Programma di Dottorato di Interesse Nazionale in "Cybersicurezza" - Candidati ammessi e candidate ammesse alla prova orale
(in ordine alfabetico)

National PhD Program in "Cybersecurity" – Candidates admitted to the interview
(in alphabetical order)

Nome	Cognome	Progetto
Yawar	Abbas	Adversarial AI: theory, attacks and defenses
Zahra	Abbas	Adversarial AI: theory, attacks and defenses
Fadi	Aburub	Paradigmi e soluzioni per lo sviluppo sicuro di sistemi AI affidabili in contesti organizzativi complessi
Yosra	Afi	Detection and Mitigation of Price Manipulation Attacks in DeFi
Yosra	Afi	Design, development, elaboration of LLMs dedicated to cybersecurity legal compliance, deployable locally and using RAG
Junaid	Ahmed	Hyperprofiling: understanding user behavior and interests from mobility big data
Junaid	Ahmed	Data Governance and Data Protection
Youssef	Ait-Erraki	AI-powered Malware Analysis for Cyber Threat Intelligence
Ejemeare Theresa	Akhimien	Data Governance and Data Protection
Adedamola	Akintunde	Intelligent Systems Security
Muhammad Haroon	Alam	Paradigmi e soluzioni per lo sviluppo sicuro di sistemi AI affidabili in contesti organizzativi complessi
Amine	Alane	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Haya	alhunaity	Ethical Issues in AI generated contents and Data Compliance
LINDA MICAELA	ANASTASIO	FACTUAL: Fact-checking Assessment with Contextual Text Understanding via AI Language Models
Kumar Ankur	Anurag	Adversarial AI: theory, attacks and defenses
Amna	Asif	AI-powered Malware Analysis for Cyber Threat Intelligence
Emma	Bagnulo	The Future of Cybersecurity Regulation: Law, Ethics, and Power in the Digital Age
Abdelkader	Baia	Intelligent Systems Security
Fadia	Baissi	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Massimiliano	Baldo	Enhancing Security in Microservice and Serverless Architectures through Advanced Service Mesh Techniques
Sergio	Barezzani	Advanced solutions for data security and privacy in emerging scenarios
Nessrine	Ben Hmida	Enhancing Security in Microservice and Serverless Architectures through Advanced Service Mesh Techniques
Mohamed Djihad	BEN ZEID	Adversarial AI: theory, attacks and defenses
Mahmud Ibr	Bennis	Intelligent Systems Security
Getamesay	Berihun	Secure cloud migration for public administration: integration of post-quantum algorithms for sensitive data protection
Federico	Bonafini	INT-COM-SEC: Sicurezza delle Comunicazioni: Utilizzo dell'interferenza nei protocolli di sicurezza di sistemi cyber-fisici e IoT
kawtar	boucht	Adversarial AI: theory, attacks and defenses
kawtar	boucht	AI-powered Malware Analysis for Cyber Threat Intelligence
kawtar	boucht	Intelligent Systems Security

