Artificial Intelligence, Cybersecurity Factor

Associate professor **Adriana-Iuliana STANCU**[1]

Abstract

Objectives: Recent cyberattacks on significant European institutions, the exponential rise in cyberthreats, and the speed at which technology is developing have brought attention to the need for increased cooperation and change in the civil-military sphere and the fact that there is no hierarchy between the military and civilian communities. As mandated by international agreements, including those pertaining to the Charter, the EU's cybersecurity policy enables it and its Member States to improve their ability to defend, detect, protect, and even prevent by appropriately utilizing the entire spectrum of security options at the civilian and military communities. Proposals and Methodology: The need to defend European values and invest in their preservation has led to the EU's cooperation structures becoming involved in the cyber offensive, including with its financial capabilities, even though each EU member state has direct responsibility for its national security, including in the sensitive cyber domain, as a direct result of Article 4(2) TEU. Results and Implications: To defend the EU, its citizens, the EUIBA, and their operations and missions in the cyber domain related to the Permanent Security and Defence Policies (PSDP), it is imperative that the actions of all European nations and European institutions, organizations, and agencies, including EUIBA, be strengthened in the upcoming period. Additionally, it highlights the need of cyber resilience at the EU level by boosting defensive capabilities in this delicate, cutting-edge area, expanding the potential for cyber defence, and generating trustworthy input from Member States. Thus, cooperation is required to improve cybersecurity.

Keywords: *EU member state; cybersecurity; European values; cyber domain.*

JEL Classification: K14

DOI: https://doi.org/10.62768/ADJURIS/2025/3/01

Please cite this article as:
Stancu, Adriana-Iuliana, „Artificial Intelligence, Cybersecurity Factor", in Devetzis, Dimitrios, Dana Volosevici & Leonidas Sotiropoulos (eds.), *Digital Lawscapes: Artificial Intelligence, Cybersecurity and the New European Order*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2025, p. 15-24.

1. Introduction

The technological development and innovations that humanity has devel-

[1] Adriana-Iuliana Stancu - "Dunarea de Jos" University of Galati, Romania, ORCID: 0000-0001-6259-5116, adriana.tudorache@ugal.ro.

oped in the recent years have reached unimaginable dimensions, and thus the development social and economic process in the technological, medical, cultural and military area in the last half century has taken different forms, whether we are talking about the defense industry, the car manufacturing industry or the IT field, which in some cases are interdependent. When the first microprocessor was invented in the early 1970s, information technology became widely used, and processing speed increased dramatically. Shortly after that, internet networks were widely used by the public, and the number of computers connected reached several hundred. This number increased even more, eventually connecting many people and accelerating the development of blockchain technology and quantum computing.

The management of data, information, and knowledge and their transformation into an optimal best management practice (BMP) for a positive outcome are linked to the evolution of computerization and computing equipment. As a result, in addition to the growth in data volume, their storage capacity has also increased, moving from the byte of the 1960s to the yottabyte and brontobyte of the modern era. The increase in storage capacity and the amount of data has required the subsequent development of computing tools, which, from classical tools and traditional computers, has reached quantum computing and the development of quantum computers that generate a real-time computing method and, in some cases, surpassing the understanding capacity of the human mind; however, the introduction of new technologies has frequently had a profound impact on society.

2. Cybersecurity in the European Union

The Council has decided on a common approach to EU cybersecurity policy regarding the 2014 cyber defence modality and its 2018 amendments. This includes reinvesting in our modern, cooperative forces, technologies, and next-generation capabilities, as well as cybersecurity and fortifying partnerships to tackle shared challenges[2].

Informatics has become an area of strategic competition at a sensitive time due to the increasing use of digital technology. Thus, it is necessary to maintain a permanent online presence, free from external influences, secure and unchanged. Information technology has facilitated Russia's war of aggression against Ukraine, which has impacted the entire world and contributed to instability and insecurity with a significant risk of permanent escalation[3]. It has also generated more internet activity than this senseless and brutal conflict.

