commission also announced the adoption of a series of initiatives on artificial intelligence, including the launch of the European AI Alliance, which is a multi-stakeholder forum that has rapidly attracted members of civil society, industry and the academic world, and the institution of a High-Level Expert Group on Artificial Intelligence (AI HLEG) [7]. The 52 experts of the AI HLEG were asked by the EC to develop a set of ethical guidelines, published in April 2019 under the name of Ethics Guidelines for Trustworthy AI [8], and to make policy and investment recommendations, which were presented in June 2019 in the document Policy and Investment Recommendations for Trustworthy AI [9]. Overall, these two documents highlighted the need to join forces at a European level, in order to develop a human-centred approach to artificial intelligence as the main feature of "AI made in Europe". This vision was reaffirmed by the EC itself in COM (2019)168 entitled "Building Trust in Human-Centric Artificial Intelligence" of April 2019 [10]. Finally, on July 2020 the AI HLEG presented its final Assessment List for Trustworthy Artificial Intelligence (ALTAI), identifying seven key requirements – human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; environmental and societal well-being; accountability – to ensure that users benefit from AI without being exposed to unnecessary risks by indicating a set of concrete steps for self-assessment [11].

The European Strategy on Artificial Intelligence was followed by the White Paper on Artificial Intelligence of February 2020 [12], accompanied by a Communication from the EC itself outlining the European Strategy for Data [13]. In general, the document suggested establishing within the European space both an "ecosystem of excellence" in the development and diffusion of AI systems, and an "ecosystem of trust" based mainly on a human-centric approach to artificial intelligence. The White Paper was also accompanied by the "Report on the Safety and Liability Implications of Artificial

Intelligence, the Internet of Things and Robotics", concluding that the current product safety legislation contains a number of gaps that needed to be addressed, notably in the Directive 2006/42/EC – the so-called "Machinery Directive" [14] [15].

During the development of the EU framework on artificial intelligence, the European institutions have also given importance to the security aspect of AI systems. In December 2020, the European Union Agency for Cybersecurity (ENISA) presented a report called "Artificial Intelligence Cybersecurity Challenges", warning that AI may open new avenues in manipulation and cyber-attack methods, as well as new privacy and data protection challenges for citizens, enterprises, and institutions [16].

In defining its approach to trustworthy AI, the European Union has decided to play the role of pioneer in the sector, as it did with the GDPR of 2016. With COM (2021)205 of 21 April 2021, the EC has in fact announced an ambitious regulatory project on AI, which is still under development [17]. On the same date, the European Commission proposed to the European Parliament and the Council of the EU a regulation on harmonised rules regarding AI applications – the so-called "Artificial Intelligence Act" – emphasising that its approach is shaped by European values and risk-based, ensuring both safety and fundamental rights protection [18]. Once approved, this regulation would represent the first legal framework in the world on the AI sector. As stated in the proposal: "By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy. Such action is especially needed in high-impact sectors, including climate change, environment and health, the public sector, finance, mobility, home affairs and agriculture. However, the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society" [18]. The EU has therefore decided to regulate these elements and lay the necessary legal bases so that artificial intelligence has rules and specific guidelines within the common European space.

The appropriate balance between fundamental rights protection and public security is indeed one of the main pillars of the proposal. The European Union wants to ensure that European citizens can benefit from safe, transparent, ethical, and impartial AI systems under human control, thus placing specific requirements for all European or foreign AI systems used in the EU territory. Specifically, it aims at addressing risks of specific uses of AI, categorising them into four different levels: "unacceptable risk", "high risk", "limited risk",

and "minimal risk". In doing so, the AI regulation will make sure that Europeans can trust the artificial intelligence they are using. For instance, the "unacceptable risk" category includes AI applications in which algorithms track users' behaviour to automatically assess what level of creditworthiness to grant to individuals and companies – these users' behaviour tracking algorithms are widely utilised in China. Examples of elements classified as "high risk" are the following: AI systems that autonomously control critical infrastructures; AI applications that could endanger the life and health of citizens; CV sorting software for hiring procedures. All these systems will be carefully evaluated before being placed on the market, will be subject to minimum transparency obligations and will be monitored throughout their life cycle. Anyway, the vast majority of artificial intelligence systems fall into the category of "minimal risk", therefore they will not be subject to the new European legislation.