Mohamed Khalil	Bourouba	Enhancing Security in Microservice and Serverless Architectures through Advanced Service Mesh Techniques
FABIO	BREZOLIN	Secure cloud migration for public administration: integration of post-quantum algorithms for sensitive data protection
Syed Humza	Bukhari	Adversarial AI: theory, attacks and defenses
antonio	campus	AI-powered Malware Analysis for Cyber Threat Intelligence
Catello	Cascone	Adversarial AI: theory, attacks and defenses
Catello	Cascone	Methods for Explainable and Reliable Neuro-Symbolic Multi-Agent Reasoning
Catello	Cascone	Secure Collaborative Learning over Quantum Networks
Gabriel	Cellammare	Cyber Intelligence in the Cyber Social Security
Mona	Chakir	Detection and Mitigation of Price Manipulation Attacks in DeFi
Habtamu	Chanie Andualem	Advanced penetration testing and security assessment methodologies for 5G network security
FRANCESCO	CIRILLO	Advanced penetration testing and security assessment methodologies for 5G network security
FRANCESCO	CIRILLO	INT-COM-SEC: Sicurezza delle Comunicazioni: Utilizzo dell'interferenza nei protocolli di sicurezza di sistemi cyber-fisici e IoT
FRANCESCO	CIRILLO	Secure cloud migration for public administration: integration of post-quantum algorithms for sensitive data protection
Gabriele Nicolò	Costa	Intelligent Systems Security
Oussama Abderrahmane	Dairi	AI-powered Malware Analysis for Cyber Threat Intelligence
Oussama Abderrahmane	Dairi	Intelligent Systems Security
DOMENICO	DANARO	Ethical Issues in AI generated contents and Data Compliance
Francesco	De Giudici	Advanced penetration testing and security assessment methodologies for 5G network security
Francesco	De Giudici	INT-COM-SEC: Sicurezza delle Comunicazioni: Utilizzo dell'interferenza nei protocolli di sicurezza di sistemi cyber-fisici e IoT
Francesco	De Giudici	Paradigmi e soluzioni per lo sviluppo sicuro di sistemi AI affidabili in contesti organizzativi complessi
Sebai	Dhia Eddin	Paradigmi e soluzioni per lo sviluppo sicuro di sistemi AI affidabili in contesti organizzativi complessi
Paolo	Di Biase	Advanced solutions for data security and privacy in emerging scenarios
Nike	Di Giacomo	Secure-by-Design Cryptographic Programming
GIUSEPPE	DI NASO	Design, development, elaboration of LLMs dedicated to cybersecurity legal compliance, deployable locally and using RAG
GIUSEPPE	DI NASO	Detection and Mitigation of Price Manipulation Attacks in DeFi
GIUSEPPE	DI NASO	Intelligent Systems Security
Rahmi	El Mechri	Secure cloud migration for public administration: integration of post-quantum algorithms for sensitive data protection
Mohamed	Elkhawaga	Adversarial AI: theory, attacks and defenses
Luca	Fantin	Hyperprofiling: understanding user behavior and interests from mobility big data
Maryam	Fatahi Vanani	Paradigmi e soluzioni per lo sviluppo sicuro di sistemi AI affidabili in contesti organizzativi complessi
Melsew Belachew	Fentahun	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Abdul	Ghaffar	AI-powered Malware Analysis for Cyber Threat Intelligence
hamza	ghitri	Intelligent Systems Security
Veronika	Glazkova	Enhancing Security in Microservice and Serverless Architectures through Advanced Service Mesh Techniques
MohammadJavad	Goodarzi	Detection and Mitigation of Price Manipulation Attacks in DeFi
Shivangi	Gupta	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Shivangi	Gupta	Intelligent Systems Security

Gizachew Teshome	Habtamu	AI-powered Malware Analysis for Cyber Threat Intelligence
Zahid	Hafeez	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Bechir	Hassani	Intelligent Systems Security
Bechir	Hassani	MFA2C - Security and Privacy of V2X Communications: Study and Development of Identification and Authentication Mechanisms and Protocols in V2X Communications
akmal	hussain	Secure Collaborative Learning over Quantum Networks
Eslam	Hussein	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Assunta	Imperatrice	Adversarial AI: theory, attacks and defenses
Assunta	Imperatrice	Intelligent Systems Security
Assunta	Imperatrice	Scalable and Secure Data Exchange Infrastrutture for Cross-Sector Innovation
Sergio	Imperiale	Intelligent Systems Security
Muhammad Shahid	iqbal	Intelligent Systems Security
Yugansh	Jain	Advanced penetration testing and security assessment methodologies for 5G network security
Moeez	Javed	Advanced penetration testing and security assessment methodologies for 5G network security
Simone	Jovon	Secure-by-Design Cryptographic Programming
Keyvan	Kazemi	Resilient Decentralized Learning
Waqar	khan	Adversarial AI: theory, attacks and defenses
Waqar	khan	AI-powered Malware Analysis for Cyber Threat Intelligence
Kawtar	Khayyi Hammou	AI-powered Malware Analysis for Cyber Threat Intelligence
YONGA EMMANUEL	KIGMO	MFA2C - Security and Privacy of V2X Communications: Study and Development of Identification and Authentication Mechanisms and Protocols in V2X Communications
Achmed Samuel	Koroma	Intelligent Systems Security
Sara	Kouki	FACTUAL: Fact-checking Assessment with Contextual Text Understanding via AI Language Models
Gaoxuan	Li	Detection and Mitigation of Price Manipulation Attacks in DeFi
XianLong	Li	Adversarial AI: theory, attacks and defenses
Pierangelo	Loi	AI-powered Malware Analysis for Cyber Threat Intelligence
Pierangelo	Loi	Cyber Intelligence in the Cyber Social Security
Rahma	Mansouri	Enhancing Security in Microservice and Serverless Architectures through Advanced Service Mesh Techniques
Rahma	Mansouri	Intelligent Systems Security
Marouane	MARHOUN	Adversarial AI: theory, attacks and defenses
ROMARICK FORKWA	MBAH	Secure cloud migration for public administration: integration of post-quantum algorithms for sensitive data protection
Raghid	Mehanna	Intelligent Systems Security
Monica	Micucci	Adversarial AI: theory, attacks and defenses
Monica	Micucci	Hyperprofiling: understanding user behavior and interests from mobility big data
Musbah	Mousa	Secure-by-Design Cryptographic Programming
Malek	Mrad	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Kiran	Nayyab	Secure-by-Design Cryptographic Programming
Kiran	Nayyab	Data Governance and Data Protection
Osama	Nusair	Adversarial AI: theory, attacks and defenses
Omar Ahmed Salad	omardeck	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Shina	Omoniwa	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support