---

[2] Forbrukerradet*, Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy,* 2018, p. 6, https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf, accessed on 15 March 2025.

[3] Jonna Järveläinen, Duong Dang, Mike Mekkanen, and Tero Vartiainen. 2025. “Towards a Framework for Improving Cyber Security Resilience of Critical Infrastructure against Cyber Threats: A

The Russian-initiated war in Ukraine has created a new strategic context and shown why European nations, the Union as a whole, and its allies must further solidify the EU's stance to eradicate cyberthreats and to bolster traditional cybersecurity and cyber defences against criminal activity and cyber security attempts in the "online" sphere.

The European institutions' will to respond quickly and effectively to threats that aim to compromise, interfere with, or take control of networks and IT systems, among other things, is emphasized in the Joint Communication on the EU Cybersecurity Policy. This Joint Communication represents a new accomplishment in the EU's comprehensive approach to resilience, response, conflict prevention, connectivity, and stability in the single cyberspace by updating the Cybersecurity Strategy and taking it to the global level in accordance with the strategic guidelines. In this context, Member State representatives stressed the need for appropriate and consistent responses from EU, its Member States and its partners, who are on standby, to the review of the guidelines for the implementation of the EU Cyber Diplomacy Toolkit as a new step development of cyber platform[4].

In applying the provisions of the 2014 Cyber Defense Policy Framework and the abdication of the next 4 years, Member State representatives, the Council, agreed on a common approach on EU cybersecurity policy to reinvest in our modern and cooperative forces and technologies and next-generation capabilities, as well as cybersecurity and strengthening partnerships to solve common problems[5].

The cyber development area has become an area of strategic competition at a time when dependence on digital technologies is increasing. Thus, it is necessary to maintain an open, independent, stable and secure online presence. The use of these computers that sparked and followed Russia's unprovoked and still wholly unjustified war of aggression against Ukraine threatens international stability and security, poses a serious risk of escalation, and adds to the already notable rise in Internet activity that occurs outside of the recent armed conflict.

From a strategic perspective, the war in Ukraine is a novel situation that has once again demonstrated the necessity for the EU, its member states, and its partners to continue supporting the EU in creating solutions to cybercrime and to uphold its reputation for cybersecurity and defence against criminal activity and

---

Dynamic Capabilities Approach." *Journal of Decision Systems* 34 (1). doi: 10.1080/12460125.2025.2479546. Also see R. Srinivasan, M. Kavitha, R. Kavitha, and S. Uma (2023). "Cybersecurity and Artificial Intelligence: A Systematic Literature Review." In Sugumaran D, Souvik Pal, Dac-Nhuong Le, Noor Zaman Jhanjhi (eds.), *Recent Trends in Computational Intelligence and Its Application.*Proceedings of the 1st International Conference on Recent Trends in Information Technology and its Application (ICRTITA, 22) 1st ed., CRC Press, London, p. 120 et seq. https://doi.org/10.1201/9781003388913.

[4] Lilian Edwards, Michael Veale (2017), „*Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For".* 16 *Duke Law & Technology Review,* pp. 18-84, p. 67.

[5] Forbrukerradet*, op. cit.*, p. 6.

tendentious acts on the "online" space. This collaboration demonstrates a new step toward a comprehensive EU vision on resilience, feedback, the eradication of conflict ideas, cooperation, and stability in the cyber space. It fulfils its cybersecurity thinking once strategic concepts are unified. In this situation, the Council of Europe has shown that direct and well-coordinated responses are needed from the EU area, its Member States and its partners, who, in turn, strongly want to review the possibilities of implementing all the instruments for cyber diplomacy in the EU as a step up in the development of this cyber platform[6].

