



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

## IL RETTORE

**VISTO** lo Statuto della Scuola IMT Alti Studi Lucca, emanato con Decreto Direttoriale n. 05973(214).I.2.02.07.19, pubblicato nella Gazzetta Ufficiale, Serie Generale - n. 163 del 13 luglio 2019, modificato con Decreto Direttoriale n. 03610(160).I.2.22.04.21 pubblicato sulla Gazzetta Ufficiale, Serie Generale, n. 108 del 7 maggio 2021 e con Decreto Direttoriale n. 04794(145).I.2.22.04.22 - Pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana – Serie Generale – n. 105 del 6 maggio 2022;

**VISTO** il Decreto MUR prot. n. 1148 del 12 ottobre 2021 con il quale il Prof. Rocco De Nicola è nominato Direttore (ora Rettore) della Scuola IMT Alti Studi Lucca per la durata di tre anni a decorrere dal 1° novembre 2021;

**VISTA** la legge 30 dicembre 2010, n. 240 "Norme in materia di organizzazione delle Università, di personale accademico e reclutamento, nonché delega al Governo per incentivare la qualità e l'efficienza del sistema universitario", e in particolare l'art. 19, "Disposizioni in materia di dottorato di ricerca";

**VISTO** l'art. 4 della Legge 3 luglio 1998, n. 210, che prevede che le Università, con proprio regolamento, disciplinino l'istituzione dei corsi di Dottorato di Ricerca, le modalità di accesso e di conseguimento del titolo, gli obiettivi formativi ed il relativo programma di studi, la durata, il contributo per l'accesso e la frequenza, le modalità di conferimento e l'importo delle borse di studio, nonché le convenzioni con soggetti pubblici e privati;

**VISTA** la Legge 30 novembre 1989, n. 398 "Norme in materia di borse di studio universitarie", e s.m.i.;

**VISTO** il D.M. 40/2018 (trasMESSO con nota del 25 gennaio 2018) con il quale il Ministero dell'Istruzione, dell'Università e della Ricerca modifica il D.M. del 18 giugno 2008 relativo all'importo annuale delle borse di studio per la frequenza ai corsi di dottorato;

**VISTO** il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

**VISTO** il D. Lgs. DECRETO LEGISLATIVO 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE);

**VISTO** il DECRETO 14 dicembre 2021, n. 226 - Regolamento recante modalità di accreditamento delle sedi e dei corsi di dottorato e criteri per la istituzione dei corsi di dottorato da parte degli enti accreditati, pubblicato sulla Gazzetta Ufficiale, Serie generale - n. 308 del 29 dicembre 2021;

**VISTO** il Decreto Ministeriale n. 351 del 9 aprile 2022 con il quale sono state attribuite, per l'anno 2022/2023, a valere sul PNRR, Missione 4, componente 1 "Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido all'Università" - Investimento 3.4 "Didattica e competenze universitarie avanzate" e Investimento 4.1 "Estensione del numero di dottorati di ricerca e dottorati innovativi per la pubblica amministrazione e il patrimonio culturale", di 2500 borse di dottorato di durata triennale per la frequenza di percorsi di dottorato accreditati ex DM 45/2013 XXXVII ciclo – Anno Accademico 2021/2022 e da accreditare ex DM 226/2021 XXXVIII ciclo – Anno Accademico 2022/2023;

**VISTO** il Decreto Ministeriale n. 352 del 9 aprile 2022 con il quale sono state attribuite, per l'anno 2022/2023, a valere sul PNRR, Missione 4, componente 2 "Dalla Ricerca all'Impresa" - Investimento 3.3 "Introduzione di dottorati innovativi che rispondono ai fabbisogni di innovazione delle imprese e promuovono l'assunzione dei ricercatori dalle imprese", di 5.000 borse di dottorato di durata triennale per la frequenza di percorsi per dottorati innovativi accreditati ex DM 45/2013 XXXVII ciclo – Anno Accademico 2021/2022 e da accreditare ex DM 226/2021 XXXVIII ciclo – Anno Accademico 2022/2023;



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



**Decreto del Rettore n. 9051(293).V.2.19.07.22**

**Rep. Albo on line n. 9052(333).I.7.19.07.22**

**Ufficio** Dottorato e Alta Formazione

**Responsabile** Serena Argentieri

**Autore** Serena Argentieri

**Classificazione** I.7

**VISTI** gli atti d'obbligo sottoscritti dalla Scuola IMT ai sensi dei sopracitati DM 351 e DM 352 del 9 aprile 2022 e i codici unici di progetto ad essi associati (M4C1 - 3.4 CUP D67G22000210001; M4C1 - 4.1 CUP D67G22000220001; M4C2 - 3.3 CUP D67G22000190001);

**VISTE** le convenzioni sottoscritte dalla Scuola IMT con università e imprese rese disponibili a cofinanziare borse di dottorato nell'ambito del DM 351 e del DM 352 del 9 aprile 2022 sopra citati;

**VISTE** le convenzioni siglate dalla Scuola IMT con Consiglio nazionale delle Ricerche e altre università rese disponibili a finanziare borse di dottorato su fondi propri;

**VISTO** il Regolamento del Dottorato di interesse nazionale in "Cybersicurezza", allegato alle sopracitate convenzioni;

**VISTO** il Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca, emanato con Decreto del Rettore n. 6172 (201).I.3.24.05.22 (Rep. Albo on line n. 6173(234).I.7.24.05.22);

**VISTO** il Codice di comportamento della Scuola IMT, emanato con Decreto Direttoriale n. 01053(095).I.3.24.03.14;

**VISTO** l'IMT *Code of Conduct and Ethics*, emanato con Decreto Direttoriale n. 01408(99).11.05.11;

**ACCERTATA** la disponibilità a bilancio sul capitolo CG.04.46.05.04.01 - Borse di studio dottorato di ricerca;

**TENUTO CONTO** che l'attivazione del Programma di Dottorato di Ricerca di interesse nazionale in "Cybersicurezza" è subordinata alla domanda di accreditamento del XXXVIII ciclo che la Scuola IMT ha presentato ai sensi del DM 226/2021, secondo le direttive per l'accREDITAMENTO e nelle modalità specificate dall'ANVUR, e al finanziamento ministeriale conferito ai sensi del DM 351 e del DM 352 del 9 aprile 2022 sopra citati

## DECRETA

l'emanazione del bando di concorso pubblico per l'accesso al XXXVIII ciclo del Programma di Dottorato di Ricerca di interesse nazionale in "Cybersicurezza" allegato al presente decreto.

Lucca, data della firma digitale

Rocco De Nicola  
Rettore  
Scuola IMT Alti Studi Lucca  
(f.to digitalmente Rocco De Nicola)



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

**BANDO DI CONCORSO PER L'ACCESSO AL XXXVIII CICLO DEL PROGRAMMA DI DOTTORATO DI RICERCA DI INTERESSE NAZIONALE IN "CYBERSICUREZZA" DELLA SCUOLA IMT ALTI STUDI LUCCA**

**ARTICOLO 1 - DESCRIZIONE DEL PROGRAMMA E POSTI A CONCORSO**

La Scuola IMT Alti Studi Lucca (nel seguito "Scuola IMT" o "Scuola") indice un concorso pubblico per l'accesso al Programma di Dottorato di Ricerca di interesse nazionale in "Cybersicurezza" (XXXVIII ciclo):

