New Perspectives in Science Education
International Conference
NEW PERSPECTIVES in SCIENCE EDUCATION


Improving the Safety Posture of Italian Research Sector in Light of New European Regulatory Frameworks

Serena Montefusco[1], Matteo Bernardini[2], Paolo Micozzi[3]

[1] HSPI S.p.A., Italy
[2] HSPI S.p.A., Italy
[3] Ministry of University and Research, Italy

Abstract

Modern cybersecurity needs have highlighted the importance of ensuring the security of data and applications from cyberattacks as well as to guarantee the national security of states [1]. This research explores the integration of training, awareness, and digital communication as tools for increasing the security level of organizations, with particular attention to the Italian research sector. The article analyzes how the correct use of these elements can mitigate the risk deriving from cyber attacks, guarantee the confidentiality and integrity of sensitive information, and protect critical infrastructures, while aligning with broader cybersecurity policies of the European Union [2]. The study begins by outlining the evolution of the relevant European legislation aimed at adopting effective and proactive security strategies, also taking into account the growing use of artificial intelligence [3]. The study continues contextualizing these recent compliance rules with reference to the Italian research sector, examining the systemic challenges they introduce, both in terms of compliance and the upskilling and reskilling of internal personnel within public organizations [4]. The study focuses on the Italian Ministry of University and Research program aimed at completing the Cybersecurity Strategy and compliance with the NIS2 regulation, detailing the related transfer of training courses, specialist consultancy and cyber knowledge to higher education institutions, necessary to promote and mitigate cyber risk, also considering a systemic training for the benefit of students, researchers and teachers [5]. Drawing on the experience gained by the Ministry of University and Research, this article offers concrete insights for policymakers, the research community, and industry professionals, proposing an applicable and replicable best practice model to enhance cyber posture, promote a culture of secure innovation, and improve stakeholders' digital skills. The adoption of these strategies can lead the research community, specifically, and the Italian public administration, in general, to improve their cyber resilience and position themselves as centers of excellence in relation to their global competitors.

Keywords: *cybersecurity, upskilling, reskilling, digital communication, security*

1. Introduction

Over the past decade, Italy has experienced a significant acceleration in digital development and transformation processes. This progress has occurred despite the persistence of a structural gap compared to the European average in terms of digital infrastructure, skills, and levels of digital adoption, as highlighted by the Digital Economy and Society Index (DESI) [4]. This evolving landscape has increasingly underscored the need to define an integrated national cybersecurity governance model capable of effectively coordinating stakeholders, policies, and instruments for the prevention, mitigation, and response to cyber risk. Within this context, several sectors have proven to be particularly exposed to cyber threats. Among these, the healthcare sector stands out, alongside the education and research sector, which has become increasingly vulnerable due to the high concentration of sensitive data, the presence of distributed infrastructures, and a high degree of digital interconnection. This research specifically focuses on the research and higher education sector, which is characterized by complex technological infrastructures, strong international connectivity, and the intensive use of sensitive data with high strategic value. Beyond traditional technological data protection measures, there is a growing recognition of the need to adopt an integrated cybersecurity approach that combines governance frameworks, capacity building, awareness-raising initiatives, and digital communication strategies. In this perspective, the human factor plays a central role. Upskilling and reskilling initiatives targeting technical-administrative staff, faculty members, students, and

researchers represent essential levers for strengthening the overall security posture and reducing systemic cyber risk [3],[4].
Building upon an analysis of the relevant literature and the evolving European and Italian regulatory framework on cybersecurity, this study presents the Cyber Sapere program promoted by the Ministry of University and Research as part of the completion of the National Cybersecurity Strategy and the alignment with the NIS2 Regulation [3]. The research examines the mechanisms for skills transfer and awareness enhancement, the associated training pathways, and the outcomes of phishing simulation campaigns conducted over the past three years within higher education institutions, with program completion planned for 2026. The overarching objective is to foster a widespread, structured, and sustainable culture of cybersecurity. From this standpoint, the study aims to demonstrate how the governance strategies and cybersecurity capacity-building initiatives adopted by the Ministry of University and Research can contribute to strengthening the cyber resilience of research institutions and public administrations, in alignment with the regulatory framework established by the NIS2 Directive.