Particular attention must be paid to biometric surveillance. Artificial intelligence powers the use of biometric technologies, including facial recognition applications, which are used for verification, identification, and categorisation purposes by private or public actors. While facial recognition markets are poised to grow substantially in the coming years, the increasing use of facial recognition technologies (FRTs) has emerged as a salient issue in the worldwide public debate on biometric surveillance. While there are real benefits in using facial recognition systems for public safety and security, their pervasiveness and intrusiveness, as well as their susceptibility to error, give rise to a number of fundamental rights concerns with regard, for instance, to discrimination against certain segments of the population and violations of the right to data protection and privacy [19]. In October 2021, the European Parliament passed a non-binding resolution that prevents the use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement, along with the creation of private facial recognition databases. With this resolution, the EP recognized that the use of AI for mass surveillance and other unlawful interference, such as the profiling of citizens in order to rank them and restrict their freedom of movement, pose a serious threat to fundamental rights [20]. The non-binding resolution sends a strong signal on how the EP is likely to vote in upcoming negotiations on the Artificial Intelligence Act.

The legislative framework on artificial intelligence will have a huge impact worldwide, as it was for the GDPR of 2016, which has become an international standard in its sector since it came into effect in 2018. With this proposal, the EU wanted to strengthen its competitive position with respect to its main competitors – China and the United States of America – by anticipating them in the definition of a regulatory framework that could thus become

the reference standard on the global scene. This political dimension was reaffirmed by the Coordinated Plan on Artificial Intelligence 2021 Review [21], which goes hand in hand with the proposal for the Artificial Intelligence Act. The new plan builds on the collaboration established between the EC and Member States – plus Norway and Switzerland – during the 2018 Coordinated Plan on Artificial Intelligence, which was a joint commitment to maximising Europe's potential to compete globally and an essential first step in defining actions and funding instruments for the uptake and development of AI across sectors. Moreover, it encouraged Member States to develop national strategies [22] [23]. The revised plan proposes around 70 actions for closer and more efficient cooperation between the EC and Member States on artificial intelligence between 2021 and 2027.

As already outlined in the White Paper on Artificial Intelligence of February 2020, the European Commission has thought about a series of tools to support the future legislation, in order to favour the birth of a public-private partnership on artificial intelligence, data and robotics to define, implement and invest in a joint strategic research and innovation program for Europe. These tools include the establishment of centres of excellence for AI, the birth of new digital innovation poles that act as one-stop shops to provide access to technical skills and experimentation – so that companies can "test before investing" – and the creation of a central European database of AI resources needed for the uses of private companies and the public sector. With funds provided by the Digital Europe (DIGITAL) and Horizon Europe (HE) programs, the European Commission intends to invest around one billion euros per year in AI and mobilise further investment from the private sector and Member States through their National Recovery and Resilience Plans (NRRPs) for a total of 20 billion a year [24].

Schematically, the European approach to artificial intelligence has four fundamental objectives: (a) establish the enabling conditions for the development and diffusion of AI; (b) build a strategic leadership in high impact sectors; (c) making the EU a place where AI can flourish; (d) ensure that AI technologies serve people. These objectives fall within the broader concept of a continent that sees in technological progress, attentive to the environment and human society, not only one of the keys necessary for the post-pandemic restart, but above all an indispensable tool for an ever-greater integration between Member States in a single entity capable of relating equally to the great world powers.