<p><b>Descrizione</b></p>	<p>Proteggere da attacchi informatici gli ambienti ibridi a cui molte organizzazioni sono passate è diventato sempre più difficile. L'adozione del cloud, il lavoro da remoto, la mobilità stanno mettendo a dura prova le capacità di difesa delle aziende e delle amministrazioni pubbliche di tutto il mondo. Per fronteggiare attacchi sempre più sofisticati, sotto forma di zero-day e nuovi malware, serve un mix di tecnologia e best practice, ma soprattutto servono persone con ottime conoscenze tecniche, legali e organizzative, in grado di limitare il divario tra le competenze necessarie e quelle disponibili nel campo della cybersicurezza, visto che questa sta sempre più incorporando il valore della tutela dei diritti nel cyberspazio. Anche se il campo della cybersicurezza si è espanso esponenzialmente nell'ultimo decennio, il fatto che la forza lavoro nel campo non sia aumentata adeguatamente è ormai evidente. Il numero di lavoratori specializzati e qualificati non è sufficiente a soddisfare la domanda, e i mercati del lavoro nazionali sono sconvolti in tutto il mondo, Europa compresa, come conseguenza.</p> <p>Il corso di dottorato di ricerca di interesse nazionale in Cybersicurezza (Ph.D.-CySec) prepara ad analizzare e risolvere un ampio spettro di problemi relativi a diversi aspetti della cybersicurezza, tutti con un elevato interesse istituzionale, sociale e industriale, con l'obiettivo primario di identificare, di volta in volta, le soluzioni più efficaci in funzione dell'obiettivo e del dominio di applicazione. Le opportunità sono quindi sia in ambito accademico, in varie discipline (ingegneria, informatica, economia, legale e gestionale), sia nel settore pubblico, ivi compresa l'Agenzia per la Cybersicurezza Nazionale, sia nei laboratori di ricerca, nei centri di studio e nei centri di competenza, sia nei settori privati per servizi, sicurezza industriale e consulenze professionali.</p> <p>L'obiettivo principale del dottorato di interesse nazionale Ph.D.-CySec è quello di formare una nuova generazione di studiosi, e futuri responsabili, che possano supportare e aumentare la resilienza di cittadini, istituzioni pubbliche e imprese rispetto ad attacchi informatici, sviluppando e implementando correttamente processi e infrastrutture digitali più sicure e affidabili.</p> <p>Durante il percorso dottorale, gli allievi/le allieve impareranno ad affrontare i problemi di sicurezza informatica da diverse prospettive, all'interno di un team inter- e multi-disciplinare di esperti di altri campi e avranno la possibilità di affrontare casi di studio reali proposti da attori e stakeholder sia del settore privato sia di quello pubblico. Al termine del dottorato, gli allievi/le allieve saranno in grado di affrontare la crescente complessità degli attacchi informatici, grazie a un approccio olistico che abbraccia aspetti tecnologici, economici, umani, sociali e legali. Gli sbocchi professionali comprendono, oltre alla carriera accademica, ruoli manageriali nel settore privato e nella pubblica amministrazione, in enti governativi, nonché l'inserimento in organismi di ricerca di vario tipo che richiedono professionisti, esperti e dirigenti caratterizzati da solide competenze scientifiche, background tecnologico e metodologico in cybersicurezza.</p> <p>Per raggiungere tali obiettivi, il dottorato di interesse nazionale Ph.D.-CySec propone un forte approccio multidisciplinare e interdisciplinare fornendo una formazione di base di ampio respiro e</p>
---------------------------	---



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

<p><b>Descrizione</b></p>	<p>concentrandosi su alcuni ambiti di specializzazione. Saranno ammessi al dottorato studenti con diverso background formativo che va dall'informatico, all'ingegnere dell'informazione, al matematico, al fisico fino all'esperto legale, all'economista e allo scienziato sociale. Il piano didattico, grazie alla numerosità e alla diversificazione culturale del collegio docenti, prevederà percorsi specializzati ritagliati sulle competenze in ingresso che punteranno ad offrire una visione olistica della cyber sicurezza ma allo stesso tempo a specializzare in diversi ambiti chiave attraverso i quattro diversi curriculum descritti di seguito.</p> <p>Il curriculum in <b>Foundational Aspects in Cybersecurity</b> offre un background scientifico per l'avanzamento della ricerca in materia di sicurezza informatica, che include elementi di crittografia, intelligenza artificiale, programmazione sicura, calcolo distribuito, metodi formali e linguaggi, e ulteriori contributi innovativi alla ricerca sulla sicurezza informatica. A conclusione del percorso dottorale, l'allievo sarà in grado di collaborare con gruppi di ricerca nel mondo accademico e in centri di ricerca privati o pubblici.</p> <p>Il curriculum in <b>Software, System, and Infrastructure Security</b> mira a fornire le conoscenze scientifiche, tecnologiche e metodologiche necessarie per affrontare, in modo appropriato e proattivo, i principali problemi posti dalla sicurezza di sistemi e infrastrutture di varia natura e complessità, inclusi software, hardware e sistemi di comunicazione, caratterizzati da requisiti di sicurezza e resilienza diversi, a seconda del loro specifico campo di applicazione. A conclusione del percorso dottorale, l'allievo sarà in grado di collaborare con team multidisciplinari per affrontare, dal punto di vista sia tecnologico sia operativo, i vari aspetti di sicurezza dei sistemi e delle infrastrutture, comprese quelle critiche.</p> <p>Il curriculum in <b>Data Governance &amp; Protection</b> affronta temi relativi alla necessità di archiviare ed elaborare i dati in modo efficace ed efficiente, di fare affidamento su piattaforme di elaborazione scalabili, efficienti e affidabili e altre questioni relative alla riservatezza e all'integrità dei dati e dell'elaborazione. A conclusione del percorso dottorale, l'allievo padroneggerà i metodi e le tecnologie per il controllo dell'accesso ai dati e la regolamentazione del loro utilizzo, riducendo al minimo l'impatto sull'utente finale e garantendo riservatezza, integrità e disponibilità dei dati in tutto il ciclo di vita dei dati stessi, dalla creazione alla elaborazione, alla trasmissione e alla memorizzazione.</p> <p>Il curriculum in <b>Human, Economic, and Legal Aspects in Cybersecurity</b> è rivolto principalmente a candidati/e con un background non STEM, a cui fornisce una solida conoscenza degli aspetti tecnici della sicurezza informatica utilizzati per comprendere e affrontare i rischi potenziali o esistenti per la sicurezza informatica e padroneggiare le strategie necessarie per ridurli e proteggere le informazioni sensibili. I profili in uscita possiederanno le necessarie conoscenze e competenze tecniche nell'ambito delle tecnologie dell'informazione, saranno in grado di comprendere il quadro socio-giuridico generale in cui operano e di progettare processi operativi in linea con gli standard di tutela dei diritti fondamentali, gli obblighi normativi, le politiche internazionali e le implicazioni economiche.</p> <p>Gli sbocchi professionali comprendono, oltre alla carriera accademica, ruoli manageriali nel settore privato e nella pubblica amministrazione, in enti governativi, nonché l'inserimento in organismi di ricerca di vario tipo che richiedono professionisti, esperti e dirigenti caratterizzati da solide competenze scientifiche, background tecnologico e metodologico in cybersicurezza.</p>
---------------------------	--

La Scuola IMT applica il principio di pari opportunità e rifiuta ogni discriminazione basata su stati e qualità personali quali il sesso, l'identità di genere, l'identità nazionale o etnica, la fede religiosa, l'orientamento sessuale, lo stato di salute e qualunque altro stato o qualità non rilevanti in relazione al procedimento di cui al presente bando.



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

**Durata del Programma di Dottorato:** tre anni.

**Inizio del Programma di Dottorato:** 1 dicembre 2022

**Coordinatore del Programma:** Prof. Rocco De Nicola.

**Lingua ufficiale dei Programmi di Dottorato:** inglese.

**Borse di dottorato: 38**, da assegnare nell'ambito dei seguenti progetti:

	Titolo progetto	Curriculum	Descrizione	Referente
1	Cybersecurity at the factory plant	Software, System, and Infrastructure Security	Allegato 1	Prof. <a href="#">Marino Miculan</a> , Università degli Studi di Udine
2	CyberSEAS (Cyber Securing Energy dAta Services)	Software, System, and Infrastructure Security	Allegato 2	Prof. <a href="#">Luigi Romano</a> , Università degli Studi di Napoli "Parthenope"
3	Study and development of algorithms and advanced identification and authentication techniques based on biometric procedures	Software, System, and Infrastructure Security	Allegato 3	Prof. <a href="#">Gian Luca Foresti</a> , Università di Udine
4	Methodologies and techniques for analysis, design, monitoring, and prevention of security and safety of critical rail infrastructure	Software, System, and Infrastructure Security	Allegato 4	Prof. <a href="#">Nicola Mazzocca</a> , Università degli studi di Napoli Federico II
5	Methodologies and techniques for preventing, detecting, and mitigating cyberattacks with privacy-preserving tools from eXplainable Artificial Intelligence	Software, System, and Infrastructure Security	Allegato 5	Prof. <a href="#">Antonio Pescapé</a> , Università degli Studi di Napoli Federico II
6	Conspiracy Theories on Social Media	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 6	Dott. <a href="#">Maurizio Tesconi</a> , Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