2. Literature Review

The literature highlights a progressive shift toward multilevel governance approaches, in which normative, institutional, technological, and capacity-building dimensions are deeply interconnected. In the Italian context, several studies examine the evolution of the national cybersecurity architecture and the protection of critical infrastructures, emphasizing the strengthening of institutional coordination and the increasingly central role of the State in defining cybersecurity strategies [1],[6]. These contributions are situated within a broader debate on transnational cybersecurity governance, which underscores existing asymmetries in national capabilities and the challenges associated with cyber capacity building, particularly about the dissemination of skills and resources across public and strategic sectors [7]. Within this framework, the implementation of the NIS2 Directive represents a critical turning point for essential and important sectors, requiring the reinforcement of IT governance models, risk management practices, and organizational accountability structures [8]. In parallel, the literature on cyber resilience emphasizes the importance of a systemic approach that integrates technical, organizational, and human measures, highlighting how the protection of critical information infrastructures also depends on the ability of institutions to learn, adapt, and evolve over time [9].
A more recent strand of research investigates the contribution of advanced technologies, particularly artificial intelligence, to strengthening cybersecurity and supporting models of sustainable digital development, while simultaneously drawing attention to persistent ethical and governance-related challenges [10]. However, despite the extensive focus on regulatory, technological, and training-related dimensions, the literature reveals a notable lack of integrated empirical studies assessing the effectiveness of governance and capacity-building strategies within the Italian public administration. This gap is particularly evident in the domains of public research and higher education, especially when examined in light of the new requirements introduced by the NIS2 regulatory framework [11].

3. Methodology

The data presented in the following paragraphs derive from the initiatives undertaken by the Ministry of University and Research within the framework of the Cyber Sapere program.
The Cyber Skill Assessment involved, from January to February 2025, the administration to the technical-administrative staff of universities and Institutions of Higher Education in Art, Music and Dance (AFAM - *Alta formazione artistica, musicale e coreutica)*, as well as to personnel of the Ministry, of an individual online questionnaire consisting of 15 technical questions covering the main thematic areas of cybersecurity. The results defined an Awareness Level according to the following thresholds: from 0 to 12 points, beginner level – from 13 to 20 points, intermediate level – from 21 to 25 points, expert level.
The asynchronous e-learning training course was delivered, through a specialized online service in cybersecurity domains, to employees of the Ministry of University and Research, from July 2025 to December 2025.

The synchronous e-learning training course was delivered, through an online platform, to the technical-administrative staff of universities and AFAM institutions and to personnel of the Ministry, from September 2025 to November 2025.
The in-person training courses were delivered by qualified instructors to technical-administrative staff and students at selected universities, as well as to personnel of the Ministry, from September 2025 to December 2025.

For all the aforementioned training courses, an individual satisfaction questionnaire was administered to participants, consisting of several questions, depending on the specific course attended. For each question, respondents were asked to express an evaluation using a rating scale ranging from 1 to 5 points. The average of the scores represented the level of user satisfaction. The questionnaires were completed anonymously, and the collected responses were not used for evaluative purposes, but with the aim of improving future training initiatives.
The three phishing campaigns conducted involved the technical-administrative staff of universities and AFAM institutions and personnel of the Ministry from June 2025 to December 2025, through individual email messages. The percentage of users who clicked on the link contained in the received email compared to the total number of emails sent represents the Click Rate of the campaign. The results defined an Awareness Level according to the following thresholds: from 3 to 5 points, beginner level – from 6 to 8 points, intermediate level – from 9 to 10 points, expert level.
The informational brochures were distributed to the technical-administrative staff of universities and AFAM institutions and to personnel of the Ministry from May 2025 to December 2025, through individual email communications.

