ieee.es
Instituto Español de Estudios Estratégicos

Opinion
Paper

70/2025 19/09/2025

Emma Talavera Rodríguez

Regulatory impact on the application of Artificial Intelligence in Defence and Security

Visit the

Receive E-NEWSLETTER

Regulatory impact on the application of Artificial Intelligence in Defence and Security

Abstract:

Artificial Intelligence (AI) is increasingly being used in defence and security, improving military strategies and operations. However, these advances also generate ethical and legal challenges regarding the privacy of the data with which these systems are trained or other issues such as biases, their autonomy and the fact that they can also be vulnerable to manipulation and attacks. This is why it is necessary to establish a regulation that guarantees the appropriate use of AI in the military environment, does not violate any fundamental rights and is safe.

Keywords:

AI, defence and security, legislation, regulation, Europe.

How to cite this document:

TALAVERA RODRÍGUEZ, Emma. *Regulatory impact on the application of Artificial Intelligence in Defence and Security*. IEEE Opinion Paper 70/2025. IEEE web link and/or bie link[3] (accessed day/month/year).

NOTE:** The ideas contained in ***Opinion Papers are the responsibility of their authors and do not necessarily reflect the views of the IEEE or the Ministry of Defence.

Introduction

Artificial Intelligence (hereinafter AI) is a technological tool that is transforming the world we live in. Its rapid advancement and the amount of data available to train these systems has a major impact on different areas of our reality, both civil and military[1] .

Due to its great capacity and scope, new developments are being carried out in relation to autonomous vehicles, medical diagnostics and automated security activities, among others, as well as new forms of employment in the military field[2] . The application of AI in the latter area can provide assistance to commanders in decision-making in military operations and strategies, as well as in anticipating and managing threats with the greatest immediacy[3] . An example of the influence AI is having on military use is the war in Ukraine, where drones and advanced AI-based technologies have been used to halt Russian advances and counterattack[4] .

Although AI, as we have seen, drives innovation and can improve the quality of human life, it also brings with it legal and ethical challenges, such as bias or privacy violations[5] . Its implementation and use must be responsible and ensure compliance with fundamental rights.

Regulations, principles and ethical codes have been established that refer to AI, but the evolution of this technology is faster than the development of legislation, and there is still a long way to go in this regard. It is important to mention what the Ministry of Defence

[1] AI Task Force. (2019). *ARTIFICIAL INTELLIGENCE IN SUPPORT OF DEFENCE.* Paris: Minèstere des Armées. Retrieved from https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf

[2] Olier, E., & Corchado, J. (2022). *Artificial Intelligence: applications to Defence.* Madrid: IEEE, CESEDEN. Retrieved from https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEEINV01_2022_EDUOLI_Inteligencia.pdf

[3] Bossio Ballesteros, V. (26 October 2023). *Artificial Intelligence in the Military: A Relevant and Useful Tool.* Retrieved from CEEEP: https://ceeep.mil.pe/2023/10/26/la-inteligencia-artificial-en-el-ambito-militar-una-herramienta-relevante-y-util/#post-23413-endnote-3

[4] Santayana, J. P. (2024). Artificial intelligence and the war in Ukraine. In J. P. Santayana, *Strategy Notebook 226. Artificial intelligence in geopolitics and conflicts* (pp. 87-103). Madrid: IEEE - CESEDEN. Retrieved from https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-226

[5] Lisi, M. (2024). AI in space: a catalyst for change. In M. Lisi, *Strategy Notebook 226. 'Artificial intelligence in geopolitics and conflicts'* (pp. 189-217). Madrid: IEEE, CESEDEN. Retrieved from https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-226

document "Vision of Artificial Intelligence in the Armed Forces"[6] says about military operations:

> *Although there are various initiatives underway to certify the use of AI in military operations, there is currently no specific legislation on the matter.*
>
> *In turn, for an AI system to be authorised for use in military operations, it must be reliable and predictable, so that control over its outcome is always maintained.*

This article analyses the need for generic international regulation of AI, especially in the military sphere. It is a tool that, in addition to facilitating innovation and providing major advances for defence, presents risks such as privacy and autonomous operation in weapons, which highlights the importance of adequate regulation.

In order to prepare the following sections, research has been carried out on the current regulatory framework for AI, identifying which regulations mention defence and security and which do not. We have also studied how they can be applied in this field, along with which needs are not being met.

Regulatory framework

Spain

Below are two artificial intelligence strategies that were developed in Spain and have provided a guideline action plan for the implementation of AI.