A step-by-step, visible and penetrating approach is essential for the development of trust, which in turn is necessary for the future establishment of a crisis management structure in the EU and beyond, in terms of constructive stability in relation to cybersecurity in this generous space. The plan thus conceived regarding crisis management is being developed by the Council. It also resumes and discusses the need to continue to develop our capabilities to defend, detect, defend and stop criminal cyber-attacks through a significant penetration of the area of knowledge of what is happening, capacity building, capacity development, training, testing and a special resistance as a non-returnable response against cyber-attacks directed towards European countries and EUIBA, the missions in the CSDP theatre of operations, using all existing possibilities. In doing so, the Council supports the High Representative and the Commission to control cyberspace, not to get involved in the management of pointless work and to ensure collaboration with existing initiatives. Understanding and coordination of European countries cybersecurity professionals must be supported in a planned manner, between all communities, both military and civilian, in the online space and between a public and a private ecosystem that inspires trust. In this situation, Member States are supported to research and permanently develop national mechanisms for civil-military cooperation, thus facilitating the mutual exchange of information, collaborate on lessons learned, contribute to supporting interoperable standards and create risk assessments by building reliable platforms for man-made or natural disasters, as well as cooperative operations, in particular at European level but also with other states, in full compliance with the European legislative provisions on the measures required to strengthen its development, exceptional cybersecurity[7].

Thus, online education, training and exercises are put back in the foreground, as they are essential to ensure their availability and effectiveness, but also because new jobs are needed at national level, through services originating from the EU space through the European Security and Defence Academy (ESDA), EDA, ENISA and the future introduction of PESCO, through projects such as the

[6] Lilian Edwards, Michael Veale, *op. cit*., p. 67.

[7] Carolina Polito, Lorenzo Pupillo (2024), „Artificial Intelligence and Cybersecurity", *Forum Journal*, Volume 59, No. 1, p. 10-13. For a few connections with human rights see Rowena Rodrigues, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities." *Journal of Responsible Technology* 4 (December 2020): 100005. https://doi.org/10.1016/j.jrt.2020.100005.

Internet Environment Associations and the EU Internet Academy as well as the Innovation Hub (CAIH). But to consolidate these efforts, the European institutions are concerned with the establishment of the EDA CyDef-X framework project to coordinate and support cybersecurity services. The Council is responsible for the development of the EDA – European Defence Agency to investigate, in close cooperation with European countries with EEAS[8], how CyDef-X can also support activities such as CYBER PHHALANX, including mutual support in compliance with the provisions of Article 42, paragraph 7 of the TEU but also in accordance with the solidarity clause as clearly follows from the provisions of Article 222 of the TFEU, as well as the Commission and ENISA in relation to civil actions. Furthermore, the Council supports the use of the CyDef-X cybersecurity test area through continuous development. Today, there are also beneficial proposals such as Cyber Range Federations. To ensure a rapid and efficient decision-making process regarding an unresolved situation in a cyber crisis, the Council points out that it is necessary to permanently organize exercises at national and mass level in the decision-making matter of the Member States.

3. Cybersecurity and Artificial Intelligence

The presence of unacceptable risks posed with AI used in ways not permitted by law will inevitably lead to prohibitions and general provisions of the 2025 Use Regulation. Although the overall effectiveness of each prohibition is linked to the establishment of control and. In the application of this Regulation, the intended use of prohibitions is essential to explain the risks that may cause disasters and to be reflected effectively in other processes such as civil law. Furthermore, the most important infrastructure management system and policy consideration must be functional before 2 August 2026, when the legislative provision will be in field. Thus, what refers to notified bodies but also to the governance structure must be applicable from 2 August 2025. In the first era of technological growth but also the adoption AI models with the clear aim of general use, the roles of AI model providers should be aligned with the general application from 2 August. The AI Office must consider that classification policies and practices are updated and comply with new technological developments. In view of all this, Member States must establish and inform the European institutions about rules sanctions, reconsider whether they are applicable when decree in question will entry into force[9].