4. The New European and Italian Regulatory Framework for Cybersecurity

Over the past decade, cybersecurity has been the subject of a significant proliferation of regulatory instruments, driven by strong legislative momentum at both the European [12] and national levels [13]. The prominence that cybersecurity has assumed within the supranational and Italian regulatory landscape highlights the importance that both the European Union and Italy attribute to this domain [14]. The long and ongoing process of improving cybersecurity posture and data protection experienced an initial and significant acceleration with the adoption of Directive (EU) 2016/1148 (NIS 1) and Regulation (EU) 2016/679 (GDPR) [15], followed by Regulation (EU) 2019/1020 and Directive (EU) 2020/1828 on cyber resilience. These general regulatory instruments were subsequently complemented by additional sector-specific and thematic legislation. Italy, as a Member State [16], has likewise strengthened its cybersecurity posture, both by transposing European directives and through autonomous legislative initiatives, such as the establishment of the National Cybersecurity Perimeter (PSNC) [17]. In 2022, a second and more substantial reinforcement of the European cybersecurity regulatory framework took place. The aforementioned legislation was revised through complex regulatory processes [18], and new, more comprehensive and far-reaching rules were adopted [19]. This forward-looking approach enabled the initiation and renewal of processes aimed at strengthening both cyber and human defenses [20], particularly in light of emerging threats related to artificial intelligence. Indeed, in the short term, threat actors are expected to benefit more significantly from the use of AI for illicit purposes and malicious activities than defensive organizations will be able to do [21]. In this context, the implementation of the NIS 2 Directive [2], together with its national transposition through Legislative Decree No. 138/2024 and the additional measures adopted by the National Cybersecurity Agency (ACN – *Agenzia per la Cybersicurezza Nazionale*), assumes relevance. Specific attention is given to the implementation of Article 24 of Legislative Decree No. 138/2024 [22] and to the systemic challenges introduced under multiple profiles, encompassing both compliance requirements and the identification of specific operational activities, as well as responsibilities related to training.
Both regulatory texts place particular emphasis on training and awareness-raising, targeting not only the administrative and governing bodies of NIS entities with regard to cyber risks and threats, but also employees and collaborators of the organizations more broadly.
Evidence of this focus is provided by Article 23 of Legislative Decree No. 138/2024, which transposes Article 20 of NIS 2 and mandates structured and systematic cybersecurity training for senior management, alongside the promotion of a structured training offer for employees. In line with the EU

Cybersecurity Strategy, the objective is to foster the acquisition of adequate knowledge and skills related to cyber risks and their management.
Ultimately, the European Union has firmly emphasized the need to develop a workforce that is not only adequately prepared in the field of cybersecurity, but also specialized, to ensure robust regulatory compliance and operational resilience [23].
Italy has adopted further implementing measures, such as Annex 2 to ACN Determination No. 379887 of 2025 and subsequent amendments and integrations. Training and awareness are considered so fundamental that the ACN has extended these requirements to the supply chain [24] and has dedicated a specific requirement to this area, identified by the code “PR.AT”. This requirement mandates the adoption and documentation of cybersecurity policies related to awareness and training, as well as the definition, implementation, updating, and documentation of a training plan that includes, at a minimum, the planning of activities, the specification of content, and the methods for verifying the acquisition of knowledge. In addition, awareness-raising activities in cybersecurity and training on the skills and knowledge necessary to perform one’s duties while taking cyber risks into account are required. Furthermore, the regulation requires that top management approve the training plan and oversee its effective implementation by consulting training activity records. An important sector-specific provision has been introduced for individuals holding specialized roles. For these profiles, such as system administrators, dedicated and targeted training is required with regard to the configuration and operation of information and network systems, cyber threats, and instructions on appropriate behavior in the event of security-relevant incidents [25].

5. Upskilling and Reskilling as Enabling Factors for a Proper Security Posture

To ensure an adequate cybersecurity posture, upskilling and reskilling are considered strategic levers: the former aims to enhance existing digital skills in order to address the growing cyber threats [26], while the latter focuses on reorienting professional profiles toward security roles and bridging the existing skills gap [4]. The rapid evolution of cyberattack typologies (ransomware, AI-driven attacks, supply-chain threats, etc.) targeting individuals and organizations [27] risks rendering defensive tools and response approaches obsolete in the absence of continuous skills updating, thereby undermining the effectiveness of incident response methodologies for complex attacks. In this context, the rapid introduction of artificial intelligence brings additional cyberattack vectors [3], such as automated attacks, advanced phishing and social engineering techniques, deepfakes, and increasingly credible and targeted disinformation campaigns. Moreover, AI enables the rapid creation and adaptation of malware and evasive attacks capable of bypassing traditional defense systems and exploiting vulnerabilities more effectively. A further threat is associated with the risk of AI model abuse, including data manipulation, ethical dilemmas, and the improper use of autonomous systems in critical environments.
In a context characterized by a pronounced shortage of digital and cybersecurity skills, reskilling represents a strategic lever for organizations. Through structured professional requalification pathways, it is possible to transition resources from adjacent IT domains into specialized cybersecurity roles [4]. This approach not only accelerates the coverage of critical positions, but also significantly reduces the time and costs associated with recruitment processes [28]. Furthermore, it limits dependence on external consultancy, fostering a more sustainable and coherent management of human capital and enhancing the value of internal professional expertise. Reskilling enables the valorization of existing competencies, strengthening employees’ sense of belonging and motivation. At the same time, it contributes to the development of an organizational culture oriented toward continuous learning and adaptation to emerging digital threats, thereby improving the overall security posture. Structured training programs represent an enabling factor for addressing the challenges posed by digital transformation in a conscious and effective manner. They support the adoption of emerging technologies such as agentic AI, cloud architectures, 5G, and the Internet of Things. Through upskilling and reskilling pathways, organizations develop technical and managerial competencies aligned with these new digital ecosystems. At the same time, such programs contribute to mitigating operational risks associated with the widespread adoption of highly interconnected platforms and services, strengthening, in particular, the security of cloud-native infrastructures and promoting the adoption of advanced identity and access management models.

