Libera Università Internazionale
degli Studi Sociali Guido Carli

LUISS

TECHNICAL SHEET A

Technical Sheet A attached to Rectoral Decree No. 243 of 4/8/2025

Project title	Security Strategies for Artificial Intelligence: Metrics, Processes, and Organizational Practices.	
Research and Innovation Topics on Cybersecurity **(Areas explored in the research project)**	**Subject 1**	Subject#6.2.1: The study and continuous enhancement of procedural frameworks for risk assessment, aimed at facilitating the identification, analysis, and quantification of risk, thereby rendering the related treatment plan (and the acceptance of risk where reasonable) more effective. In particular, this R&I topic includes models for impact assessment.
	Subject 2	Subject#6.3.1: Innovation in the standardization of business processes for cybersecurity, leveraging, for example, Capability Maturity Models (CMM) and zero trust security models.
	Subject 3	Subject#6.1.1: Research on the cybersecurity ecosystem economy, particularly on supply chains.
PROJECT GOALS AND IMPLEMENTATION CAPABILITIES		
Project goals	The security of Artificial Intelligence represents a crucial challenge for organizations, which must balance the protection of systems with the economic sustainability of investments and the need to adopt standardized practices. This research project aims to develop an integrated framework to assist companies and policymakers in managing AI-related risks through economic assessment tools, security maturity models, and market incentives. A primary objective is the application of Return on Security Investment (ROSI) as a strategic decision-support tool, enabling managers to allocate resources for AI protection proportionally to risk and consistent with governance and regulatory requirements. The analysis of specific risks related to	

	generative AI will enable the development of metrics to guide the optimization of investments, ensuring a balance between costs, benefits, and the achieved level of security. Simultaneously, the project explores the role of the Capability Maturity Model (CMM) as a lever to promote security in AI markets. Maturity models provide a structured framework to progressively improve protection capabilities, encouraging both organizations offering AI-based services and policymakers to adopt shared standards. From this perspective, the project proposes the development of an AI Security Index—an indicator designed to measure the security level of enterprises along the AI supply chain, incentivizing the continuous improvement of cybersecurity practices. Finally, the project incorporates a reflection on the economics of cybersecurity and security along AI supply chains. Considering the protection of AI systems not only at the organizational level but as a common goal of the entire ecosystem highlights the role of security investments in the resilience of digital supply chains. The combination of ROSI, AI Security Index, and security governance will help define more effective strategies to protect critical AI infrastructures and promote greater collaboration among companies, suppliers, and institutions. Through this integrated approach, the project aims to provide practical and theoretical tools for more effective management of AI security, fostering convergence between economic assessment, security governance, and standardization in the markets.
Relevance of the project to the topics of the Agenda	The project aligns with three key themes of the Research Agenda, offering both theoretical and practical contributions on risk assessment, security standardization, and the management of digital supply chains. Firstly, the project addresses Topic 6.2.1, which concerns the study and continuous improvement of procedural frameworks for risk assessment. The integration of ROSI enables the development of metrics to quantify the specific risks of generative AI and evaluate the economic impact of security strategies. This approach will contribute to more effective risk

	identification, analysis, and mitigation, rendering the treatment plan more structured and sustainable. Secondly, the project is consistent with Topic 6.3.1, related to innovation in the standardization of business processes for cybersecurity. The use of the CMM provides a model to measure and incentivize the progressive improvement of AI security, facilitating the adoption of shared practices. Furthermore, the development of the AI Security Index represents an innovative contribution, as it enables the evaluation of AI security maturity within organizations and creates incentives for the continuous enhancement of protection practices. Finally, the project addresses Topic 6.1.1, which pertains to research on the cybersecurity economy and security along the supply chain. The AI Security Index can become a strategic tool to measure and incentivize security throughout the entire AI value chain, creating a market mechanism that encourages companies to adopt higher levels of protection. Integration with ROSI aligns investment choices with the need for distributed security, contributing to the resilience of the AI ecosystem as a whole.
Project implementation methods, including available enabling factors	The doctoral project spans four years, integrating theoretical research, model development, and empirical validation through collaboration with companies and institutions in the security and artificial intelligence sectors. In the first year, the candidate will acquire methodological training with advanced courses in social sciences, qualitative and quantitative analysis, and cybersecurity, along with topics on management, information systems, and digital governance. This will ensure a solid interdisciplinary foundation to address the challenges of AI security and digital risk management. In the second year, an economic assessment framework for AI security will be developed, integrating ROSI for investment decisions and CMM to improve security in AI-based markets. Simulation techniques, such as the Monte Carlo method, will also be explored to refine risk assessment metrics. Interactions with companies and stakeholders will be initiated, testing the framework through case studies. Collaboration with the Cyber