	<b>Titolo progetto</b>	<b>Curriculum</b>	<b>Descrizione</b>	<b>Referente</b>
7	Automatic software vulnerability detection	Software, System, and Infrastructure Security	Allegato 7	Prof. <a href="#">Gabriele Costa</a> , IMT School for Advanced Studies Lucca
8	Machine learning for network security and malware detection	Software, System, and Infrastructure Security	Allegato 8	Prof. <a href="#">Luca Spalazzi</a> , Università Politecnica delle Marche
9	Security mechanisms at system level	Software, System, and Infrastructure Security	Allegato 9	Prof. <a href="#">Alessandro Biondi</a> , Scuola Superiore Sant'Anna
10	Integrated self-defense of interconnected systems	Software, System, and Infrastructure Security	Allegato 10	Prof. <a href="#">Franco Callegati</a> , Alma Mater Studiorum - Università di Bologna
11	Discovery of False Information on digital communication channels	Software, System, and Infrastructure Security	Allegato 11	Prof. <a href="#">Giuseppe Lo Re</a> , Università di Palermo
12	Formal methods for system security	Foundational Aspects in Cybersecurity	Allegato 12	Prof. <a href="#">Rosario Pugliese</a> , Università degli Studi di Firenze
13	Security of 5G infrastructure and its evolution to 6G	Foundational Aspects in Cybersecurity	Allegato 13	Prof. <a href="#">Giuseppe Bianchi</a> , Università degli Studi di Roma "Tor Vergata"
14	Well-founded cybersecurity techniques	Foundational Aspects in Cybersecurity	Allegato 14	Prof. <a href="#">Riccardo Focardi</a> , Università Ca' Foscari, Venezia
15	Innovative and practical cybersecurity solutions for systems and infrastructures	Software, System, and Infrastructure Security	Allegato 15	Prof.ssa <a href="#">Flaminia Luccio</a> , Università Ca' Foscari, Venezia
16	Software security: analysis and verification of properties	Software, System, and Infrastructure Security	Allegato 16	Prof.ssa <a href="#">Cinzia Bernardeschi</a> e Prof. <a href="#">Gian Luigi Ferrari</a> , Università di Pisa



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

17	Data protection and privacy in innovative application scenarios	Data Governance and Protection	Allegato 17	Prof.ssa <a href="#">Elena Ferrari</a> , Università degli Studi dell'Insubria
	<b>Titolo progetto</b>	<b>Curriculum</b>	<b>Descrizione</b>	<b>Referente</b>
18	Certification Languages for Compliance and Security of Cloud Services	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 18	Dott.ssa <a href="#">Marinella Petrocchi</a> e Dott. <a href="#">Fabio Martinelli</a> , Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy
19	Cognitive characterization of fake media and media manipulation	Data Governance and Protection	Allegato 19	Prof. <a href="#">Mauro Barni</a> , University of Siena
20	Human and socio-legal dimensions for a better-safe Cyberspace	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 20	Prof. <a href="#">Andrea Simoncini</a> , Università degli Studi di Firenze
21	Methods and tools for the security assessment of critical information infrastructures	Foundational Aspects in Cybersecurity	Allegato 21	Dott. <a href="#">Letterio Galletta</a> , IMT School for Advanced Studies Lucca
22	Enhanced soft computing techniques for fake news detection	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 22	Prof. <a href="#">Vincenzo Loia</a> , Università degli Studi di Salerno
23	Cyber Security and Cyber Intelligence measures for Monitoring, Preventing, and Mitigating Radicalisation Pathways	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 23	Prof. <a href="#">Giuseppe Fenza</a> , Università degli Studi di Salerno
24	Cryptographic protocols for the cyberspace	Foundational Aspects in Cybersecurity	Allegato 24	Prof. <a href="#">Alfredo De Santis</a> , Università degli Studi di Salerno
25	Keeping systems, data, and your identity secure	Software, System, and Infrastructure Security	Allegato 25	Prof. <a href="#">Andrea Pugliese</a> , Università della Calabria



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

26	Advanced usage control approaches for data protection	Data Governance and Protection	Allegato 26	Dott. <a href="#">Fabio Martinelli</a> , IIT-CNR
	Titolo progetto	Curriculum	Descrizione	Referente
27	Use of Artificial Intelligence for the protection of Critical Infrastructure	Software, System, and Infrastructure Security	Allegato 27	Prof. <a href="#">Eugenio Di Sciascio</a> , Politecnico di Bari
28	Formal Models of Cyber Security	Foundational Aspects in Cybersecurity	Allegato 28	Prof. <a href="#">Emilio Tuosto</a> , GSSI
29	Cybersecurity of Complex Systems	Software, System, and Infrastructure Security	Allegato 29	Prof. <a href="#">Alessandro Armando</a> , Università degli Studi di Genova
30	Foundations and Methodologies for Secure Programming of CPS	Foundational Aspects in Cybersecurity	Allegato 30	Prof. <a href="#">Michele Loreti</a> , Università di Camerino
31	The Anti-Digital Forensics Cyber Kill Chain	Software, System, and Infrastructure Security	Allegato 31	Prof. <a href="#">Giampaolo Bella</a> , Università di Catania
32	Investigation on GAN-Generated Malware	Software, System, and Infrastructure Security	Allegato 32	Prof. <a href="#">Corrado Aaron Visaggio</a> , University of Sannio
33	Application of zero-knowledge techniques to IoT constrained devices	Software, System, and Infrastructure Security	Allegato 33	Prof. <a href="#">Leonardo Mostarda</a> , Università di Camerino
34	Hardware implementation of Post Quantum Cryptography algorithms	Software, System, and Infrastructure Security	Allegato 34	Prof. <a href="#">Paolo Prinetto</a> , Politecnico di Torino
35	Data protection in emerging scenarios	Data Governance and Protection	Allegato 35	Prof.ssa <a href="#">Pierangela Samarati</a> , Università degli Studi di Milano
36	Human-centered Framework to integrate trustworthy and cyber intelligence in digital systems	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 36	Prof. <a href="#">Danilo Caivano</a> , Università degli Studi di Bari Aldo Moro





**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

37	Design of novel security firmware for modern microarchitectures	Software, System, and Infrastructure Security	Allegato 37	Prof. <a href="#">Bruno Crispo</a> , Università di Trento
38	Cyber security applied to 4/5G Mission Critical Networks and Applications	Software, System, and Infrastructure Security	Allegato 38	Prof. <a href="#">Mirco Tribastone</a> , IMT School for Advanced Studies Lucca
	<b>Titolo progetto</b>	<b>Curriculum</b>	<b>Descrizione</b>	<b>Referente</b>
39	Evolutionary application of AI techniques in cybersecurity	Software, System, and Infrastructure Security	Allegato 39	Prof. <a href="#">Rocco De Nicola</a> e Dott. <a href="#">Simone Soderi</a> , IMT School for Advanced Studies Lucca
40	Analysis of a highway operator's automated critical IT and OT infrastructure systems and identification of innovative cybersecurity solutions	Software, System, and Infrastructure Security	Allegato 40	Dott. <a href="#">Letterio Galletta</a> e Dott. <a href="#">Massimiliano Masi</a> , IMT School for Advanced Studies Lucca
41	Development of technologies for automatic recognition of (deep) fake news on OSN	Human, Economic, and Legal Aspects in Cybersecurity	Allegato 41	Prof. <a href="#">Sebastiano Battiato</a> , Università degli Studi di Catania

I posti possono essere aumentati a seguito di finanziamenti erogati da soggetti pubblici o privati che si rendessero disponibili anche dopo l'emanazione del presente bando. Di tale evenienza è data comunicazione mediante pubblicità sul sito web e all'Albo on line della Scuola o con altri mezzi ritenuti idonei.

**Importo lordo delle borse di dottorato:** 16.243,00 euro annuali (per i dettagli si veda il successivo art. 8).

**Ulteriori *benefit* per i vincitori della presente selezione:**

- totale esenzione dal pagamento delle tasse di iscrizione. Tale esenzione non comprende il pagamento della tassa regionale per il diritto allo studio (attualmente pari a 140€/anno);
- possibilità di usufruire di *benefit* aggiuntivi, come indicato nelle schede dei progetti allegate al presente bando.