These harmonization provisions set out in the Regulation should apply to all sectors and, subject to the new legal framework, existing Union legislation

[8] European Union External Action Service.

[9] Daron Acemoglu, *Opinion: The AI we should fear is already here*, in The Washington Post (2021), in https://www.washingtonpost.com/opinions/2021/07/21/ai-we-should-fear-is-already-here/, accessed on 15 March 2025.

should not be affected, in particular the GDPR protection which are already guaranteed, of operational workers, but also product safety, which complement the Regulation[10], the compensation amount for any damages incurred, as stipulated in Council Directive 85/374/EEC, is still in effect and completely enforceable. Furthermore, the Regulation is opposed by its provisions to Union law in relation to social policy and legal provisions in labor law, relating to employment and the protection of workers, to working conditions in general, fair practices in the field of employment, safety at work, including cooperation between employers and employees. In a positive sense, the Regulation does not call into question the existence of fundamental rights in democratic exercise in the Member States of the Union, including the right correlated with the freedom to know and to carry out other types of activities associated with certain operational systems belonging to members of the governments of European countries, such as the right to mediation, to conclude collective agreements and to apply them or to take joint action, in compliance with European legal provisions for by national law[11].

Those providing physical or virtual components must bear in mind As AI systems created for direct action with people have been created, developed and approved so that people interact directly with the AI system, with one exception when the matter is obvious for well-founded reasons, which a prudent or just attentive person, in relation to the existing circumstances and the level at which it is used, can establish through his own perceptions. The obligation does not lie with AI systems authorized by law to investigate, determine, prevent or pursue the commission of crimes in the field, in relation to the protection of the rights and freedoms of third parties, given that such systems exist in the public domain for the detection of crimes.

Individuals or legal entities that market AI systems, including AI systems that create artificial content, i.e. transform voices, images, which can be video or text, must be sure that the results of the AI system can be processed, to establish the artificial creation or use. Those who create such systems must consider that the solutions are efficient, credible but also with collaborative potential and with operational possibilities depending on the content, costs but also on the development of the technology that must be public, according to the standards in force. The obligation is not applicable when AI systems perform a routine editing auxiliary function or do not modify the substance of the data provided by the implementer or its content or if they are required by law to detect, prevent, investigate or detect crime[12].

---

[10] https://www.gov.uk/data-protection, accessed on 15 March 2025.

[11] Daniel J. Solove, *The digital person. Technology and Privacy in the Information Age,* New York University Press, 2004, p. 22 et seq., https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&con text=faculty_publications, accessed on 15 March 2025.

[12] Working Party, "Article 29" *On Data Protection*, *Guidelines on automated individual decision-making and profiling under Regulation* (EU) 2016/679, Adopted on 3 October 2017 as last revised and adopted on 6 February 2018, p. 13, https://ec.europa.eu/newsroom/document.cfm?doc_id=47742, accessed on 15 March 2025.

Where these providers belong to third countries, they must send a representative to the European Union to specify the requirements of the Order.

Regarding persons who implement emotional recognition systems or use biometric classification, they are obliged by law (informed consent) to inform the individuals thus exposed about the functioning of the system and its use for the processing of personal data, as set out in the Regulations in the field promoted at European level as well as in the 2016 Directive. The obligation presented does not apply to AI systems created specifically for biometric classification and establishing emotions, used in the criminal field and under the aegis of criminal laws, for the prevention and investigation of crimes, in compliance with the provisions of the Code of Criminal Procedure created in compliance with the rights and freedoms recognized to all persons, because they are under the aegis of European legislation[13].

Those implementing the AI system that creates or uses images, voices or video fragments develops deepfakes that indicate artificially composed or used content. This obligation is not applicable if its use is in the spirit of the provisions of criminal law for the detection, prevention, prosecution or repression of crimes[14]. When this content is part of a work or program of a known artistic, creative, satirical, opinion-based or similar nature, the obligations to disseminate information contained in the legal provision in question, have the sole recognized purpose of highlighting the processed or manipulated content but which does not contradict the exposition or agreement of the work. The requirements thus requested become mandatory when the entire EU legal system cannot be undermined[15].