Sara	Ouarti	Adversarial AI: theory, attacks and defenses
Sara	Ouarti	AI-powered Malware Analysis for Cyber Threat Intelligence
Sara	Ouarti	Intelligent Systems Security
Paolo	Palmiero	Scalable and Secure Data Exchange Infrastrutture for Cross-Sector Innovation
PAOLO	POZZAN	INT-COM-SEC: Sicurezza delle Comunicazioni: Utilizzo dell'interferenza nei protocolli di sicurezza di sistemi cyber-fisici e IoT
Virginia Roberta	Pravatà	The Future of Cybersecurity Regulation: Law, Ethics, and Power in the Digital Age
Ylenia	Putortì	Ethical Issues in AI generated contents and Data Compliance
Ylenia	Putortì	FACTUAL: Fact-checking Assessment with Contextual Text Understanding via AI Language Models
Saud	Rahman	Methods for Explainable and Reliable Neuro-Symbolic Multi-Agent Reasoning
Roberta	Romano	The Future of Cybersecurity Regulation: Law, Ethics, and Power in the Digital Age
Ritabrata	Roy Choudhury	Adversarial AI: theory, attacks and defenses
Essmat Ahmed Saeed	Saeed	Secure-by-Design Cryptographic Programming
Amjad	Saleem	Paradigmi e soluzioni per lo sviluppo sicuro di sistemi AI affidabili in contesti organizzativi complessi
Enrico	Soldà	Methods for Explainable and Reliable Neuro-Symbolic Multi-Agent Reasoning
Aditya	Srivastava	Resilient Decentralized Learning
Louis-Marie	Szymkowiak	AI-powered Malware Analysis for Cyber Threat Intelligence
Ivan	Tizzanini	Hyperprofiling: understanding user behavior and interests from mobility big data
Moaz	Usama	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Bernardo	Valente	Emerging Risks of Artificial Intelligence: Models and Techniques for Integrated Security
Daria	Vernon De Mars	Cyber Intelligence in the Cyber Social Security
Michele	Vulpio	Advanced solutions for data security and privacy in emerging scenarios
Michele	Vulpio	Hyperprofiling: understanding user behavior and interests from mobility big data
Michele	Vulpio	Secure cloud migration for public administration: integration of post-quantum algorithms for sensitive data protection
iyad	wehbe	Secure Collaborative Learning over Quantum Networks
Babar	Yousaf	Ethical Issues in AI generated contents and Data Compliance
Hafiz Muhammad	Yousaf	Methods for Explainable and Reliable Neuro-Symbolic Multi-Agent Reasoning
Muzamil	Zahoor	Generative AI and Data Privacy: Risk Mitigation and AI-Driven Compliance Support
Hina	Zulifiqar	AI-powered Malware Analysis for Cyber Threat Intelligence

Lucca, 26 settembre 2025

La responsabile del procedimento amministrativo
Dott.ssa Serena Argentieri
(f.to Serena Argentieri)