On March 2022, the European Parliament's Special Committee on Artificial Intelligence in a Digital Age (AIDA) adopted a report on artificial intelligence. On one hand, it

emphasised that the digital transition in the EU must be human-centric and compatible with the Charter of Fundamental Rights of the European Union. On the other hand, the report cautioned that the EU has fallen behind in the global race for technological leadership. This might result in a risk for standards that need to be developed elsewhere in the future, often by non-democratic actors [25]. The delay of the EU compared to its main competitors is the reason why the European Commission proposed the creation of the EU-US Trade and Technology Council (TTC), which was established in June 2021 to promote coordination between the two shores of the Atlantic Ocean on everything related to the technology sector – from regulation to taxation, passing through cybersecurity [26]. On May 2022, during the meeting at the second Ministerial Summit of the TTC in Paris, both parties discussed the implementation of common AI principles and agreed to develop a joint roadmap on evaluation and measurement tools for trustworthy AI and risk management [27]. However, the European approach places the European Union at the forefront of regulation in the field of artificial intelligence, as it happened with the GDPR of 2016. In the end, given the European focus on the values underlying the rules, aimed at avoiding the systematic violation of privacy and individual freedoms as is the case in the Chinese system, it seems that the EU and the US are destined to converge in this sector.

The legislative process relating to the proposed regulation is currently proceeding. The EP Committee on the Internal Market and Consumer Protection (IMCO) and the EP Committee on Civil Liberties, Justice and Home Affairs (LIBE) jointly released a draft report on the EC proposal in April 2022 [28]. The document includes proposed amendments to the original text proposed by the European Commission. The most significant changes proposed in the draft report include the ban on using artificial intelligence to implement predictive policing practices, the obligation to register AI-based technologies and greater alignment with the GDPR.

AI for Law Enforcement applications

Referring to AI systems used by law enforcement agencies (LEAs), an important document has been elaborated by Europol through the launch of the Accountability Principles for Artificial Intelligence – the so-called AP4AI project – in February 2022 [29]. This multidisciplinary project is led by Europol and the Centre of Excellence in Terrorism, Resilience, Intelligence, and Organized Crime Research of Sheffield Hallam University (CENTRIC) and represents a practical toolkit to support AI accountability within the internal security domain. The project is specifically designed for security and justice practitioners and it is aimed at preventing misuse of AI by internal security practitioners and safeguarding accountability. The document states the legislative gap in terms of accountable use of artificial intelligence within the internal security domain and addresses the challenge of creating a comprehensive global framework for the accountability of Policing, Security and Justice [29]. The AP4AI should be seen as a "living document" for the further creation of an AI Accountability Agreement (AAA) [29].

Accountability is considered by the AP4AI as the core value for AI deployments within internal security domains [29]. Accountability is defined as "the acknowledgement of an organisation's responsibility to act in accordance with the legitimate expectations of stakeholders and the acceptance of the consequences" [29]. Accountability should be taken also as a basis for creators in order to develop AI coherently with the legal use they are allowed to. AP4AI is innovative in aiming at creating a comprehensive legal framework that does not refer only to LEAs but to all the stakeholders (i.e., industry, non-governmental organisations, researchers, citizens) who take part or are affected by AI. Hence, while there is widespread knowledge of risk assessment within the internal security sector, there is scarce awareness of how the risk can be mitigated in practice and who are the involved actors that should be considered. The report briefly focuses on EU efforts and then refers to other countries' legislation (the US's in particular) to take it as a model approach for further legislation.

AP4AI consists of the introduction of 12 principles that together define requirements for achieving accountability in the use of AI: legality, universality, transparency, pluralism, independence, commitment to robust evidence, enforceability and redress, compellability, explainability, constructiveness, conduct and learning organisation. Here, the 12 principles will not be revised in detail, but an overview of the main concepts to implement an accountable use of artificial intelligence will be provided. The document argues the necessity to encompass national approaches and provide enforcement mechanisms applicable to the entire AI system and associated actors. Within the scope of the document, covering the entire AI system means ensuring accountability in all the

areas of the AI lifecycle – from design and development to concrete application in various contexts – and to all the stakeholders involved in artificial intelligence. In this regard, a multi-level collaboration within civil society, public and private organisations is necessary.

Given the speed of development of AI, the document recognises the exigence of having a regulatory assurance body that identifies the risks and can give advice to stakeholders and the government.

