PhD Programme in ELECTRONIC AND COMPUTER ENGINEERING Curriculum 1: COMPUTER ENGINEERING AND AUTOMATIC CONTROL Curriculum 2: ELECTRONICS AND TELECOMMUNICATIONS	
DISCIPLINARY SCIENTIFIC AREA	09 - INDUSTRIAL AND INFORMATION ENGINEERING
COORDINATOR	PROF. BARBARA CANNAS
HEAD DEPARTMENT	DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
DURATION	3 years
LEARNING OUTCOMES AND RESEARCH TOPICS	The PhD programme in Electronic and Computer Engineering aims to train young researchers to make them ready to carry out academic and industrial research projects in the following areas: 1. Automatic Control 2. Bioengineering 3. Computer Engineering 4. Electrical engineering 5. Electric and Electronic Measurements 6. Electromagnetic fields 7. Electronics 8. Power Electronic Converters, Electrical Machines and Drives 9. Telecommunications The central point of the doctoral education is the development of an original research project to be carried out in close contact with the supervisor and strongly aimed to the advancement of knowledge in the relevant field of engineering. The main goal of the PhD programme is to create professionals who find suitable job placement at academic institutions, research centres, high-tech firms, and that they are potentially able to initiate economic undertaken with high scientific and technological content.
ELIGIBILITY AND OTHER REQUIREMENTS FOR CANDIDATES	EVERY ITALIAN 2ND CYCLE DEGREE (*LAUREA MAGISTRALE/SPECIALISTICA/VECCHIO ORDINAMENTO*) AND EQUIVALENT AND SUITABLE FOREIGN ACADEMIC DEGREES
ADMISSION TESTS FOR CANDIDATES APPLYING FOR THE ORDINARY POSITIONS	ASSESSMENT OF QUALIFICATIONS AND CURRICULUM VITAE, IN-PERSON INTERVIEW The interview will aim to ascertain the candidate's ability to orient on the main areas of study inherent in the doctorate and to verify his/her analytical, processing and communication skills. During the interview, a three-year research project proposed by the candidate will be discussed, which must be presented, in addition to the documents required by art. 3 of the call for applications, by uploading it to the system by the call expiry date (file name: research_project_surname_name). Candidates unable, for justified reasons, to take the interview at the established venue, may be granted the possibility of carrying it out by videoconference, on the same date and time established for face-to-face interviews, according to the procedure indicated in the notice of competition.
ADMISSION TESTS FOR FOREIGN CANDIDATES APPLYING FOR THE RESERVED POSITION	ASSESSMENT OF QUALIFICATIONS AND CV, AND ONLINE INTERVIEW During the interview, a three-year research project proposed by the candidate will be discussed, which must be presented, in addition to the documents required by art. 3 of the competition announcement (certificate attesting the award of a 2nd level foreign degree needed to access a PhD programme, including exams and marks, with a translation in Italian or English; certificate

	attesting the award of a 1st level foreign degree, including exams and marks, with a translation in Italian or English; signed Curriculum Vitae preferably in EU format, in English or Italian; additional qualifications, certifications, publications; copy of a valid passport), by uploading it to the system, by the expiry date of the announcement (file name: research_project_surname_name). The interview can also be conducted in English. Reference letters (up to 3) must be written in English, using the form available on the webpage https://web.unica.it/unica/en/studenti_s01_ss05.page (How to apply for PhD selection: Guidelines and forms- Annex D), by a university professor or an expert in the research fields of the PhD programme, on letterhead of their institution, dated and signed. Evaluators will send their letters directly to the email address phdcall_referenceletter@unica.it (object: surname and name of the candidate being evaluated and name of the PhD programme for which he/she is applying).
POSITIONS	14, 2 of which without scholarship, and 4 reserved as follows: • 1 for a foreign candidate with a 2nd level degree awarded abroad; • 2 for scholarship holders under Grant Agreement no. 101168796 - FITNESS project - HORIZON-MSCA-2023-Doctoral Networks (DN) - 01 - CUP F23C24000620006 - Positions DC8 (Contact person and co-PI: Marco Martalò) and DC9 (Contact person and co-PI: Virginia Pilloni) • 1 for a scholarship holder from a foreign country
SCHOLARSHIPS	9: - 1 funded by the University of Cagliari (funds from Regional Law no. 7 of 7.8.2007, allocated to the University pursuant to Regional Council Resolution no. 45/84 of 27.11.2024) – CUP F23C24001130002 - 1 funded with funds from the Department of Electric and Electronic Engineering (RICALTRO_WP_2023_AISAC_PERSONALE_FANTI) - 6 funded with funds from PR FSE+ 2021-2027 (PNR 2021-2027 research and innovation area: Health; Security for Social Systems; Digital, Aerospace Industry; Climate, Energy, Sustainable Mobility; Food, Bio-economy, Natural Resources, Agriculture, Environment - S3 Specialisation Area: Aerospace, Agro-industry, Biomedicine, ICT, Smart Networks for Efficient Energy Management; Tourism, Culture and Environment): • 3 on Line A, reserved for university female and male graduates under 35 years at the time of application • 3 on Line B, reserved exclusively for university female graduates under 35 years at the time of application - 1 in the field of cybersecurity funded by the National Cybersecurity Agency (CUP F22B25000220005). Project title: *Measuring the risk of new threats through generative AI* (project ID: 132771_166_UniCA). Scientific supervisor: Prof. Giorgio Giacinto. The PhD student awarded the scholarship funded by the Agency will be required to carry out the research project in line with the details provided below.
CONTACT PERSON	PROF. BARBARA CANNAS EMAIL: barbara.cannas@unica.it - TEL. +39 0706755858
WEBSITE	https://web.unica.it/unica/en/phd_200_1111.page