Organizational culture and internal awareness represent strategic elements of an organization's cybersecurity posture, as they extend beyond purely technical aspects to encompass processes, behaviors, and governance models. In this context, continuous training programs play a fundamental role in promoting widespread awareness and shared responsibility with respect to cyber risks. Through ongoing update and awareness-raising activities, employees develop an enhanced ability to recognize threats such as phishing and the improper use of information. This contributes to reducing human error, which is often a primary cause of security breaches. At the same time, training fosters more effective collaboration between IT, business, and compliance functions, strengthening alignment between operational needs and data protection requirements. In this way, the organization consolidates an integrated approach to security, in which skills, behaviors, and governance converge toward a common objective: ensuring long-term resilience and protection.

6. The Approach of the Sector Authority of the Ministry of University and Research

Within the context of the Italian research system, the Ministry of University and Research has been designated as the NIS Sector Authority pursuant to Article 11 of Legislative Decree No. 138/2024, with the task of supporting, through its sector-specific expertise, the functions of the National Competent NIS Authority. Its responsibilities include validating the list of NIS entities within its sector of competence, proposing additional governmental designations where appropriate, coordinating sector-specific working groups, and fostering cooperation at both national and international levels (e.g., with other Member States, ENISA, and the European Commission).
The Italian research sector is highly heterogeneous, comprising a wide range of public and private actors, including authorized research institutes, universities, Institutions of Higher Education in Art, Music and Dance (AFAM), as well as research bodies and institutions. Within this landscape, the level of cybersecurity posture is equally variable and diversified.
By virtue of its dual role as an entity subject to the obligations established by the NIS2 regulatory framework and, at the same time, as the sector authority for the research domain, the Ministry has launched a set of synergistic and coordinated initiatives aimed at strengthening the overall cybersecurity posture. These actions are intended not only to enhance the Ministry's internal levels of organizational, technological, and procedural security, but also to provide systematic support to the reference research entities by promoting training and the adoption of shared models, tools, and practices for cyber risk management [28]. Within this framework, the Ministry assumes a guiding and facilitating role, fostering the dissemination of a structured and informed approach to digital security across the entire national research ecosystem.
Within the framework of the National Cybersecurity Strategy 2022–2026 [29], the Ministry of University and Research launched the program entitled Cyber Sapere, aimed at strengthening cybersecurity culture and developing targeted skills among its own personnel, as well as the technical-administrative staff and students at universities and AFAM institutions. The program, scheduled to conclude in 2026, has implemented a structured set of initiatives articulated along two main lines of action: on the one hand, strengthening staff competencies through training and awareness-raising activities; on the other, improving the security level of internal infrastructures through technical activities focused on prevention, monitoring, and verification.

6.1. Cyber Skill Assessment

The program included a preliminary Cyber Skill Assessment activity aimed at understanding the level of knowledge and familiarity with cybersecurity-related topics. The assessment made it possible to identify both the areas in which competencies were less consolidated and those exhibiting a higher level of maturity. The results obtained enabled the definition of the training plan and the identification of content and in-depth topics aligned with the actual needs of the target audience. The following table highlights the main results of the Cyber Skill Assessment questionnaire.