Human-centric AI

The main vision characterising the EU approach to artificial intelligence is the creation of human-centric AI, which ensures it works for people and protects the fundamental rights of European citizens. The EC proposal for the Artificial Intelligence Act states that AI systems must always be under human control. However, no mention is made of the training of personnel responsible for supervising these systems, except that it has to be adequate for the task [18]. This lack of attention to this practical aspect has concerned the whole process of elaboration of the EU framework on AI.

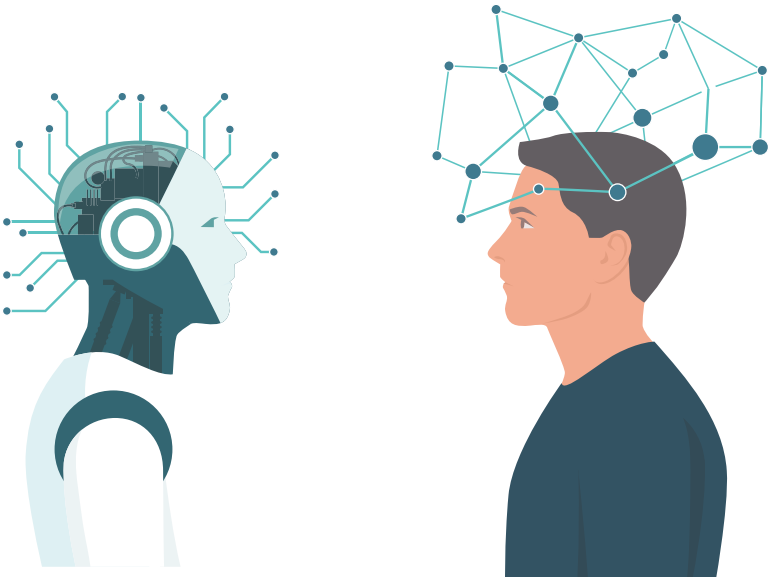
The Ethics Guidelines for Trustworthy A I [8], published by the High-Level Expert Group on Artificial Intelligence in April 2019, promoted a set of 7 key requirements that AI systems should meet in order to be deemed trustworthy, including "human agency and oversight". According to this key requirement, AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches . With COM(2021)205 of 21 April 2021 [18], the European Commission has accepted the content of the aforementioned document, but it has not taken steps to regulate the training issue. Article 14 on "Human Oversight" states that "high-risk" AI systems should be designed and developed in such a way that natural persons can effectively oversee their functioning [18]. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. Where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and it is responsive to the human operator, and that the natural persons to whom human oversight is assigned have the necessary competence, training and authority to carry out that fundamental role.

In general, the European Commission's proposal does not go beyond the recognition of the need for the training of the personnel responsible for controlling AI systems to be adequate for their supervision. Furthermore, it is not established whether this training should be regulated at European level or left to the competence of Member States.

As a comparative example, the US National Artificial Intelligence Initiative (NAAI) – which became law in January 2021 – focuses on training an AI-ready workforce. The United States is investing in current and future generations of American workers through apprenticeships, skills programs, and education in science, technology, engineering, and mathematics (STEM), with an emphasis on information technology, to ensure that American workers are able to take full advantage of the opportunities of AI [30]. The lack

of any legislative provision in this regard is particularly serious considering that AI systems may be responsible for the management of sensitive sectors and infrastructures within the EU territory. In recent years, the European Union has launched a set of initiatives aimed at developing knowledge of AI systems, but they have always been conceived as a support to the European digital transition rather than training the personnel who carries out the supervision of the artificial intelligence implemented in critical areas or defence systems. Some of these initiatives are listed below.

Open to businesses, organisations and public administrations from all over the continent, the Digital Europe programme (DIGITAL) is actually investing in learning and training opportunities – i.e., specialised masters and education programmes in key capacity areas – that will create new AI experts within the European Union [31]. Moreover, the Digital Education Action Plan (2021-2027) is a renewed European policy initiative to support the sustainable and effective adaptation of the education and training systems of EU Member States to the digital age. In order to enhance digital competences for the digital transformation of Europe, this policy aims to update the European digital skills framework to include AI and data skills [32].