<table>
<tr><th colspan="3">Information about the scholarship funded by the National Cybersecurity Agency</th></tr>
<tr><td rowspan="4">Research and Innovation Topics on Cybersecurity</td><td>Topic 1</td><td>2.2.1 – use of machine learning for cyberthreat intelligence</td></tr>
<tr><td>Topic 2</td><td>2.1.2 - malware detection and response</td></tr>
<tr><td>Topic 3</td><td>6.2.2 – KPI on cybersecurity</td></tr>
<tr><td>Topic 4</td><td>2.1.1 - new attack techniques and defence measures</td></tr>
<tr><th colspan="3">PROJECT OBJECTIVES AND IMPLEMENTATION CAPACITY</th></tr>
<tr><td>Project objectives</td><td colspan="2">Generative artificial intelligence (AI) techniques, and in particular Large Language Models (LLMs), are proving to be extremely useful for contextualising and correlating information extracted from different types of cyber threats. The models have been designed to include numerous data sources of different types, including technical reports on cyber-attacks, source code written in different programming languages, and executable binary code. This property allows LLMs to be used to analyse documents and code thanks to their ability to associate new content with the syntax and semantics of cybersecurity.

Several studies and experimental activities, including those conducted within our research group, show that LLMs enable the correlation of source code, executable code, and information produced by static and dynamic application analysis tools. In this project, they will be used both to directly utilise the textual report produced by LLMs downstream of a prompt and to use intermediate values produced by generative models (embeddings) as a representation for further machine learning processing to calculate the similarity between different threats. Using generative models as intermediate tools for representing threat characteristics allows similarities and differences with other known threats to be highlighted. Preliminary experiments, recently carried out both within our research group and by other national and international laboratories, show the potential of these tools to highlight even weak clues of malicious behaviour hidden by obfuscation, correlating different contextual information from multiple structured and unstructured threat intelligence sources.

We will leverage the knowledge and experience accumulated over the years in our laboratory regarding the use of machine learning techniques for cybersecurity. One approach that has proven effective is the use of specialised techniques to process different types of data or threats, using cascading and/or parallel architectures to progressively refine the analysis. The malicious components of a threat are increasingly hidden in behaviour that is very similar to legitimate behaviour, requiring detailed analysis and contextual information.

The analysis carried out in this way is aimed at creating structured reports that can be used not only as a source of information for the creation of automatic protection rules, where feasible, but also as tools that allow a given organisation to measure the specific risk associated with the new threat. The system that will be developed will make it possible to correlate the description of the threat, in terms of preconditions and actions performed on networks and systems, with the description of the network and systems of a given organisation. This correlation will make it possible to measure the degree of risk mitigation generated by the new threat ensured by the measures in place for protection, detection and response.

This activity will consider various operating environments such as Windows, Android and other Linux kernel-based systems often used in various IoT devices. It will also test the ability of these tools to analyse threats generated</td></tr>
</table>