## ARTICOLO 2- REQUISITI DI AMMISSIONE AL CONCORSO

Possono partecipare al concorso coloro che, entro la data di scadenza per la presentazione della domanda di partecipazione, siano in possesso dei seguenti requisiti:

1. **Titolo di studio** (per la documentazione necessaria si veda il successivo art. 3) in alternativa tra i seguenti:
  - Laurea magistrale o specialistica, ai sensi del D.M. n. 509 del 3 novembre 1999, e successive modifiche, o



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

laurea quadriennale o quinquennale conseguita ai sensi del previgente ordinamento, o titolo di studio conseguito all'estero e dichiarato equipollente;

- titolo/i di studio conseguito/i all'estero che non sia/siano già stato/i dichiarato/i equipollente/i ai titoli sopra citati, purché sia/siano riconosciuti idoneo/i dalla Commissione di Concorso ai soli fini dell'ammissione al concorso. A tale scopo, la durata minima complessiva del percorso universitario del candidato/della candidata deve essere pari ad almeno 4 anni in regime di tempo pieno. Tale requisito è da ritenersi necessario ma non sufficiente.

Ai candidati/Alle candidate si chiede di allegare online i documenti come descritti all'articolo 3, "Tabella 2 – Allegati" del presente bando.

- 2. Conoscenza della lingua inglese:** i candidati/le candidate devono dichiarare la conoscenza della lingua inglese selezionando uno dei livelli previsti nella sezione dedicata del modulo d'iscrizione online.

Possono altresì partecipare al concorso coloro che prevedano di conseguire un titolo accademico valido per l'ammissione entro il giorno **31 ottobre 2022**. In tal caso l'ammissione al concorso è disposta "con riserva" e il candidato/la candidata è tenuto/a a presentare, entro e non oltre il giorno dell'immatricolazione, una autocertificazione del conseguimento del titolo (per i titoli conseguiti in Italia) o una copia del certificato del conseguimento del titolo (per i titoli conseguiti all'estero) a pena di esclusione. È possibile anticipare il documento sopraindicato via e-mail all'indirizzo [phdapplications@imtlucca.it](mailto:phdapplications@imtlucca.it).

### ARTICOLO 3- DOMANDA DI AMMISSIONE

La domanda di ammissione deve essere obbligatoriamente **compilata in lingua inglese e confermata** utilizzando esclusivamente la procedura on line resa disponibile dalla Scuola IMT, **a pena di esclusione**, entro e non oltre le **ore 12.00 (ora italiana)** del giorno **3 ottobre 2022**.

Non sono ammesse domande di partecipazione pervenute con modalità diverse, salvo espressa autorizzazione da parte della Scuola IMT a fronte di richiesta motivata del candidato/della candidata in relazione a eventuali impedimenti di carattere tecnico.

Si precisa che gli allegati devono essere caricati esclusivamente tramite l'apposito modulo disponibile online. Non sono ammessi documenti pervenuti con modalità diverse da quella descritta, salvo espressa autorizzazione da parte della Scuola IMT a fronte di richiesta motivata del candidato/della candidata in relazione a eventuali impedimenti di carattere tecnico. **Ogni allegato deve essere un unico documento in formato .pdf** e non deve superare la **dimensione massima di 30 MB**.

La Commissione di Concorso (in seguito anche "Commissione") prende in considerazione ai fini della valutazione solo i documenti prodotti in lingua **italiana e/o inglese** (salvo laddove diversamente specificato nelle tabelle seguenti).

Informazioni		
<b>Dati personali</b>	Obbligatorio	In questa sezione i candidati/le candidate devono inserire i propri dati personali (nome, indirizzo, contatti, ecc.).
<b>Livello di conoscenza della lingua inglese</b>	Obbligatorio	I candidati/le candidate devono dichiarare la conoscenza della lingua inglese selezionando uno dei livelli previsti nella sezione dedicata del modulo d'iscrizione online.
<b>Informazioni aggiuntive/</b>	Obbligatorio	I candidati/Le candidate devono indicare la modalità con cui intendono svolgere l'esame (qualora ammessi al termine della preselezione):



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

<b>Preferenza sulla modalità di svolgimento dell'esame</b>		<ul style="list-style-type: none"> <li>• presso la sede della Scuola IMT a Lucca, con spese di viaggio a carico del candidato/della candidata;</li> <li>• in videoconferenza o con altra tecnologia che consenta la visualizzazione del candidato/della candidata: in tal caso il documento di riconoscimento utilizzato nella <i>online application form</i> deve essere esibito prima dell'inizio della prova al fine di consentire l'identificazione del candidato/della candidata;</li> <li>• telefonicamente presso un'Ambasciata o un Consolato Italiano dove il funzionario competente provvederà all'identificazione del candidato/della candidata.</li> </ul>
<b>Informazioni aggiuntive/Eventuali disabilità per le quali sia necessario un ausilio all'esame</b>	Opzionale	I portatori/Le portatrici di handicap che intendano usufruire di un ausilio sono tenuti a richiederlo.
<b>Informazioni aggiuntive/Modalità con cui i candidati/le candidate sono venuti a conoscenza di IMT</b>	Obbligatorio	I candidati/Le candidate devono indicare le modalità con cui sono venuti a conoscenza della Scuola IMT.
<b>Titoli di studio</b>	Obbligatorio	I candidati/Le candidate devono attestare i titoli di studio, indicati come requisito per l'ammissione al concorso all'art. 2 del presente bando, di durata complessiva minima di quattro anni in regime di tempo pieno, relativa media degli esami sostenuti ed eventuale votazione finale.
<b>Titoli di studio aggiuntivi</b>	Opzionale	In questa sezione i candidati/le candidate possono specificare qualsiasi altra qualifica considerata rilevante in relazione alla domanda.
<b>Elenco pubblicazioni</b>	Opzionale	I candidati/Le candidate possono indicare propri articoli pubblicati, libri o altro materiale che possa essere considerato rilevante per il Dottorato e le attività di ricerca.
<b>Referee</b>	Obbligatorio	<p>I candidati/Le candidate devono <b>indicare i nominativi e i dati di contatto di due referee.</b></p> <p>I <i>referee</i> riceveranno una notifica automatica via email e potranno far pervenire le <b>lettere di referenza in lingua inglese entro il giorno 10 ottobre 2022 alle ore 12.00 (ora italiana)</b> esclusivamente attraverso la piattaforma online.</p> <p>I candidati/Le candidate riceveranno una notifica automatica via email per ciascuna lettera pervenuta, ma non potranno accedere alle referenze fornite.</p>

**Allegati**



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

1	<b>Copia di un documento di riconoscimento</b>	Obbligatorio	<p>I candidati/Le candidate devono allegare copia di un documento di riconoscimento in corso di validità:</p> <ul style="list-style-type: none"> <li>- per cittadini italiani e della UE: carta di identità o passaporto</li> <li>- per cittadini non-UE: carta di identità o passaporto (il passaporto è altamente preferibile)</li> </ul> <p>Sulla copia <u>devono essere apposti <b>la data, il luogo e la firma del candidato/della candidata</b></u>. In particolare, il documento deve contenere la/e pagina/e con la fotografia, i dati anagrafici, il numero del documento, il luogo e la data di rilascio. Non sarà considerato valido qualsiasi altro documento che non abbia tutte le informazioni predette.</p> <p>Nel caso in cui il documento non sia in lingua <b>italiana</b> o <b>inglese</b>, ai fini della corretta identificazione del candidato/della candidata, è richiesta una <b>traduzione</b> nelle suddette lingue a cura del candidato stesso/della candidata stessa.</p> <p>Nel caso in cui il documento allegato sia poco leggibile, è facoltà della Commissione di Concorso, qualora il candidato/la candidata risulti ammesso/a all'esame, chiederne una nuova produzione.</p>
2	<b>Curriculum vitae et studiorum</b>	Obbligatorio	<p>I candidati/Le candidate devono allegare il proprio curriculum vitae et studiorum, redatto in lingua <b>italiana</b> o <b>inglese (quest'ultima è altamente preferibile)</b>, con indicazione dei titoli di livello universitario posseduti, delle esperienze di lavoro e di ricerca più significative e di eventuali pubblicazioni.</p>
3	<b>Titoli di studio</b> (indicati come requisito per l'ammissione al concorso)	Obbligatorio	<p>I candidati/Le candidate devono allegare uno dei seguenti documenti in lingua <b>italiana</b> o <b>inglese</b>:</p> <ul style="list-style-type: none"> <li>- per i <b>titoli conseguiti in Italia</b> e/o in <b>Francia, Belgio, Irlanda, Danimarca</b> e <b>Germania</b>: una <b>autocertificazione</b> attestante il possesso dei titoli di studio di cui all'art. 2 del presente bando, la data e l'Università di conseguimento, l'eventuale votazione finale;</li> <li>- per i <b>titoli conseguiti in tutti gli altri Paesi UE ed Extra-UE</b>: una <b>certificazione</b> attestante il possesso dei titoli di studio di cui all'art. 2 del presente bando, la data e l'Università di conseguimento e l'eventuale votazione finale.</li> </ul>
4	<b>Academic transcript/Diploma supplement</b>	Obbligatorio	<p>Per ogni titolo di studio inserito ai fini dell'ammissione al concorso (art. 2), i candidati/le candidate devono allegare uno dei seguenti documenti redatti in lingua <b>italiana</b> o <b>inglese (quest'ultima è altamente preferibile)</b>:</p> <ul style="list-style-type: none"> <li>- un certificato, <i>Academic transcript</i> o un'autocertificazione contenente <b>l'elenco degli esami sostenuti e la relativa votazione conseguita, o, in alternativa,</b></li> <li>- il <i>Diploma Supplement</i>, certificazione rilasciata dall'università contestualmente al titolo di studio e recante tutte le informazioni previste dalla normativa europea</li> </ul>