The NATO approach

One of the consequences of the lack of a European legislative provision on the training of personnel in charge of supervising the AI systems used is that in the defence sector it will continue to be carried out in the context of the Atlantic Alliance.

Over the last few years, the North Atlantic Treaty Organization (NATO) has paid particular attention to the so-called "emerging and disruptive technologies" (EDTs), endorsing a Coherent Implementation Strategy on EDTs in February 2021 [33]. Their importance for deterrence, defence and capability development was also recognised by the report entitled "NATO 2030: United for A New Era", which was commissioned by Secretary General Jens Stoltenberg and published in November 2020 [34]. In particular, the Atlantic Alliance is developing specific plans for each of the following technological areas: (a) data and computing; (b) artificial intelligence; (c) autonomy; (d) quantum-enabled technologies; (e) biotechnology and human enhancements; (f) hypersonic technologies; (g) space; (h) novel materials and manufacturing; and (i) energy and propulsion [35] [36]. Of all these dual-use technologies, artificial intelligence is known to be the most pervasive, especially when combined with others like big data, autonomy, or biotechnology. Due to its cross-cutting nature, AI will pose a broad set of international security challenges, affecting both traditional military capabilities and the realm of hybrid threats. This is the reason why NATO has prioritized AI, identifying it as critical for its operations and a key enabler for modernisation and cooperation in the Atlantic Alliance.

At the Meeting of NATO Ministers of Defence held in Brussels in October 2021, the Allied Defence Ministers formally launched the NATO Artificial Intelligence Strategy [37]. Only a summary of the document has been made public. The strategy is meant to provide a common policy basis to support the adoption of AI systems among Member States in order to achieve NATO's three core tasks: collective defence, crisis management, and cooperative security. In particular, in accordance with international law and values of the Atlantic Alliance, the document established six basic principles of safe and responsible use of artificial intelligence in the field of defence: (a) lawfulness, (b) responsibility and accountability, (c) explainability and traceability, (d) reliability, (e) governability, and (f) bias mitigation [38]. All AI systems developed by NATO and its partners will have to comply with these principles, which are quite similar to the Ethical Principles for Artificial Intelligence adopted by the US Department of Defense in February 2020, but with a plan to verify that the principles are followed [39]. By adopting a comparative approach, the EC's proposal for the Artificial Intelligence Act seems to be more restrictive for high-risk applications of AI, although its impact on defence will be indirect, as it does not apply to the military domain. The Artificial Intelligence in Defence Action Plan – finalized by the

The NATO approach

European Defence Agency at the end of 2020 – shares more similarities with the NATO Artificial Intelligence Strategy, as it focuses on identifying modes and means for EU Member States to collaborate in the development of AI for their militaries [40].

While it emphasizes collaboration with private technology companies, academics and start-ups, the NATO's new AI strategy needs further refinement as AI would help NATO's military and civilian personnel interlink devices on different platforms, perform rigorous data analytics, and quicken response time in response to conventional or hybrid attacks. In this sense, the 2022 Strategic Concept will play a central role. The Strategic Concept is one of NATO's most important documents, as it informs military alliance's planning, resource allocation, and programming based on changes in the threat environment. The last version of the document has not been updated since 2010 [41]. But, as established at the 2021 NATO Summit in Brussels, the Atlantic Alliance endorsed its new Strategic Concept at the 2022 NATO Summit in Madrid, which was held in 2022 [42].