Type of entity	Entities involved	Users involved	Certificates issued	Awareness level
Universities	103	11.413	14/25	Intermediate
AFAM	129	1.299	14/25	Intermediate
Ministry	1	141	13/25	Intermediate
Totals & Media	233	12.853	14/25	Intermediate

6.2. Asynchronous e-Learning Training Course

Based on the outcomes of the Cyber Skill Assessment, the Ministry made available an asynchronous e-learning training platform dedicated exclusively to its internal staff. The distinctive feature of this asynchronous course, with a total duration of 27 hours, lies in its foundation on a continuous micro-learning approach, providing short, clear, and progressively structured multimedia content, thereby fostering effective learning aligned with principles of cognitive load sustainability.
In 2025, the first two of the three planned training modules—the basic and intermediate levels—were delivered, for a total of 15 hours, while the advanced module will be made available in 2026. The following table highlights the main results achieved so far by the asynchronous e-learning training course.

Type of entity	Entities involved	Users involved	Certificates issued	User satisfaction
Ministry	1	389	214 [1]	N/A

6.3. Synchronous e-Learning Training Course

A synchronous online training course was delivered with a total duration of 32 hours (8 sessions of 4 hours each). The course, delivered by instructors in a virtual classroom setting, was developed according to a modular approach, aimed at progressively supporting technical-administrative staff in the acquisition and consolidation of cybersecurity competencies. In particular, the training pathway was divided into two macro-modules: the first focused on fundamental principles and the theoretical foundations of cybersecurity, with content accessible also to participants with no prior experience; the second module provided an in-depth exploration of technical and specialized topics, such as Cyber Threat Intelligence activities and the use of tools supporting the prevention of and response to cyber threats. The following table highlights the main results of the synchronous e-learning training course.

Type of entity	Entities involved	Users involved	Certificates issued	User satisfaction
Universities AFAM	100 148	1.151 781	974 435	3,80 / 5,00 [2]
Ministry	1	38	35	4,05 / 5,00 [3]
Totals & Media	249	1.969	1.444	3,82 / 5,00

6.4. In-person Training Course

With specific reference to the target group of students, six training events were delivered in 2025, two hosted at the Ministry and three hosted at three Italian universities, each with a duration of 2 hours. During the sessions, the main cybersecurity topics were addressed with interactive digital tools based on edugame mechanisms, including quizzes and simulations. This approach was adopted to stimulate active participation and foster a higher level of engagement among participants, based on the assumption that educational game-based approaches may offer advantages over conventional teaching methods [30]. The following table highlights the main results of the in-person training course.

Type of entity	Entities involved	Users involved	Certificates issued	User satisfaction
Universities Ministry	3 1	75 39	75 30	4,65 / 5,00 [4] 4,28 / 5,00 [5]
Totals & Media	4	114	114	4,42 / 5,00

[1] 115 diplomas for the basic level and 99 diplomas for the intermediate level
[2] 344 users responding to the questionnaire (AFAM University)
[3] 22 users responding to the questionnaire
[4] 22 users responding to the questionnaire
[5] 37 users responding to the questionnaire

6.5. Phishing Campaigns

In support of the training offer, three simulated phishing campaigns were conducted in 2025, aimed at verifying the effective assimilation of the skills acquired and training personnel to recognize and appropriately handle potential attempts to compromise information systems. The following table highlights the main results of the phishing campaigns.

	Type	Entities involved	Users involved	Click Rate	Awareness level
Campaign 1	Universities AFAM Ministry	33 26 1	21.343 1.234 398	8% 26% 30%	7–Intermediate 5-Beginner 5-Beginner
	Totals & Media	60	22.975	9%	8–Intermediate
Campaign 2	Universities AFAM Ministry	28 18 1	17.700 679 302	13% 18% 10%	6–Intermediate 5-Beginner 7- Intermediate
	Totals & Media	47	18.681	14%	6– Intermediate
Campaign 3	Universities AFAM Ministry	19 15 1	10.252 620 302	7% 14% 10%	7– Intermediate 6- Intermediate 5- Intermediate
	Totals & Media	35	11.174	10%	7– Intermediate

6.6. *Informational Brochures*

To complement the training activities described above, during 2025 the Ministry oversaw the dissemination of six periodic informational brochures, aimed at promoting informed behaviors and contributing to the development of a safer and more resilient digital environment within public administrations. These brochures were shared not only within the Ministry, but also with the higher education institutions involved in the Cyber Sapere program.