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

			( <a href="https://ec.europa.eu/education/diploma-supplement_en">https://ec.europa.eu/education/diploma-supplement_en</a> ).
5	<b>Progetto di ricerca</b>	Obbligatorio	Ai candidati/Alle candidate è richiesto di esprimere la preferenza per uno o più progetti di ricerca (massimo 6) di cui all'articolo 1 del presente bando. Tale preferenza non ha valore vincolante in sede di assegnazione del progetto ai vincitori/alle vincitrici (si veda l'art. 5).
6	<b>Research Statement</b>	Obbligatorio	Al fine di valutare l'attitudine dei candidati/delle candidate alla ricerca, con specifico riferimento all'inserimento nel Programma di Dottorato di interesse nazionale in "Cybersicurezza" della Scuola IMT, si richiede la compilazione di un <i>research statement</i> <b>redatto obbligatoriamente in lingua inglese, di lunghezza massima pari a 10.000 caratteri, spazi inclusi</b> , in cui siano descritte: <ul style="list-style-type: none"> <li>- le competenze ed esperienze acquisite in metodi e ambiti di studio rilevanti per il/i progetto/i prescelto/i e come si ritiene che possano essere impiegate per affrontarlo/i;</li> <li>- le motivazioni relative alla domanda di ammissione alla Scuola IMT ed in particolare rispetto al progetto scelto/ai progetti scelti dal candidato/dalla candidata;</li> <li>- progetti futuri.</li> </ul>

Nel caso in cui la domanda risulti mancante di una informazione o di un allegato definito come "obbligatorio", la Commissione può decidere di ammettere il candidato/la candidata alla valutazione con riserva e la domanda sarà considerata valida solo ove lo stesso produca i documenti richiesti entro il giorno previsto per l'esame.

Le informazioni e gli allegati definiti come "opzionali" sono comunque ritenuti utili al fine di consentire alla Commissione una più approfondita valutazione del candidato/della candidata.

La **corretta conclusione** della procedura è **confermata dall'invio automatico di un messaggio di posta elettronica** all'indirizzo email indicato nella domanda dal candidato/dalla candidata; il suddetto messaggio di conferma certifica esclusivamente l'avvenuta ricezione della domanda e la data della stessa. La Scuola IMT non è tenuta ad effettuare alcuna verifica di validità e completezza delle domande nel periodo antecedente la scadenza del termine per la presentazione delle stesse.

**Una volta chiusa la domanda di ammissione al concorso non sarà possibile modificare i dati inseriti nel sistema.**

La Scuola IMT non assume alcuna responsabilità per la dispersione di comunicazioni dipendente da inesatta indicazione del recapito o dell'indirizzo di posta elettronica da parte dei candidati/delle candidate o da mancata o tardiva comunicazione del cambiamento degli stessi, né per eventuali disguidi informatici o comunque imputabili a fatto di terzi, a caso fortuito o forza maggiore.

#### ARTICOLO 4 - COMMISSIONE DI CONCORSO

La Commissione di Concorso è nominata dal Rettore della Scuola IMT con proprio Decreto ed è composta da esperti nelle aree di riferimento dei progetti in cui si articola il Programma, anche appartenenti ad altre istituzioni e alle



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

aziende partner, secondo quanto previsto dal Regolamento del Dottorato di interesse nazionale in "Cybersicurezza" e dal Regolamento del Dottorato di Ricerca della Scuola IMT.

## **ARTICOLO 5 - CRITERI DI VALUTAZIONE E PROCEDURA DI SELEZIONE**

### **Criteria di valutazione**

Prima di procedere alla valutazione dei titoli, la Commissione definisce i criteri riferiti ai titoli e più in generale all'intera procedura di valutazione. In ogni caso la Commissione valuta i seguenti elementi:

- percorso di studi, conoscenze, competenze e valore scientifico del candidato/della candidata;
- attitudine del candidato/della candidata alla ricerca e possibilità di inserimento nelle attività di ricerca specifiche del progetto selezionato/dei progetti selezionati nella domanda;
- grado di interdisciplinarietà del profilo, conoscenze e competenze del candidato/della candidata in relazione alla multidisciplinarietà del Programma di Dottorato e al progetto prescelto/ai progetti prescelti.

### **Preselezione**

L'esame di concorso è preceduto da una preselezione per titoli. La valutazione dei titoli è effettuata in relazione alle specifiche del Programma di Dottorato e dei progetti in cui si articola ai soli fini dell'ammissione all'esame.

In fase di preselezione, la valutazione del candidato/della candidata è effettuata dalla Commissione, di cui all'art. 4 del presente bando, sulla base delle dichiarazioni rese nella domanda, dei documenti allegati alla stessa (secondo le modalità di cui al precedente articolo 3) e delle lettere di referenza pervenute.

Sulla base della valutazione dei titoli, la Commissione individua i candidati/le candidate da ammettere alla fase successiva (esame) mediante la stesura di una *shortlist*, senza graduatoria di merito.

L'elenco degli ammessi all'esame sarà pubblicato sul sito web e all'Albo On Line della Scuola IMT. Tale comunicazione ha valore di notifica a tutti gli effetti. Non vengono effettuate comunicazioni personali ai singoli candidati/alle singole candidate.

### **Esame**

I candidati ammessi/Le candidate ammesse all'esame dovranno confermare la loro partecipazione inviando una email all'indirizzo [phdapplications@imtlucca.it](mailto:phdapplications@imtlucca.it) entro 2 giorni dalla pubblicazione della lista degli ammessi all'esame. Essi/e dovranno altresì confermare la preferenza, già indicata in sede di domanda di ammissione alla partecipazione al concorso, circa la modalità di svolgimento dell'esame (come definito all'articolo 3 del presente bando).

L'esame consiste in un colloquio in lingua inglese, volto ad approfondire la valutazione delle conoscenze e delle competenze del candidato/della candidata in relazione alle specifiche del progetto/dei progetti per cui è stata presentata la candidatura.

La Commissione avrà a disposizione 100 punti per la valutazione dell'esame e il punteggio minimo per il superamento dell'esame è fissato in 70/100.

Ogni informazione sulla procedura e il calendario di svolgimento dell'esame saranno pubblicati sul sito web e all'Albo on line della Scuola IMT. Tale pubblicazione ha valore di notifica a tutti gli effetti. Non verranno effettuate comunicazioni personali ai singoli candidati/alle singole candidate.

### **Graduatoria finale**



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

Al termine dell'esame, per i candidati risultati idonei/le candidate risultate idonee, la Commissione procede alla stesura di una graduatoria di merito in base alla votazione riportata all'esame, per ciascun progetto. La preferenza espressa dal candidato/dalla candidata in fase di domanda non è vincolante per la Commissione, la quale può assegnare il candidato/la candidata alla graduatoria del progetto a bando che sia ritenuto maggiormente corrispondente al proprio profilo.

A parità di punteggio, la preferenza è determinata dalla minore età del candidato/della candidata.

In caso di rinuncia, si scorrerà la graduatoria fino alla copertura delle posizioni previste (come indicato all'art. 1 del presente bando).

La graduatoria, approvata con provvedimento del Rettore, è immediatamente efficace e pubblicata sul sito web nonché all'Albo on line della Scuola IMT. Dell'avvenuta pubblicazione è dato avviso sulla Gazzetta Ufficiale.

#### **ARTICOLO 6 - IMMATRICOLAZIONE DEI CANDIDATI AMMESSI/DELLE CANDIDATE AMMESSE**

La domanda di immatricolazione, il cui modello sarà trasmesso via e-mail ai candidati ammessi/alle candidate ammesse, deve pervenire alla Scuola **entro il termine di 5 giorni** decorrente **dalla data di pubblicazione della graduatoria finale di merito**.