By setting NATO's strategic direction for the next decade and beyond, the 2022 Strategic Concept highlights the essential role of EDTs in collective defence, ensuring that the military alliance will continue to adapt to a changing world. However, the document should focus less on the emergence of new technologies and more on how NATO's military and civilian personnel use them – i.e., human training on artificial intelligence and other EDTs. With the aim to build greater digital capacity within the Atlantic Alliance, NATO institutions are aware of the importance of providing education, training and instruction to both military and civilian personnel in various areas consistent with the objectives and priorities identified by NATO's new security policies. During the 2021 NATO Summit, the Heads of State and Government of the thirty member countries decided to support internal cooperation and technological development through the creation of two new structures: the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund. Both bodies aim to consolidate the technological advantage within the Atlantic Alliance, considered precisely one of the foundations on which NATO's ability to dissuade and defend itself from potential external threats is based [43]. In this perspective, the 2022 Strategic Concept establishes deeper cooperation between NATO and the private sector, academia and non-governmental organisations, which may provide new tools, strategies and practices to improve the knowledge, expertise and capability of personnel in the supervision of AI systems.

Conclusions

In the context of the global race for artificial intelligence, the European Union aims to strengthen its competitive position with respect to its main competitors – the United States and China – by anticipating them in the definition of a comprehensive regulatory framework on trustworthy AI that could become a global standard. Indeed, acting as a tech regulator, the European Commission believes that the Artificial Intelligence Act will become an international point of reference for similar legislation, thanks to its balanced approach between fundamental rights protection and public security. Structured around a risk-based approach, the proposed regulation introduces obligations in proportion to the potential harmful impact of AI applications on humans, where riskier AI systems deserve tighter obligations.

AI systems are efficient tools at the disposal of security practitioners and citizens but it is necessary to safeguard accountability and avoid misuse that can endanger national security and the respect for human rights. In this direction, the AP4AI Project has been established by Europol in February 2022.

The EC proposal for the Artificial Intelligence Act of April 2021 does not address the issue of human training on AI. The proposal simply states that it needs to be adequate for the task, without establishing minimum technical requirements or setting up specific training structures [18]. Therefore, this fundamental aspect will not be regulated in the European framework – meaning, the training of personnel responsible for supervising AI systems may be informally delegated to the structures and initiatives of the Member States.

The NATO approach was described to explore possible parallelisms between defence and civil security with regard to Artificial Intelligence preparedness of human operators. However, related documents are focused on the emergence of new technologies rather than on how military and civilian personnel use them.

The civil security community of NOTIONES expresses concerns about this rather significant gap, especially since the future EU framework on Artificial Intelligence aims to become an international standard and advises the need to promote new tools, strategies and practices to improve the knowledge, expertise and capability of personnel in the supervision of AI systems used for Security, Intelligence and Law Enforcement. From a long-term perspective, it is crucial that the EU – in the search for strategic autonomy – continues to allocate public resources for the development of a leading "AI made in Europe" and favours the creation of a European environment that stimulates private investment.

References

[1] European Parliament, "European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics," 16 February 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&from=EN. [Accessed 31 May 2022].

[2] European Parliament, "Artificial intelligence: Threats and Opportunities," 4 May 2022. [Online]. Available: https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200918STO87404/20200918STO87404_en.pdf. [Accessed 3 June 2022].

[3] European Parliamentary Research Service (EPRS), "European Framework on Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies," 28 September 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU(2020)654179_EN.pdf. [Accessed 3 June 2022].

[4] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Commitee of the Regions. Artificial Intelligence for Europe," 25 April 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&rid=1. [Accessed 31 May 2022].

[5] European Parliament and Council of the EU, "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 [...], and Repealing Directive 95/46/EC (General Data Protection Regulation)," 27 April 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. [Accessed 31 May 2022].

[6] Official Journal of the European Union, "Consolidated Version of the Treaty on European Union - Title I Common Provisions - Article 2," Official Journal of the European Union, 26 October 2012. [Online]. Available: https://eur-lex.europa.eu/eli/treaty/teu_2012/art_2/oj. [Accessed 3 June 2022].

[7] European Commission, "The European AI Alliance," European Commission, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance. [Accessed 3 June 2022].

[8] European Commission, "Ethics Guidelines for Trustworthy AI," European Commission, 8 April 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. [Accessed 3 June 2022].

References

[9] High-Level Expert Group on Artificial Intelligence (IA HLEG), "Policy and Investment Recommendations for Trustworthy AI," 26 June 2018. [Online]. Available: https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf. [Accessed 3 June 2022].