The National Artificial Intelligence Strategy (ENIA) was published in December 2020 with the aim of committing the European Union to becoming a leader in the development of ethical, inclusive and economically efficient AI[7] . This strategy does not explicitly mention defence and security in its wording.

The Artificial Intelligence Strategy 2024 was approved in Spain in May 2024. This initiative aims to accelerate and promote the implementation of AI at the national level, as well as

[6] Ministry of Defence. *Vision of Artificial Intelligence in the Armed Forces,* 2024
[7] Government of Spain. *National Artificial Intelligence Strategy (ENIA).* Government of Spain, 2020. Available at: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf

to reinforce the ENIA[8] . This text also does not contemplate application in the military sphere.

With regard to specific defence and national security documents, there are policies and strategies which, although some of them do not clearly address AI, establish different frameworks in which the use and development of this tool could be specifically included. Furthermore, in the Ministry of Defence's own documents, the precepts can be extrapolated to establish certain criteria on the legitimacy of the application of AI.

The Defence Technology and Innovation Strategy (ETID) promotes R&D&I projects that strengthen national research groups technologically to participate in defence projects[9] . This is relevant because it deals with issues of technology in weapons and ammunition, among other aspects, although AI as such is not mentioned.

In the context of military behaviour, the Royal Ordinances of the Armed Forces set out military conduct and ethical principles in accordance with legal regulations[10] . There is no reference to AI either, but it can be anticipated that its use may raise ethical dilemmas both in the area of conflict and in management tasks[11] .

Similarly, the National Security Strategy states that initiatives will be carried out to address crisis situations, such as applying technologies that integrate AI with knowledge management[12] .

Europe

Europe was a pioneer in establishing the AI Act in 2024, a comprehensive regulation on AI that makes it a global benchmark in this area[13] . This regulation aims to establish a uniform regulatory system for the development and use of AI systems. Furthermore, it is

[8] Government of Spain. Artificial Intelligence Strategy 2024. Ministry of Economy, Trade and Business, 2024. Available at: https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf

[9] Ministry of Defence. *Defence Technology and Innovation Strategy (ETID) 2020.* Ministry of Defence, 2020. Available at: https://publicaciones.defensa.gob.es/estrategia-de-tecnologia-e-innovacion-para-la-defensa-etid-2020-libros-papel.html?___store=es

[10] Ministry of Defence. *Royal Ordinances for the Armed Forces.* Royal Decree 96/2009, of 6 February. Published in the Official State Gazette, no. 33, of 7 February 2009. Available at: https://www.defensa.gob.es/Galerias/fuerzasarmadas/realesordenazas/RROOFAS_2009_BOE.pdf

[11] Military School of Legal Studies. *Spanish Journal of Military Law 116.* Ministry of Defence, 2021. Available at: https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/e/redem_116.pdf

[12] National Security Council. *National Security Strategy 2021.* Government of Spain, 2021. Available at: https://www.dsn.gob.es/sites/default/files/documents/ESN2021%20Accesible_1.pdf

[13] European Commission. *AI Act.* European Commission. Retrieved on 5 June 2025 from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

the first regulation to regulate AI exclusively[14] . It does not apply to the military sphere, as indicated in Article 2(3):

"3. This Regulation shall not apply to areas that fall outside the scope of Union law and, in any case, shall not affect the competences of Member States in matters of national security, regardless of the type of entity to which Member States have entrusted the performance of tasks related to those competences.

This Regulation shall not apply to AI systems which, and to the extent that, they are placed on the market, put into service or used, with or without modification, exclusively for military, defence or national security purposes, regardless of the type of entity carrying out these activities.

This Regulation shall not apply to AI systems that are not placed on the market or put into service in the Union where their output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out these activities.[15] .

With regard to data protection, Europe has a legal framework that covers both personal and non-personal data. The laws that comprise it are relevant in this context because, when using technologies, including AI, this data must be used responsibly.

In this regard, the GDPR (General Data Protection Regulation) of 2016 stands out, protecting the personal data of natural persons and its processing. This regulation excludes national security from its scope of application in Article 2.2:

"2. This Regulation shall not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by Member States when carrying out activities falling within the scope of Chapter 2 of Title V of the TEU;

[14] European Commission. *AI Act.* European Commission. Retrieved on 5 June 2025 from: https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai

[15] 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 Regulation). *Official Journal of the European Union,* 12 July 2024, No. 1689.

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[16] .