La domanda è considerata valida solo se corredata di tutta la documentazione richiesta dagli uffici competenti.

La domanda deve essere consegnata secondo una delle seguenti modalità: a mano presso la Scuola IMT, spedita tramite servizio postale (in tal caso farà fede la data del timbro postale) o tramite servizio di posta elettronica certificata ai recapiti sottoelencati:

- Scuola IMT Alti Studi Lucca  
Ufficio Dottorato e Alta Formazione  
Piazza S. Ponziano 6,  
55100 Lucca – Italy
- Posta elettronica certificata: [imtlucca@postecert.it](mailto:imtlucca@postecert.it)

La mancata consegna della domanda con le modalità ed entro i termini sopradetti si intende quale rinuncia alla partecipazione al Programma di Dottorato e implica la perdita del diritto all'immatricolazione e lo scorrimento della graduatoria secondo quanto previsto dal Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca e dal presente bando.

Nel caso in cui uno o più documenti allegati alla domanda di ammissione non corrispondano a quelli inviati in fase di immatricolazione rivelando dichiarazione falsa e mendace, il candidato/la candidata perderà automaticamente il diritto all'immatricolazione.

L'immatricolazione avviene di norma il giorno di inizio dei corsi, salvo eventuali casi particolari gestiti dall'Amministrazione, previa autorizzazione del Rettore, ferma restando la necessaria acquisizione del titolo di studio. Assenze ingiustificate il giorno di inizio dei corsi possono annullare la procedura di immatricolazione.

#### **ARTICOLO 7 - INCOMPATIBILITÀ**

Coloro che risultano già iscritti a un corso di Dottorato di Ricerca possono accedere al Programma di Dottorato della Scuola IMT a seguito del superamento del relativo concorso, purché rinuncino al corso frequentato e inizino dal primo anno del Programma per cui sono stati ammessi.



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

## **ARTICOLO 8 - BORSE DI DOTTORATO**

L'importo annuale della borsa di dottorato è di euro 16.243,00, al lordo degli oneri previdenziali a carico dell'allievo/a previsti dalla normativa vigente.

La borsa di dottorato è corrisposta in rate mensili, ad eccezione di quanto previsto dall'art. 15 del Regolamento del Dottorato di Ricerca della Scuola IMT Alti Studi Lucca.

Per il soggiorno fuori sede all'estero per attività di formazione e/o ricerca, l'importo della borsa è incrementato del 50% fino ad un massimo di 12 mesi.

Alle borse di dottorato per la frequenza dei Programmi di Dottorato di Ricerca si applicano le disposizioni in materia di agevolazioni fiscali di cui all'art. 4 della Legge del 13 agosto 1984, n. 476.

La borsa di dottorato del dottorato di ricerca è soggetta al versamento dei contributi previdenziali INPS (Gestione Separata), ai sensi dell'articolo 2, comma 26, della Legge 8 agosto 1995, n. 335 e successive modificazioni, nella misura di due terzi a carico dell'Amministrazione e di un terzo a carico del beneficiario.

Chi abbia già usufruito di una borsa di dottorato per un corso di Dottorato di Ricerca in Italia non può beneficiarne nuovamente in caso di iscrizione ad un nuovo corso di Dottorato.

Le borse di dottorato non sono cumulabili con assegni di ricerca o altre borse, a qualsiasi titolo conferite, tranne che con quelle concesse da istituzioni nazionali o straniere utili ad integrare, con soggiorni all'estero, l'attività di ricerca dell'allievo/a.

La borsa di dottorato ha durata di tre anni ed è soggetta a conferma annuale, previa verifica, secondo quanto stabilito dagli artt. 15 e 16 del Regolamento del Dottorato di Ricerca della Scuola IMT. Eventuali estensioni della durata del percorso di studio non implicano l'ampliamento del periodo di fruizione della borsa di dottorato.

L'erogazione della borsa è sospesa nei casi previsti dal Regolamento del Dottorato di Ricerca della Scuola IMT.

Gli allievi/Le allieve con borsa di dottorato che rinunciano o sono esclusi dal Programma entro i primi 45 giorni dall'inizio dello stesso o dall'immatricolazione, non maturano il diritto alla fruizione della borsa. In tale caso, si procede con lo scorrimento della graduatoria, scorrimento da chiudersi entro la scadenza fissata annualmente dal Ministero dell'Università e della Ricerca per il monitoraggio dei dottorati accreditati e la registrazione dei dati degli allievi immatricolati/delle allieve immatricolate nell'anno accademico di riferimento.

In caso di rinuncia alla sola borsa di dottorato, il Collegio Docenti può deliberare l'assegnazione della borsa al primo/alla prima dei candidati idonei/delle candidate idonee, ove ve ne siano.

Il diritto alla borsa di dottorato, per gli/le aventi diritto immatricolati oltre 45 giorni dopo l'inizio del Programma, matura dal giorno dell'immatricolazione e si conclude allo scadere del periodo di svolgimento del Programma (durata di tre anni).

## **ARTICOLO 9 - TRATTAMENTO DEI DATI PERSONALI**

In attuazione e nel rispetto del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati) e del D. Lgs. 196/03 ("Codice in materia di protezione dei dati personali"), come modificato dal D. Lgs. 10 agosto 2018, n. 101, la Scuola IMT si impegna, come titolare dei dati personali forniti dal candidato/dalla candidata, ad utilizzare tali dati unicamente per l'espletamento delle procedure concorsuali ex art. 6, comma 1, lett. e) del Regolamento.





Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



**Decreto del Rettore n. 9051(293).V.2.19.07.22**  
**Rep. Albo on line n. 9052(333).I.7.19.07.22**  
**Ufficio** Dottorato e Alta Formazione  
**Responsabile** Serena Argentieri  
**Autore** Serena Argentieri  
**Classificazione** I.7

Il conferimento dei dati è necessario per il conseguimento delle finalità sopra indicate. In assenza di tali dati il candidato/la candidata non sarà ammesso alla selezione.

Il titolare del trattamento dei dati è il Direttore della Scuola IMT, Prof. Rocco De Nicola. I dati di contatto del Titolare del trattamento dei dati personali sono: [imtlucca@postecert.it](mailto:imtlucca@postecert.it).

I dati forniti sono trattati dal titolare e/o dal personale degli uffici della Scuola interessati dal procedimento e dai componenti della commissione concorsuale o selettiva.

Il DPO della Scuola IMT è il Dott. Giulio Bolzonetti. I dati di contatto del DPO sono i seguenti: [dpo@imtlucca.it](mailto:dpo@imtlucca.it); [imtlucca@postecert.it](mailto:imtlucca@postecert.it).

I dati personali saranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono trattati e con specifico riguardo al principio di limitazione della conservazione di cui all'art. 5, lett. "e" del Regolamento UE 2016/679.

Si precisa che i dati sono trattati con o senza l'ausilio di strumenti elettronici, specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

L'interessato ha il diritto di accedere ai propri dati personali e ottenere le informazioni rilevanti sul trattamento, ai sensi dell'art. 15 del Regolamento.

L'interessato ha diritto di esercitare i diritti di cui alla sezione 2, 3 e 4 del Capo III del Regolamento UE 2016/679, ove per quanto applicabili allo specifico trattamento.

L'interessato ha inoltre il diritto di proporre reclamo al Garante per la Protezione dei Dati se ritiene che il trattamento che lo riguarda violi il Regolamento UE 2016/679, ai sensi e nelle modalità dell'art. 77 di detto Regolamento o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

La partecipazione al concorso implica la pubblicazione dei nominativi dei candidati/delle candidate e dei dati relativi all'esito della selezione sul sito web e all'Albo on Line della Scuola IMT.

#### **ARTICOLO 10- RESPONSABILE DEL PROCEDIMENTO**

A tutti gli effetti del bando, è individuata quale responsabile del procedimento la Dott.ssa Serena Argentieri, presso l'Ufficio Dottorato e Alta Formazione, sito in Piazza S. Ponziano, 6 - 55100 Lucca (tel. 0583-4326530 – indirizzo di posta elettronica: [phdapplications@imtlucca.it](mailto:phdapplications@imtlucca.it)).

Per maggiori informazioni relative al presente bando e alla procedura di selezione, è possibile contattare l'Ufficio Dottorato e Alta Formazione sia per posta elettronica, scrivendo all'indirizzo [phdapplications@imtlucca.it](mailto:phdapplications@imtlucca.it), sia per telefono, al numero +39 0583 4326530.