[10] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building Trust in Human-Centric Artificial Intelligence," European Commission, 8 April 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence. [Accessed 3 June 2022].

[11] European Commission, "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment," European Commission, 17 July 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment. [Accessed 3 June 2022].

[12] European Commission, "White Paper on Artificial Intelligence - A European Approach to Excellence and Trust," 19 February 2020. [Online]. Available: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. [Accessed 31 May 2022].

[13] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data," 19 February 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN. [Accessed 4 June 2022].

[14] European Commission, "Commission Report on Safety and Liability Implications of AI, the Internet of Things and Robotics," European Commission, 19 February 2020. [Online]. Available: https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en. [Accessed 4 June 2022].

[15] European Parliament and Council of the EU, "Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on Machinery, and amending Directive 95/16/EC (Recast)," 9 June 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0042&from=EN. [Accessed 4 June 2022].

References

[16] European Union Agency for Cybersecurity (ENISA), "Artificial Intelligence Cybersecurity Challenges," European Union Agency for Cybersecurity (ENISA), 15 December 2020. [Online]. Available: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges. [Accessed 3 June 2022].

[17] European Commission, "Communication on Fostering a European Approach to Artificial Intelligence," European Commission, 21 April 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence. [Accessed 4 June 2022].

[18] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonized Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts," 21 April 2021. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF. [Accessed 31 May 2022].

[19] European Parliamentary Research Service (EPRS), "Regulating Facial Recognition in the EU," September 2021. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. [Accessed 4 June 2022].

[20] European Parliament, "Use of Artificial Intelligence by the Police: MEPs Oppose Mass Surveillance," European Parliament, 6 October 2021. [Online]. Available: https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance. [Accessed 4 June 2022].

[21] European Commission, "Coordinated Plan on Artificial Intelligence 2021 Review," European Commission, 21 April 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review. [Accessed 31 May 2022].

[22] European Commission, "Communication from the Commission to the European Commission, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Coordinated Plan on Artificial Intelligence," 7 December 2018. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0002.02/DOC_1&format=PDF. [Accessed 31 May 2022].

References

[23] Council of the EU, "Conclusions on the Coordinated Plan on Artificial Intelligence," 11 Febrary 2019. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf. [Accessed 31 May 2022].

[24] European Commission, "A European Approach to Artificial Intelligence," European Commission, 23 February 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/commission-invest-eu292-million-digital-technologies-and-cybersecurity. [Accessed 3 June 2022].

[25] Special Committee on Artificial Intelligence in a Digital Age (AIDA), "Report on Artificial Intelligence in a Digital Age," 22 March 2022. [Online]. Available: https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.pdf. [Accessed 4 June 2022].

[26] European Commission, "Digital in the EU-US Trade and Technology Council," European Commission, 16 May 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council. [Accessed 3 June 2022].

[27] European Commission, "EU-US Trade and Technology Council: Strengthening our Renewed Partnership in Turbulent Times," European Commission, 16 May 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3034. [Accessed 3 June 2022].

[28] EP Committee on the Internal Market and Consumer Protection and EP Committee on Civil Liberties, Justice and Home Affairs, "Draft Report on Artificial Intelligence Act," 20 April 2022. [Online]. Available: https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf. [Accessed 17 June 2022].

[29] European Union Agency for Law Enforcement Cooperation (Europol), "Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain," 22 February 2022. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf. [Accessed 15 June 2022].

[30] US White House, "American Artificial Intelligence Initiative: Year One Annual Report," February 2021. [Online]. Available: https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf. [Accessed 18 June 2022].

References

[31] European Parliament and Council of the EU, "Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240," 29 April 2021. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:321918fd-6af4-11e8-9483-01aa75ed71a1.0003.03/DOC_1&format=PDF. [Accessed 15 June 2022].

[32] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Digital Education Action Plan 2021-2027," European Commission, 30 September 2020. [Online]. Available: https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education-action-plan. [Accessed 15 June 2022].