To facilitate the availability and exchange of data between EU countries, thereby benefiting both citizens and businesses, the DGA (Data Governance Act) has been in force since 2022. Unlike the GDPR, the DGA covers both personal and non-personal data[17] , but it does not apply to defence and national security, as indicated in Article 1.5:

"5. This Regulation shall be without prejudice to the competences of Member States with regard to activities concerning public security, defence and national security."[18] .

Finally, it is also worth mentioning European regulations on cybersecurity, notably the NIS2 Directive and the DORA Regulation**,** both from 2022. The former establishes measures to achieve greater cybersecurity in the European Union and improve the internal market[19] . The latter strengthens the cybersecurity of financial institutions. Neither applies to defence and national security functions, as stated in Article 2.7 of the NIS2 Directive:

"7. This Directive shall not apply to public administration entities carrying out their activities in the areas of national security, public security, defence or the enforcement of law, including the prevention, investigation, detection and prosecution of criminal offences."

and in recital 17 of the DORA Regulation: "In accordance with Article 4(2) of the Treaty on European Union, and without prejudice to judicial review by the Court of Justice, this

[16] 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). *Official Journal of the European Union,* 4 May 2016, No. 119.

[17] European Commission. *A European strategy for data.* European Commission. Retrieved on 5 June 2025 from: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[18] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation). *Official Journal of the European Union,* 3 June 2022, No. 152.

[19] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union,* 27 December 2022, No. 333.

Regulation should not affect the responsibility of Member States for essential State functions relating to public security, defence and the safeguarding of national security, for example in cases where the provision of information would be contrary to the safeguarding of national security."[20]

Commitments

Having reviewed some of the regulatory documents currently in force in Spain and Europe, we will now look at other types of documents that apply only to the countries that subscribe to them, such as the 2019 OECD AI Principles. This is the first intergovernmental standard and promotes reliable and innovative AI that respects human rights[21] , but no mention is made of the military sphere. Countries such as the United States, Spain, Japan and the United Kingdom have adhered to these principles[22] .

Similarly, there is the 1980 Convention on Certain Conventional Weapons (CCW). This is based on the principles of other standards to prohibit and restrict the use of weapons to protect civilians and prevent serious damage to the environment[23] . It is relevant because it sets limits on the use of weapons in conflicts in order to cause as little harm as possible to the aforementioned groups.

To conclude with this type of document, the Hiroshima AI Process consists of a set of guiding principles to be followed by organisations developing AI to promote safe and reliable AI globally[24] . These principles do not expressly exclude defence and national security, but neither do they mention them. One part of the text, translated into Spanish, states: "These principles should apply to all AI actors, when and as applicable, to cover the design, development, deployment and use of advanced AI systems."

[20] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. *Official Journal of the European Union,* 27 December 2022, No. 333.

[21] OECD. *AI principles.* OECD. Retrieved on 5 June 2025, from: https://www.oecd.org/en/topics/ai-principles.html

[22] OECD. *OECD Legal Instruments.* OECD. Retrieved on 5 June 2025 from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents

[23] Sandoz, Y. *Convention of 10 October 1980 on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (Convention of 10 October 1980).* United Nations, 2010. Available at: https://legal.un.org/avl/pdf/ha/cprccc/cprccc_s.pdf

[24] European Commission. *G7 Leaders' Statement on the Hiroshima AI Process.* European Commission, 2023. Retrieved 5 June 2025, from: https://digital-strategy.ec.europa.eu/es/library/g7-leaders-statement-hiroshima-ai-process

We look forward to further developing these principles as part of the global policy framework, with input from other nations and broader stakeholders from academia, business, and civil society.[25] .

Others

Among other documents related to AI, many countries, such as China and India, have developed their own codes of ethics on the use of this tool. These documents can be used as a reference, but they do not impose sanctions. Furthermore, instead of having specific regulations on AI, they have laws that cover cybersecurity in a more general way, without focusing on specific technologies.

In contrast to the Western approach to the use of AI, China is rapidly implementing the use of AI for purposes such as population assessment, which would be impossible to transfer under the legislation applicable here. Considering that even the civil sphere is limited in this regard, it is less feasible to take the military world into account.

On the other hand, there are organisations and conferences that bring together researchers and academics from different territories to discuss issues related to AI, such as the Iberamia association, whose objective is to promote scientific and technological activities involving the use of AI in Ibero-American and Spanish- and Portuguese-speaking countries[26] . Similarly, in the European context, there is the AI HLEG (High-Level Expert Group on Artificial Intelligence), which has more than 4,000 members from the European Union[27] . Another example of a global meeting is the REAIM (Responsible AI in the Military domain Summit), whose objective is to discuss the responsible use of AI in the military context[28] .