Ulteriori informazioni sul Programma di Dottorato e, in generale, sulla Scuola IMT sono disponibili sul sito web [www.imtlucca.it](http://www.imtlucca.it).

#### **ARTICOLO 11 - RINVIO AD ALTRE NORME E NORME FINALI**

Avendo adottato tutte le misure necessarie allo svolgimento delle attività previste per gli Anni Accademici 2019/20, 2020/21 e 2021/22 durante l'emergenza sanitaria da COVID-19, nel caso in cui suddetta emergenza dovesse protrarsi, la Scuola IMT erogherà le attività e i servizi previsti per l'AA 2022/23 con modalità tali da consentire ai nuovi allievi/alle nuove allieve di immatricolarsi, frequentare le attività formative e intraprendere il proprio percorso dottorale.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



**Decreto del Rettore n. 9051(293).V.2.19.07.22**

**Rep. Albo on line n. 9052(333).I.7.19.07.22**

**Ufficio** Dottorato e Alta Formazione

**Responsabile** Serena Argentieri

**Autore** Serena Argentieri

**Classificazione** I.7

Per tutto quanto non previsto dal presente bando si fa riferimento alle disposizioni vigenti, al Regolamento del Dottorato di Ricerca di interesse nazionale in "Cybersicurezza", al Regolamento del Dottorato di Ricerca della Scuola IMT Altissimi Studi Lucca e a quant'altro compatibile con la disciplina di settore.

L'attivazione del Programma è subordinata alla verifica dei requisiti richiesti per l'accREDITAMENTO secondo le modalità definite dagli organismi competenti, ai sensi del DM 226/2021, e ai finanziamenti ministeriali conferiti ai sensi del DM 351 e del DM 352 del 9 aprile 2022.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## NATIONAL PHD PROGRAM IN IN "CYBERSECURITY" - RESEARCH PROJECTS

### Index

1. Cybersecurity at the Factory Plant .....	3
2. CyberSEAS (Cyber Securing Energy dAta Services) .....	4
3. Study and development of algorithms and advanced identification and authentication techniques based on biometric procedures .....	5
4. Methodologies and techniques for analysis, design, monitoring, and prevention of security and safety of critical rail infrastructure.....	6
5. Methodologies and techniques for preventing, detecting, and mitigating cyberattacks with privacy-preserving tools from eXplainable Artificial Intelligence .....	7
6. Conspiracy Theories on Social Media.....	8
7. Automatic software vulnerability detection .....	9
8. Machine learning for network security and malware detection .....	10
9. Security mechanisms at system level .....	11
10. Integrated self-defense of interconnected systems .....	12
11. Discovery of False Information on digital communication channels .....	13
12. Formal methods for system security .....	14
13. Security of 5G infrastructure and its evolution to 6G .....	15
14. Well-founded cybersecurity techniques .....	16
15. Innovative and practical cybersecurity solutions for systems and infrastructures.....	17
16. Software security: analysis and verification of properties.....	18
17. Data protection and privacy in innovative application scenarios .....	19
18. Certification Languages for Compliance and Security of Cloud Services .....	20
19. Cognitive characterization of fake media and media manipulation.....	21
20. Human and socio-legal dimensions for a better-safe Cyberspace .....	22
21. Methods and tools for the security assessment of critical information infrastructures .....	23
22. Enhanced soft computing techniques for fake news detection .....	24
23. Cyber Security and Cyber Intelligence measures for Monitoring, Preventing, and Mitigating Radicalisation Pathways .....	25
24. Cryptographic protocols for the cyberspace.....	26
25. Keeping systems, data, and your identity secure .....	27
26. Advanced usage control approaches for data protection.....	28



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



27. Use of Artificial Intelligence for the protection of Critical Infrastructure .....	29
28. Formal Models of Cyber Security .....	30
29. Cybersecurity of Complex Systems .....	31
30. Foundations and Methodologies for Secure Programming of CPS .....	32
31. The Anti-Digital Forensics Cyber Kill Chain .....	33
32. Investigation on GAN- Generated Malware .....	34
33. Application of zero-knowledge techniques to IoT constrained devices .....	35
34. Hardware implementation of Post Quantum Cryptography algorithms .....	36
35. Data protection in emerging scenarios .....	37
36. Human-centered Framework to integrate trustworthy and cyber intelligence in digital systems .....	38
37. Design of novel security firmware for modern microarchitectures .....	39
38. Cyber security applied to 4/5G Mission Critical Networks and Applications .....	40
39. Evolutionary application of AI techniques in cybersecurity .....	41
40. Analysis of a highway operator's automated critical IT and OT infrastructure systems and identification of innovative cybersecurity solutions .....	42
41. Development of technologies for automatic recognition of (deep) fake news on OSN.....	43



Finanziato  
dall'Unione europea  
NextGenerationEU



## 1. Cybersecurity at the Factory Plant

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università degli Studi di Udine

**Funds:** DM 352-PNRR: Cleverynext s.r.l.

**Additional benefits:**

**Website:**

**Contact person:** [Marino Miculan](#)

### Description

The objective of this Ph.D. project is to study and develop advanced techniques for protecting network-connected machines in an industrial plant from cyberattacks. The area is Operational Technology (OT), encompassing both SCADA, DCS, and PLC systems. The problem of identifying and locating cyber vulnerabilities and recognizing anomalies is critical in the operational environment of industrial plants, especially when processes are critical to physical, environmental, and economic security. For this reason, any improvement to the accuracy and precision of the models and algorithms for this purpose represents a step toward full or partial automation of several processes of high economic and social interest.

The Ph.D. candidate will develop specific knowledge of the various methods of analysis and modeling of problems related to cybersecurity of computer networks in industrial plants. The Ph.D. student will be able to design, develop, and test compliance assessment and penetration testing systems for OT networks, adapting them to certain real-world contexts in industrial settings and specific operational requirements. A prototype of a security device equipped with an anomaly detection algorithm for monitoring and protection devices connected to the industrial plant network will be developed.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 2. CyberSEAS (Cyber Securing Energy dAta Services)

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università degli Studi di Napoli "Parthenope"

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:** Possibility to supplement the scholarship with a research contract

**Website:**

**Contact person:** [Luigi Romano](#)

### Description

CyberSEAS ambition is to improve the resilience of energy supply chains, protecting them from disruptions that exploit the enhanced interactions and extended involvement models of stakeholders and consumers in complex attack scenarios characterized by the presence of legacy systems and the increasing connectivity of data feeds. It has three strategic objectives: 1) countering the cyber risks related to highest impact attacks against electric power and energy systems (EPES); 2) protecting consumers against personal data breaches and attacks; and 3) increasing the security of the Energy Common Data Space. All three objectives are equally important since cyber-criminals are shifting tactics to favor multi-stage attacks for which stealing sensitive data is a precondition for the real attack and enables them to maximize damage and profits (while traditionally, infrastructure cyber-attacks used to be direct attacks on the machinery and typically targeted control systems, not data). To achieve these objectives, CyberSEAS will deliver an open and extendable ecosystem of customizable security solutions providing effective support for key activities, in particular: risk assessment; interaction with end devices; secure development and deployment; real-time security monitoring; skills improvement and awareness; certification, governance, and cooperation. CyberSEAS solutions will be validated through experimental campaigns consisting in the context of realistic use cases.