7. Conclusion

In the near future, cybersecurity will be required to address increasingly complex challenges, driven by the growth of automated and artificial intelligence–enhanced attacks capable of rapidly adapting and targeting critical infrastructures and distributed systems. The continuous expansion of cloud computing, IoT, and hybrid environments will further enlarge the attack surface, making it more difficult to ensure control, resilience, and data protection across the entire digital value chain. An additional critical factor will be the shortage of specialized skills, which will necessitate structured investments in training and in the promotion of a security culture at all organizational levels.

Within this context, upskilling and reskilling represent fundamental levers for minimizing the risks associated with cybersecurity challenges. Through the Cyber Sapere program, the Ministry of University and Research aims to mitigate the cybersecurity skills gap and to enhance the security posture of participating stakeholders. Although the program is scheduled to conclude in 2026, at the time of writing the partial results achieved are already substantial and constitute a valuable basis for measurement and comparison. The body of information currently being accumulated by the Cyber Sapere program represents a unique asset within the research sector in terms of scope and completeness. It enables not only the comparison of cyber awareness levels among the various actors involved, but also the design of tailored remediation plans aligned with the actual needs of institutions and individual personnel.

The high level of participation in the proposed training activities confirms a strong interest in specialized cybersecurity education, perceived as essential for the effective performance of professional roles. Participant feedback further indicates a clear preference for non-traditional training formats, with a stronger focus on multimedia micro-learning content and educational game-based approaches.

The results of the initial Cyber Skill Assessment indicate an overall medium level of security posture for both universities and AFAM institutions, while a significant difference emerges in the outcomes of phishing campaigns between universities and AFAM institutions on the one hand and the Ministry on

the other, in favor of greater awareness among the former. Assuming the statistical sample to be reliable, this result is, at present, difficult to explain other than by considering endogenous factors that generate distinct sensitivity toward the proposed campaigns. At the conclusion of the program period and following the additional phishing campaigns planned under the Cyber Sapere initiative, this heterogeneity of results may be further investigated to identify the underlying characteristics that have contributed to its emergence.

REFERENCES

[1] De Zan, Tommaso, Giampiero Giacomello, and Luigi Martino. “Italy’s Cybersecurity Architecture and Critical Infrastructure.” Routledge Companion to Global Cyber-Security Strategy, edited by Mary Manjikian and Scott Romaniuk, Routledge, 2021, pp. 121–131.

[2] European Cyber Security Organisation, “NIS2 Implementation: challenges and priorities.”, 2025. https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf

[3] Wenbo, G., Yujin, P., Tianneng, S., Zhun, W., Andy, Z., Dawn, S., “Frontier AI's Impact on the Cybersecurity Landscape.”, Arxiv, 2025. https://doi.org/10.48550/arXiv.2504.05408

[4] Micozzi, P., Montefusco, S., “Digitalization of Services and the Creation of New Barriers: Upskilling and Reskilling as a Way to Mitigate the Digital Divide.” In Firenze Pixel, The Future of Education Conference Proceedings 2025. Filodiritto Publisher, 2025, 561-567. doi: https://doi.org/10.26352/L625_2384-9509

[5] Tolossa, N. D., “Importance of Cybersecurity Awareness Training for Employees in Business. Vidya”, A Journal of Gujarat University, 2023, 2. 104-107. https://doi.org/10.47413/vidya.v2i2.206.

[6] Martino, L. “Evolution of Italy’s National Cybersecurity Governance. In: Cybersecurity in Italy.” SpringerBriefs in Cybersecurity. Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-64396-5_4

[7] Calderaro, A.and Craig, A. J. S. “Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building.” Third World Quarterly, 2020, 41 (6), 917-938. 10.1080/01436597.2020.1729729

[8] Matīss V., Lasmanis L., and Romānovs A. “IT Governance in Critical Sectors: Towards the NIS2 Implementation.” 2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), 2024, 1-7.

[9] Tiirmaa-Klaar, H. “Building national cyber resilience and protecting critical information infrastructure.” Journal of Cyber Policy, 2016, 1(1), 94–106. https://doi.org/10.1080/23738871.2016.1165716

[10] Lezzi, M., Montefusco, P., Lazoi, M., & Corallo, A. “AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions.” Journal of Industrial Information Integration, 2025, 48, 100980. https://doi.org/10.1016/j.jii.2025.100980

[11] Pramod, D. Gamification in cybersecurity education; a state of the art review and research agenda. Journal of Applied Research in Higher Education, 2025, Vol. 17 No. 4 pp. 1162–1180. doi: https://doi.org/10.1108/JARHE-02-2024-0072

[12] Casolari F., Ferri F., Villani S., “La costituzionalizzazione della cybersicurezza nell’ordinamento dell’Unione europea”, in “Governare la sicurezza degli (eco)sistemi cyberfisici – Regolamentazione, diritti e Politiche” ed. Brighi R., Adinolfi G., Giappichelli Editore, 2025, 27-49.