[25] European Commission. *International guiding principles of the Hiroshima process for an advanced AI system.* European Commission, 2023. Retrieved 5 June 2025, from: https://digital-strategy.ec.europa.eu/es/library/hiroshima-process-international-guiding-principles-advanced-ai-system
[26] Iberamia. *Institutional information.* Iberamia. Retrieved 5 June 2025, from https://www.iberamia.org/iberamia/informacion-institucional/
[27] European Commission. *High-Level Expert Group on Artificial Intelligence.* European Commission. Retrieved on 5 June 2025, from: https://digital-strategy.ec.europa.eu/es/policies/expert-group-ai
[28] REAIM. *REAIM Summit 2024.* REAIM. Retrieved 5 June 2025, from: https://www.reaim2024.kr/reaimeng/index.do

Application of regulations

As noted in the previous point, there are various regulations governing technology at the national, European and international levels; however, most of them exclude its use for defence and national security. Therefore, although Europe is a pioneer in developing specific legislation addressing the implementation and use of AI, it cannot be considered a benchmark in the military field unless, as specified in the Act itself, AI systems developed in this field are used temporarily or permanently for other purposes, such as civil or humanitarian purposes[29] .

So, what is the real impact of these regulations on defence and security? How could these regulations be applied to defence and security? What ethical and legal challenges arise within the current regulatory framework in this regard?

AI is playing an increasingly important role in national defence and security, raising regulatory and ethical issues that must be addressed, either by creating new regulations or by amending existing ones, including the relevant sections.

One example of this is the application of AI in drone swarms. These drones coordinate with each other and, in many cases, human intervention is not necessary. They are more effective than individual drones because, in this case, they are capable of performing different tasks and their activity can continue if one of them has a problem or is inoperative. In turn, some drone swarm methods are based on highly sophisticated algorithms inspired by the collective behaviour of birds or insects, which also enable them to respond to new situations thanks to AI. This technology can be applied to the search for missing persons, for example[30] . The United States is working on various projects related to this type of drone operation, such as the *Gremlins* programme for *UAVs*

[29] 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 Regulation). *Official Journal of the European Union,* 12 July 2024, No. 1689.

[30] U.S. Government Accountability Office. *Science & Tech Spotlight: Drone Swarm Technologies.* U.S. Government Accountability Office, 14 September 2023. Retrieved 5 June 2025 from: https://www.gao.gov/products/gao-23-106930

(Unmanned Air Vehicles) and CICADA (Close In Covert Autonomous Disposable Aircraft)[31] .

This is just one of many cases in which AI can be applied in a military context, implying that this tool is gradually being integrated into this field and is already forming part of operational strategies and tools. The absence of a regulatory framework applicable to this area gives States greater freedom when it comes to implementing and using AI-based systems. However, this freedom, in turn, raises ethical and legal questions.

In this context, it is up to each state to follow a series of ethical measures and principles, which is still a subjective issue and which, as previously stated in this article, leads to a misalignment of ethical codes and regulations.

"AI governance is a global issue, not just a national one. Effective governance of AI systems requires international cooperation, as AI systems and their effects do not respect national borders. Countries must work together to establish global standards and norms for the use of AI"[32] .

The reality is that the development of weapons and tools will continue to evolve in line with the constant advancement of new technologies and, in this case AI, generating new situations that will continue to raise the same dilemmas mentioned above.

Initially, the following questions may arise: Who is responsible for the actions of AI? How can we ensure that decisions are not made based on bias? What type of data is used to train these systems? Is citizens' privacy respected?

The current legal framework does not provide clear answers to these questions.

[31] Gómez de Ágreda, Á. *Artificial intelligence on the battlefield.* In Ministry of Defence (Ed.), *Military uses of Artificial Intelligence, automation and robotics (IAA&R).* 2020. Available at: https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx.-_VV.AA.pdf

[32] Marwala, T. *Militarisation of AI Has Severe Implications for Global Security and Warfare.* UNU, 24 July 2023. Retrieved 5 June 2025, from: https://unu.edu/article/militarization-ai-has-severe-implications-global-security-and-warfare

In 2021, NATO specified a framework in which six principles of responsible use for AI in defence were approved: "Legality, Responsibility and Accountability, Explainability and Traceability, Reliability, Governance and Bias Mitigation."[33] .

These principles, for example, could be taken into account for AI training. Humans make decisions based on their biases and prejudices, even if unconsciously. AI will make its decisions based on the data it is trained with, so impartiality and diversity in that data are crucial to ensuring quality and fair results. But how is the use of this data regulated? There are various regulations that govern and penalise data protection violations, such as the GDPR in Europe, but the military environment is excluded from its scope.