	automatically or semi-automatically using AI techniques.	
Relevance of the project to the topics on the Agenda	The project mainly falls within Area 2, Cyber Threat Management, and in particular sub-area 2.1, Attack and Defence, topics 2.1.2, Malware Detection and Response; 2.1.1, New Attack Techniques and Defence Measures; sub-area 2.2, Cyber Threat Intelligence, topic 2.2.1, Use of Machine Learning for Cyber Threat Intelligence. The results of the analyses will be used to measure KPIs, thus being consistent with sub-area 6.1, organisational aspects, topic 6.2.2, KPIs on cyber security. The analyses that will be developed are therefore consistent with the objectives of the agenda, Area 2, which aim to develop new methods of analysis and correlation of information aimed at estimating the specific risk that a new threat poses to a given organisation, thus allowing the relevant KPIs to be updated. In this project, generative artificial intelligence technologies will be used creatively to fully exploit their potential for representing knowledge rather than the knowledge they may have learned during the design and learning process. Since it is not possible to control the data used in the training phase, it is not possible to rely solely on the internal knowledge of these tools. However, the domain knowledge encapsulated in the trained models allows these models to be used to interpret new content and correlate it, enabling new knowledge to be extracted. This knowledge will be put into practice by incorporating it into a mechanism for continuous verification of cybersecurity KPIs.	
Project implementation methods, including in terms of available enabling factors	The research group at the Department of Electrical and Electronic Engineering has gained experience and expertise in the forensic sector and malware analysis in more than 25 years of activity. Over the years, numerous innovative approaches have been developed for detecting different types of cyber attacks using machine learning-based methodologies. Relevant activities include: detection of attacks through network traffic analysis, detection of botnets through DNS traffic analysis, malware analysis for Android devices, and analysis of malware conveyed through PDF and Microsoft Office documents. Over the years, numerous industrial research and development activities have been carried out with private companies, as well as collaboration with the public administration and judicial authorities in the context of internships carried out by students enrolled in Master's degree courses and PhD students with advanced training apprenticeship contracts. Collaboration with public administration, police forces, and private companies allows for continuous verification of the relevance of the research topics addressed and measurement of their impact. The introduction in 2018 of a Master's degree course in Cybersecurity and Artificial Intelligence, which also develops skills in malware analysis and forensic analysis, provides a potential pool of graduates with specific training in these subjects. The University of Cagliari is responsible for Spoke 3, “Attacks and Defences”, of the SERICS Extended Partnership funded under the PNRR, whose activities fall entirely within sub-area 2.1, “Attacks and Defences”, of the agenda.	
PROJECT ELEMENTS RELATED TO PRIORITY ISSUES		
Distinctive contribution of the project in relation to priority topics	**Priority topic**	6.2.2 – KPI on cybersecurity
	Artificial intelligence tools, especially generative AI tools, can be used as support tools for the automatic analysis of information obtained from cyber threat intelligence sources, allowing it to be correlated with contextual information in order to increase the organisation's ability to respond to cyber threats. Generative AI, in addition to enabling such analysis, is emerging as a useful	

	tool for producing knowledge that can be used in all subsequent stages of threat prevention and management, as well as in risk assessment and management processes. The knowledge produced by using generative AI tools for cyber threat intelligence will be used to improve the measurement of cyber security KPIs for a specific organisation based on the knowledge acquired from the analysis of new threats and correlation with contextual information. The techniques that will be developed will enable the effectiveness of security procedures and techniques in mitigating the new threat to be verified in a structured and quantitative manner.
COLLABORATIONS WITH OTHER PUBLIC AND PRIVATE ENTITIES	
Reasons and evidence for the involvement in the research project of companies, public or private research bodies and laboratories linked to Italian and/or European entities, international organisations	Agreement with the postal police for internship activities for students enrolled in the doctoral programme in electronic and computer engineering at the Department of Electrical and Electronic Engineering. Agreements for internships with private companies specialising in IT security and forensic analysis. Specifically, Abissi srl regularly hosts master's degree students and PhD students for internships and has previously funded a PhD position with a higher education apprenticeship contract. Collaboration with various universities and research centres in Europe for research activities, both in the context of research projects funded by the European Commission and in the context of activities carried out abroad by PhD students.
Completion of a period of study abroad in European Union countries in the context of the research project	The PhD student will spend six months abroad with one of the research groups with which we have active collaborations and where other PhD students have previously spent their period abroad, such as TU Berlin (DE), TU Wien (AT), Eurecom (FR), University College London (UK), Universidad de Malaga (ES), IMDEA (ES). The choice of location will be made at the end of the first year of activity, which will allow the specific topic to be identified that can be further developed in collaboration.
Duration of the period abroad	6 months
Obligations of the recipient PhD student	The PhD student receiving the scholarship funded by the Agency must carry out the research project in line with the guidelines set out in the research project proposal approved for funding, and must comply with the obligations relating to intellectual property.
Intellectual property and research results	Without prejudice to the moral right of authorship of doctoral students, ownership of the research results of projects funded by the Agency shall be divided equally between the Agency and the University. Consequently, the University shall promptly inform the Agency – by certified email (PEC) to acn@pec.acn.gov.it – of the existence of research results so that the Agency may, within the following sixty days, express its willingness to waive its right by certified email (PEC) to acn@pec.acn.gov.it. In this case, the University will acquire full ownership of the research results.
Revocations, failure to award scholarships, waivers, forfeitures and terminations	The Agency will revoke the funding entirely, with the University being obliged to repay any amounts already paid, in the following cases: • failure to start the doctoral programme in the 41st doctoral cycle within the established deadlines; • interruption of courses for reasons attributable to the University itself; • failure to comply with the University's obligations as set out in the Call for Applications and the Implementation Regulations; • implementation of the research project in a manner that differs from that approved for funding.

	In the event that the doctoral student receiving the scholarship does not obtain a PhD, or in the event that the doctoral student receiving the scholarship is not evaluated positively for the purposes of renewing the scholarship, or renounces it, the funding will be partially revoked, with the obligation to refund the amounts paid following the last annual report submitted by the University to the Agency. Any sums not yet paid will be considered not due and payments will be suspended.