[33] North Atlantic Treaty Organization, "New Focus on Emerging and Disruptive Technologies Helps Prepare NATO for the Future," North Atlantic Treaty Organization, 3 March 2021. [Online]. Available: https://www.nato.int/cps/en/natohq/news_181901.htm. [Accessed 15 June 2022].

[34] Reflection Group (NATO), "NATO 2030: United for a New Era," 25 November 2020. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf. [Accessed 15 June 2022].

[35] North Atlantic Treaty Organization, "Emerging and Disruptive Technologies," North Atlantic Treaty Organization, 7 April 2022. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_184303.htm. [Accessed 15 June 2022].

[36] NATO Science & Technology Organization, "Science & Technology Trends 2020-2040. Exploring the S&T Edge," March 2020. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf. [Accessed 15 June 2022].

[37] North Atlantic Treaty Organization, "NATO Releases First-Ever Strategy for Artificial Intelligence," North Atlantic Treaty Organization, 22 October 2021. [Online]. Available: https://www.nato.int/cps/en/natohq/news_187934.htm. [Accessed 15 June 2022].

[38] North Atlantic Treaty Organization, "Summary of the NATO Artificial Intelligence Strategy," North Atlantic Treaty Organization, 22 October 2022. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_187617.htm. [Accessed 15 June 2022].

References

[39] US Department of Defense, "DOD Adopts Ethical Principles for Artificial Intelligence," US Department of Defense, 24 February 2020. [Online]. Available: https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/. [Accessed 15 June 2022].

[40] European Defence Agency (EDA), "Annual Report 2020," 30 May 2021. [Online]. Available: https://eda.europa.eu/docs/default-source/eda-annual-reports/eda-annual-report-2020.pdf. [Accessed 15 June 2022].

[41] North Atlantic Treaty Organization, "2010 Strategic Concept," 20 November 2010. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf. [Accessed 15 June 2022].

[42] North Atlantic Treaty Organization, "2022 NATO Summit," North Atlantic Treaty Organization, 3 June 2022. [Online]. Available: https://www.nato.int/cps/en/natohq/news_196144.htm. [Accessed 15 June 2022].

[43] North Atlantic Treaty Organization, "Brussels Summit Communiqué," North Atlantic Treaty Organization, 14 June 2021. [Online]. Available: https://www.nato.int/cps/en/natohq/news_185000.htm. [Accessed 15 June 2022].

Disclaimer

This document contains material which is copyright of certain NOTIONES consortium parties. All NOTIONES consortium parties have agreed to the full publication of this document.

Neither the NOTIONES consortium as a whole, nor any certain party of the NOTIONES consortium warrants that the information contained in this document is capable of use, or that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using the information.

The contents of this document are the sole responsibility of the NOTIONES consortium and can in no way be taken to reflect the views of the European Commission. The European Commission is not responsible for any use that may be made of the information it contains.

The commercial use of any information contained in this document requires a license from the proprietor of that information. For information and permission requests, contact the NOTIONES project coordinator Erkuden Rios Velasco (TECNA) at *Erkuden.Rios@tecnalia.com*.

The content of this document may be freely distributed, reproduced or copied as content in the public domain, for non-commercial purposes, at the following conditions:

a) it is requested that in any subsequent use of this work the NOTIONES project is given appropriate acknowledgement with the following suggested citation:

White paper "The EU Framework onArtificial Intelligence" (2022), Authors: Domenico Frascà, Zanasi & Partners, IT, produced under the NOTIONES project, which has received funding from the European Union's Horizon2020 Programme for research and innovation under grant agreement No. 101021853. Available at: *Home - Notiones*

b) this document may contain material, information, text, and/or images created and/or prepared by individuals or institutions external to the NOTIONES consortium, that may be protected by copyright. These sources are mentioned in the "References" section, in captions and in footnotes. Users must seek permission from the copyright owner(s) to use this material.

NOTIONES

Coordinator

Scientific Technical Coordinator

Project Security Officer

Academic | Think-Tanks | Research

Technology Providers

Practitioners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101021853.