Implementers of an AI system generate, or process published documents publicly displayed for the purpose of informing the public about situations important to individuals indicating that this book was written or used. The obligation itself does not apply when the use is provided for and accepted according to the law to establish, investigate or prosecute "detectable crimes or if the content created by AI was investigated through an editorial sample responsibility for publication" or and. content belonging to a natural or legal person.

Information must be delivered to those interested as clearly and precisely as possible, up until the moment of the first presentation or contact. This information must be established according to accessibility requirements.

Thus, the AI office supports and creates the possibility of developing and promoting good practices policies throughout the Union to facilitate the efficient

---

[13] Lilian Edwards, Michael Veale, *op. cit*., p. 67; Forbrukerradet*, op. cit.,* p. 6.

[14] Adriana Iuliana Stancu, (2024). „Combating The Financing Terrorism: an Analysis of the EU Regulatory Framework and Enforcement Mechanism", in Ojars Sparitis (ed.), *Proceedings of 11th SWS International Scientific Conference on Social Sciences - ISCSS 2024*, SGEM WORLD SCIENCE (SWS) Scholarly Society, DOI: 10.35603/sws.iscss.2024/s02/06.

[15] Agencia Española de Protección de Datos (2020), *RGPD compliance of processing that embed Artificial Intelligence. An introduction*, 2020, p. 6, https://www.aepd.es/guides/gdpr-compliance-processings-that-embed-ia.pdf, accessed on 15 March 2025.

establishment of functions in relation to the determination and identity of substances produced or created by this inventive process. The Commission may adopt any legislation to implement or approve each of the elements of good practice[16].

The moment when the supervisory authority of a European country establishes with clear evidence that an AI system presents elements of risk, according to the Regulation, an assessment of the performance possibilities of the AI system is required, in relation to the requirements and obligations requested that go beyond the framework of the Regulation, with an emphasis on AI systems with special risk in relation to vulnerable groups of people. The supervisory authority is only required to notify and work in permanent cooperation with the government that is in charge of the controls or with the pertinent entities mentioned in the Order when dangers to fundamental rights are identified.

4. Conclusions

Beyond the Framework Decision's content, the EU's examination of cybercrime must be viewed in the context of its significant importance. The scope of cybercrime issues covered by this thorough investigation is substantially wider, which directly contributes to the identification of legislative tools of significant relevance to the EU that impact both the first and third pillars of the EU. The development of the areas of freedom, justice, and security is where the third pillar's battle against cybercrime lies.

Making a broader criticism, namely in the light of the fact that the Framework Decision was verified by the European Commission in close connection with the case C-176/03 of the Court of Justice of the EU, regarding the division of competences in the field of criminal cases, reported to the European Commission and the Council of the EU, a permanent reflection is required on the issues raised by the legislation on cybercrime, at the EU institutional level. Another issue that requires increased attention is the way in which the EU solves the thorny issue of data protection, in parallel with the legislation at the global level that approaches this topic from a different perspective, creating a negative impact. However, we must acknowledge that the EU has added value in combating cybercrime in the areas of freedom, justice, and security that define it. The Council of Europe Treaty on Cybercrime is especially valuable in this regard. It transcends the boundaries of the EU Framework Decision and is distinguished by the fact that any nation interested in resolving this complex issue can do so. This new feature in the field of Council instruments has been used for the first time. The ratification of the Framework Decision was included, relatively recently, in the annex to the Communication from the Commission to the European Parliament

[16] Ancuța Gianina Opre, Simona Șandru, „The right to be forgotten on the internet, a means of combating discrimination" in M. Tomescu (ed.), *Non-discrimination and equal opportunities in contemporary society*, Pro Universitaria Publishing House, Bucharest, 2015, p. 288.

and the Council on the results of the 2005 Court judgment in case C176/03.