	4.0 Competence Center and the Fastweb+Vodafone Chair will facilitate access to the advanced industrial ecosystem. In the third year, the framework will be tested in organizational contexts involving generative AI, with validation of the AI Security Index aimed at measuring the security level of companies along the AI supply chain. Collaboration with the AI4Society research center will ensure a multidisciplinary environment. In the fourth year, the project will focus on finalizing the analysis by integrating feedback received through interactions with national and international academic networks, including the Cybersecurity PhD program, the ITASEC community, the Association for Information Systems (AIS), the Design Science Research (DESRIST) community, the European Research Center for Information Systems (ERCIS) network, the European Safety and Reliability (ESREL) community, and the Society for Risk Analysis Europe (SRA-E).	
<u>PROJECT ELEMENTS RELATED TO PRIORITY THEMES</u>		
PROJECT ELEMENTS RELATED TO PRIORITY THEMES	**Subject 1**	The study and continuous improvement of procedural frameworks for risk assessment, aimed at facilitating the identification, analysis, and quantification of risk, thereby rendering the related treatment plan (and the acceptance of risk where reasonable) more effective. In particular, this R&I topic includes models for impact assessment.
	Subject 2	Subject#6.3.1 Innovation in the standardization of business processes for cybersecurity, leveraging, for example, Capability Maturity Models (CMM) and zero trust security models..
	Subject 3	Research on the cybersecurity ecosystem economy, particularly on supply chains.

	The research project makes an innovative contribution to managing risks related to Artificial Intelligence (AI) and security in AI systems, with particular focus on the standardization of business processes for cybersecurity, as outlined in the Cybersecurity Research and Innovation Agenda. The developed framework will assist organizations in allocating investments for AI security by combining economic assessment and security considerations, and will be applicable at both the corporate level and for policymakers. The approach is based on Return on Security Investment (ROSI) and the AI Security Index, tools that enable the definition of priority interventions and the standardization of guidelines for AI security. This will allow public administrations and regulatory bodies to direct cybersecurity investments more effectively, using a quantitative score that links investment returns to protection against AI-related risks. Moreover, the framework will facilitate the systematic and standardized collection of data on organizational security, improving the ability to monitor and continuously strengthen security over time. This approach will ensure greater uniformity in security assessment and monitoring processes, enhancing risk management at both the enterprise and ecosystem levels, and fostering increased collaboration between the public and private sectors. The project also addresses the challenge of security governance in the adoption and development of AI technologies by combining ROSI and the Capability Maturity Model (CMM) to support strategic security investment planning. The proposed framework is positioned as a key tool to strengthen the resilience of the digital ecosystem, promoting standardization and the dissemination of best practices in cybersecurity, with a significant impact on the growth of AI applications in the market.
COLLABORATIONS WITH OTHER PUBLIC AND PRIVATE ENTITIES	
Motivation and evidence of the involvement in the research project of companies, public or private research	The project benefits from a broad network of collaborations with national and international entities and companies, providing the doctoral candidate with access to essential

institutions and laboratories linked to Italian and/or European entities, as well as international organizations	resources and ensuring a significant impact on AI security. In particular, it is embedded within the PRIN Data4Innovation project, which explored data governance in distributed environments, laying the groundwork to address challenges related to data security—a crucial theme in cybersecurity. The Fastweb+Vodafone Chair and the collaborations of the AI4Society center on AI and data governance topics, together with the Confindustria network, offer the opportunity to collect cybersecurity data by testing the security assessment framework. The direct connection between research and market will enhance the practical validity of the results. These collaborations will ensure that the proposed framework aligns with international research needs and security practices.
Undertaking a study period abroad within the European Union, contextualized to the research project	The doctoral project includes a study period abroad to be carried out at one of the universities or research centers that are members of the European alliance ENGAGE.EU, of which Luiss is a partner. The choice of the host institution will depend on the opportunities available within the network, which includes renowned European universities such as Tilburg, Mannheim, Sofia (University of National and World Economy), Toulouse Capitole, Vienna (WU), Hanken School of Economics (Helsinki/Vaasa), Ramon Llull (Barcelona), and the Norwegian School of Economics (NHH) in Bergen. During this period, the doctoral candidate will have the opportunity to collaborate with researchers engaged in digitalization topics. In particular, participation in initiatives within the Industry-Academia Network of the Cybersecurity Skills Academy, promoted by ENGAGE.EU, will allow the candidate to develop applied skills in managing the security of emerging technologies, integrating theory with practical field experience. Furthermore, the doctoral candidate will benefit from collaboration with the Department of Information Systems at the University of Agder in Norway, where an ongoing partnership focuses on cybersecurity and AI topics.
Duration of the study period abroad	4 months
Scientific coordinator	Prof. Paolo Spagnoletti