[13] Cfr. fra gli altri Serini F., “La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021”, in Federalismi.it, 2022, 12: 241-272.

[14] Matassa M. “Sicurezza cibernetica e nazionale nell’ordinamento multilivello: quale possibile convivenza”, in “Cybersecurity e Istituzioni democratiche un’indagine interdisciplinare: diritto, informatica e organizzazione aziendale - Vol. 1 No. 30 TCRS 1/2025 - Teoria e Critica della Ragione Sociale”, ed. Heritier P. e Rossa S., Mimesis, 2025, 73-86.

[15] Markopouloua D., Papakonstantinoua V., De Hert P. “The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation”, Computer law & security review, 2019. https://doi.org/10.1016/j.clsr.2019.06.007

[16] Niels Vandezande, “Cybersecurity in the EU: How the NIS2 Directive stacks up against its

predecessor", Computer Law & Security Review: The International Journal of Technology Law and Practice, Volume 52, 2024, 10.

[17] Previti L. "Convergenze e deviazioni in materia di cybersicurezza: implicazioni sistematiche e nuovi interrogativi", in "Cybersecurity e Istituzioni democratiche un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale - Vol. 1 No. 30 TCRS 1/2025 - Teoria e Critica della Ragione Sociale", ed. Heritier P. e Rossa S., Mimesis, 2025, 107-122.

[18] Cfr. fra gli altri Chiara P.G. "IlCyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", Rivista italiana di informatica e diritto, 2023, 144-151. https://doi.org/10.32091/RIID0108

[19] Cfr. Capo IV, artt.20-25, Direttiva (UE) 2022/2555 (NIS2), Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione, in G.U.U.E. L 333, del 27 dicembre 2022.

[20] Fioriglio G., "Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone", i-lex - Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale. Vol. 18 n. 2, 2025. https://doi.org/10.60923/issn.1825-1927/22648

[21] Wenbo, G., Yujin, P., Tianneng, S., Zhun, W., Andy, Z., Dawn, S. (2025). Frontier AI's Impact on the Cybersecurity Landscape. Arxiv. https://doi.org/10.48550/arXiv.2504.05408

[22] Cfr. fra le altre Determine ACN nn. 370977 e 379887 del 2025.

[23] Adamos K., Di Franco F., Leventopoulos S., "Cybersecurity roles and skills for nis2 essential and important entities", European Union Agency for Cybersecurity (ENISA), 2025, 5.

[24] Det. ACN n. 379887 del 2025, Allegato 2, requisito 1.5.1.1 "Gestione del rischio di cybersecurity della catena di approvvigionamento" (GV.SC.01-01).

[25] Det. ACN n. 379887 del 2025, Allegato 2, requisiti 3.2 "Consapevolezza e formazione" (PR.AT.01 e PR.AT.02).

[26] Sandi, S., & Van den Berg, C. L. "Cybersecurity mindset and upskilling: Resilience via lifelong learning and security education." South African Journal of Information Management, 2025, 27(1), a2044. DOI: 10.4102/sajim.v27i1.2044

[27] Rapporto Clusit – Aggiornamento di ottobre 2025 - https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_aggiornamento_10-2025_web.pdf

[28] Totobayo, B. W., Rajkaran, S., & Ntuli, C. "Cost of reskilling employees versus the profitability of a business: a reflection on selected small businesses in Mthatha, Eastern Cape." International Journal of African Reflections: Multi-, Inter- and Transdisciplinary Perspectives, 2024. https://doi.org/10.47348/IJAR/2024/a4

[29] Strategia Nazionale di Cybersicurezza - https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

[30] Wang, LH., Chen, B., Hwang, GJ. et al. "Effects of digital game-based STEM education on students' learning achievement: a meta-analysis." IJ STEM, 2022, Ed 9, 26. https://doi.org/10.1186/s40594-022-00344-0