All the States signatories to the Treaty have embarked on a common path, with a sustained effort, and with an extended range of action, possibly at global level, in the active fight against cybercrime.

A consensus is desired on the measures required to control cybercrime and of course a total elimination of cybercrime, but these are unlikely goals to be achieved, and so the cyberspace will always have a space to fight to make things right. What is wonderful is that remarkable progress has been made in this almost unknown area and common solutions have been found to address cybercrime. Not every issue has been resolved or identified to date, but coordinating efforts to develop a more comprehensive definition of cybercrime and standardizing laws in this innovative area across all EU member states are crucial steps in the European fight against this new type of highly intrusive, cross-border crime.

Bibliography

1. Acemoglu, Daron, *Opinion: The AI we should fear is already here*, in The Washington Post (2021), in https://www.washingtonpost.com/opinions/2021/07/21/ai-we-should-fear-is-already-here/, accessed on 15 March 2025.
2. Agencia Española de Protección de Datos (2020), *RGPD compliance of processing that embed Artificial Intelligence. An introduction*, 2020, https://www.aepd.es/guides/gdpr-compliance-processings-that-embed-ia.pdf, accessed on 15 March 2025.
3. Edwards, Lilian & Michael Veale (2017), „*Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For".* 16 *Duke Law & Technology Review,* pp. 18-84.
4. Forbrukerradet*, Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy,* 2018, https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf, accessed on 15 March 2025.
5. Järveläinen, Jonna, Duong Dang, Mike Mekkanen, and Tero Vartiainen. 2025. "Towards a Framework for Improving Cyber Security Resilience of Critical Infrastructure against Cyber Threats: A Dynamic Capabilities Approach." *Journal of Decision Systems* 34 (1). doi: 10.1080/12460125.20 25.2479546.
6. Opre, Ancuţa Gianina & Simona Șandru, „The right to be forgotten on the internet, a means of combating discrimination" in M. Tomescu (ed.), *Non-discrimination and equal opportunities in contemporary society*, Pro Universitaria Publishing House, Bucharest, 2015.
7. Polito, Carolina & Lorenzo Pupillo (2024), „Artificial Intelligence and Cybersecurity", *Forum Journal*, Volume 59, No. 1, p. 10-13.
8. Rodrigues, Rowena, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities." *Journal of Responsible Technology* 4 (December 2020): 100005. https://doi.org/10.1016/j.jrt.2020.100005.
9. Solove, Daniel J., *The digital person. Technology and Privacy in the Information Age,* New York University Press, 2004, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications, accessed on

15 March 2025.

10. Srinivasan, R., M. Kavitha, R. Kavitha, and S. Uma (2023). "Cybersecurity and Artificial Intelligence: A Systematic Literature Review." In Sugumaran D, Souvik Pal, Dac-Nhuong Le, Noor Zaman Jhanjhi (eds.), *Recent Trends in Computational Intelligence and Its Application.*Proceedings of the 1st International Conference on Recent Trends in Information Technology and its Application (ICRTITA, 22) 1st ed., CRC Press, London, https://doi.org/10.1201/9781003388913.
11. Stancu, Adriana Iuliana (2024). „Combating The Financing Terrorism: an Analysis of the EU Regulatory Framework and Enforcement Mechanism", in Ojars Sparitis (ed.), *Proceedings of 11th SWS International Scientific Conference on Social Sciences - ISCSS 2024*, SGEM WORLD SCIENCE (SWS) Scholarly Society, DOI: 10.35603/sws.iscss.2024/s02/06.
12. Working Party, "Article 29" *On Data Protection*, *Guidelines on automated individual decision-making and profiling under Regulation (EU) 2016/679*, Adopted on 3 October 2017 as last revised and adopted on 6 February 2018, https://ec.europa.eu/newsroom/document.cfm?doc_id=47742, accessed on 15 March 2025.