Although AI aims to improve human performance, it does not yet have the ability to interact socially and, therefore, to identify and understand complex behaviours that occur or are necessary on the battlefield[34] .

The following paragraphs will present two illustrative cases, without implying any criticism of them, which reflect the lack of regulation of AI.

The first example is the Chinese government's use of this technology in Xinjiang province. Facial recognition and genomic surveillance systems were implemented, and it is estimated that between 10% and 20% of Uyghurs[35] , an ethnic group of Turkish descent and practising Islam found in this Chinese province[36] , have been detained. According to Amnesty International, China purchased digital surveillance systems from companies in France, Sweden and the Netherlands[37] to establish this control.

---

[33] NATO. *Summary of NATO's revised Artificial Intelligence (AI) strategy.* NATO, 2024. Retrieved 5 June 2025, from: *https://www.nato.int/cps/en/natohq/official_texts_227237.htm#:~:text=Within%20the%20AI%20Strategy%2C%20Allies,Reliability%2C%20Governability%20and%20Bias%20Mitigation.*

[34] Las Heras, P. *The challenge of artificial intelligence for security and defence.* University of Navarra, 18 October 2023. Retrieved on 5 June 2025, from: https://www.unav.edu/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa

[35] Feldstein, S. *China's high-tech surveillance drives oppression of Uyghurs.* Bulletin of the Atomic Scientists, 27 October 2022. Retrieved 5 June 2025, from: https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/

[36] Fernández Aparicio, P. *The Uyghurs and the Chinese dragon at a crossroads (reprint).* IEEE-CESEDEN, 2024. Disponible en: https://www.defensa.gob.es/documents/2073105/2265107/Los+uigures+y+el+drag%C3%B3n+chino+en+la+encrucijada+%28reedici%C3%B3n%29.pdf/56606714-9d21-b311-b1b9-4bdb021136da?t=1732097514224

[37] Amnesty International. *EU companies selling surveillance tools to China's human rights abusers.* Amnesty International, 21 September 2020. Retrieved on 5 June 2025, from: https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/

In this case, we can see both China's responsibility for human rights violations and that of these companies which, albeit indirectly, are involved in the measures taken by this great power[38] .

The second example is the use of Turkish-made STM Kargu-2 drones in Libya in 2020, which, according to a United Nations Security Council report, are autonomous drones that were used to target retreating soldiers[39] . There were no casualties, but they could have been attacked autonomously, and the report confirms that, although attempts have been made to ban this type of weapon, these drones were used nonetheless[40] .

Conclusions

The current regulatory framework governing the development and application of AI, whether national, European or international, in the field of defence and national security, poses ethical and legal challenges, as has been evident throughout this document.

On the one hand, there is the problem already mentioned in the introduction: legislation lags far behind the advancement of technology in general, not just the advancement of AI. This is an obstacle to establishing up-to-date and clear regulations to deal with new technologies.

On the other hand, current regulations that do take these tools into account exclude defence and security from their scope of application or do not mention them directly in their texts, which creates legal uncertainty as to which regulations the development and use of AI-based military systems should be subject to, as well as the legal and ethical limits. Furthermore, there is the added difficulty that in the military sphere, many decisions are based on confidential criteria and national strategic interests.

In conclusion, the lack of regulation of AI in defence and security poses a risk to both the military and civilian spheres due to the potential misuse of this tool. This is why international collaboration is necessary in order to develop regulations that cover all areas

[38] Ibid.
[39] Official Association of Engineers of Castilla-La Mancha. *A drone has attacked people completely autonomously for the first time.* Official Association of Engineers of Castilla-La Mancha, 21 September 2020. Retrieved on 5 June 2025 from: https://coiiclm.org/un-dron-ha-atacado-a-personas-de-forma-totalmente-autonoma-por-primera-vez/
[40] AS. *A drone attacks humans without being ordered to do so: Its autonomous AI decided on the attack.* AS, 2021. Retrieved on 5 June 2025, from: https://as.com/meristation/2021/05/28/betech/1622234551_710916.html

and aspects of AI, especially in the defence and security environment. Although this would limit innovation to some extent, its main objective would be to establish a set of common rules that could be aligned with current legislation and would facilitate the responsible treatment and use of AI in this field.

Emma Talavera
*Rodríguez**Rodríguez****
Intern at the IEEE
Master's student in Cybercrime, Nebrija University