Finanziato  
dall'Unione europea  
NextGenerationEU



### 3. Study and development of algorithms and advanced identification and authentication techniques based on biometric procedures

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università di Udine

**Funds:** DM 352-PNRR: ACRM NET

**Additional benefits:**

**Website:**

**Contact person:** [Gian Luca Foresti](#)

#### **Description**

During the first year, the doctoral student will delve into the state of the art in computer system security, focusing on identification and authentication techniques based on biometric procedures. He/she will acquire specific databases for training and testing the systems developed during the doctoral activities. During the second year, he/she will classify weaknesses in authentication systems concerning the techniques he/she intends to develop. Different methods of user identification and authentication through insecure communication channels will be designed and implemented, some evaluation tests will be carried out (also choosing an appropriate calculation and ranking method) to select the best methods according to different application contexts. During the third year, based on the obtained results, the student will refine the alignment functions while identifying evolution criteria useful for adapting the proposed technique. The most promising algorithms in different application contexts will be improved, and final evaluation tests will be conducted. The Ph.D. student will prepare several scientific papers for submission to national and international scientific conferences and international scientific journals.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



#### **4. Methodologies and techniques for analysis, design, monitoring, and prevention of security and safety of critical rail infrastructure**

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università degli studi di Napoli Federico II

**Funds:** Hitachi Rail

**Additional benefits:** Possibility of supplementing the scholarship with company funds

**Website:** <http://www.dieti.unina.it>

**Contact person:** [Nicola Mazzocca](#)

##### **Description**

Critical infrastructures, particularly transportation and mobility infrastructures, are strategic assets that fall within the national security perimeter and provide primary services for citizens and the industrial system. Their security is required to ensure an adequate level of services to citizens. Their security is also to protect them from possible catastrophic damage, such as earthquakes, landslides, and floods, therefore, addressing both "physical" integrity caused by natural events and "cyber" integrity caused by cyber attacks. The objective of the Ph.D. fellowship is to study and research innovative theoretical and practical methodologies to analyze the threats of increasingly connected critical infrastructures and the associated risks to mitigate them with specific mechanisms and policies. Specifically, the study activities will include specific threat analysis, threat analysis, and threat intelligence systems, security and reliability frameworks for selecting and configuring security controls, security assessment and static and dynamic security testing of security properties of systems, as well as proactive protection mechanisms to increase resilience and respond to novel attacks.





Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 5. Methodologies and techniques for preventing, detecting, and mitigating cyberattacks with privacy-preserving tools from eXplainable Artificial Intelligence

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università degli Studi di Napoli Federico II

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:** Possibility of supplementing the scholarship with project funds

**Website:** <http://www.dieti.unina.it>

**Contact person:** Antonio Pescapé

### Description

Distributed digital systems, of which the Internet is both an emblematic example and the main communication infrastructure, have become increasingly important for economic and social development on a global scale. With these technologies, however, the range of vulnerabilities and the number and heterogeneity of systems and critical infrastructures subject to attacks have significantly expanded. The objective of the fellowship is foundational and applied research on tools and techniques for prevention, detection and mitigation of cyber attacks with a focus on trustworthiness and privacy. Topics will include methodologies and techniques for Intrusion Prevention/Detection System (IPS/IDS), Anomaly Detection System (ADS), Censorship Detection, Censorship Circumvention, Privacy-preserving Network Monitoring, Surveillance.

For these purposes, artificial intelligence (AI) has proven to be an indispensable tool to capitalize on data collected from the Internet, local area networks, data centers, and applications. However, the adoption of advanced Deep Learning-based solutions is hindered by their inherent black-box nature, which is a limitation to their improvement and an ethical and legal barrier to real-world applications. Therefore, the search for explainable AI techniques (eXplainable AI) will be a necessary tool to make AI models (and the systems that use them) interpretable, manageable, and reliable (trustworthy).

## 6. Conspiracy Theories on Social Media

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy

**Funds:** Istituto di Informatica e Telematica

**Additional benefits:**

**Website:**

**Contact person:** [Maurizio Tesconi](#)

### Description

Conspiracy theories are often denoted as beliefs in the existence of a network of powerful people with malevolent intents who control complex socio-political events, especially when they lack a clear explanation by the authorities or by the scientific community. It is a global phenomenon affecting almost every field of human activity. The conspiracy mindset has notoriously led to episodes of prejudice, witch hunts, obstacles to public health improvements, discrediting science, negative economic impacts, strengthening of radicalized and extremist groups, not to mention wars and genocides. A new generation of radicalization processes seems to take place on social media, where conspiracy theories are shared through many communities that reinforce confirmation bias, segregation, and polarisation. This project proposes a research action on conspiracy spreaders both within and across social media, which will lead to analyzing the conspiracy phenomenon by exploiting a synergy of multidisciplinary expertise in the area of data science and social science. The main objectives will be to define the phenomenon contours identifying the number and typology of the conspiracy theories taking place at a certain time, and to characterize both the users that act as spreaders and those who fall for a conspiracy theory reinforcing its dissemination. This characterization will be carried out through socio-demographic profiling, analysis of social media activity, writing style, psycho-linguistic traits, political orientation, and so on.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 7. Automatic software vulnerability detection

**Curriculum:** Software, System, and Infrastructure Security

**University:** IMT School for Advanced Studies Lucca

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:** Full board accommodation

**Website:** <https://sysma.imtlucca.it>

**Contact person:** Gabriele Costa

### Description

Formal modeling and verification techniques have the potential to provide the strongest security guarantees and to support full automation. However, implementing effective vulnerability detection tools based on these techniques is still an open issue. The main reasons are the poor scalability and the lack of formal semantics of real programming languages. The goal of this project is to investigate novel methodologies that (i) provide formal security guarantees and (ii) can be applied to real world software and services. Many types of analysis may be considered. Among them are, for instance, symbolic exploration, model checking and security testing. Application domains of interest include (but are not limited to) software behavioral analysis, malware detection and classification, binary and web applications vulnerability disclosure, security assessment of smart contracts.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 8. Machine learning for network security and malware detection

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università Politecnica delle Marche

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:** <https://www.univpm.it>

**Contact person:** Luca Spalazzi

### Description

The research project will aim at developing, testing and validating machine learning techniques for network security, with focus on detection of network traffic generated by malicious entities. This will leverage previous research activities of the proposing research unit concerning the use of machine learning and natural language processing techniques for physical layer authentication over wireless networks and identification of algorithmically generated domain names within DNS queries and responses. Based on such a background, the candidate will address new scenarios possibly involving further types of data (e.g., audit records coming from security information and event management systems - SIEMs) and the identification of more complex threats. The use of collected and extracted information will also be addressed by the candidate, possibly involving its application to a regional Computer Security Incident Response Team (CSIRT). For these purposes, the candidate will be asked to develop and use state-of-the-art software tools for machine learning and cybersecurity, to be applied to the aforementioned contexts.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 9. Security mechanisms at system level

**Curriculum:** Software, System, and Infrastructure Security

**University:** Scuola Superiore Sant'Anna

**Funds:** DM-351-PNRR: Ateneo; Co-financed by the ReTiS Laboratory

**Additional benefits:** Board; Possibility of supplementing the scholarship with project funds; canteen (lunch)

**Website:**

**Contact person:** [Alessandro Biondi](#)

### Description

Research activities will aim to study techniques for detecting cyber attacks and designing defense mechanisms at the system level (e.g., at the operating system level, hypervisor, or in the context of tools such as compilers or neural inference engines). The mechanisms to be designed will be geared toward embedded systems and, therefore, should be resource-efficient and predictable in terms of execution time.

The research activities will be carried out within the ReTiS laboratory (<https://retis.santannapisa.it/>) of the Scuola Superiore Sant'Anna, where it will be possible to develop prototypes of the designed mechanisms and test them on state-of-the-art embedded platforms, including in the context of applications such as the control of self-driving vehicles.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 10. Integrated self-defense of interconnected systems

**Curriculum:** Software, System, and Infrastructure Security

**University:** Alma Mater Studiorum - Università di Bologna

**Funds:** Research funds

**Additional benefits:**

**Website:**

**Contact person:** [Franco Callegati](#)

### Description

The research project focuses on a near future scenario where IT and OT systems in industrial plants and supply chains will be more integrated. The objective of the research is to propose new methodologies and tools for the assessment of cybersecurity and cyber resilience, and to define the necessary technological and governance measures to be integrated for the continuous improvement of the cyber posture. The research wants to propose innovative methodologies and solutions of general validity in terms of mapping architectures and processes in order to detect vulnerabilities, single points of failure, bottlenecks and other issues that could be addressed through integrated self-defensive components possibly based on AI/ML. To this end, new approaches will be analyzed and evaluated, also based on simulation models of systems, possibly integrated by digital twins, as well as machine/deep learning approaches for the analysis, evaluation, and semi-autonomous treatment of risks. The research will mainly focus on application scenarios such as manufacturing industries, critical infrastructure and smart cities and will consider the main driver technologies, including cloud and edge architectures, 5G and software-defined network infrastructures, taking into account that security, resilience and safety must also be guaranteed for the IoT elements that represent the current frontiers of production, from the so-called digital factory to the servitization of plants and products.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 11. Discovery of False Information on digital communication channels

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università di Palermo

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:**

**Contact person:** [Giuseppe Lo Re](#)

### Description

The patterns of dissemination of false or partially true information can vary significantly depending on several characterizing factors, including the environment chosen to convey the attack (social networks, websites, messaging systems, etc.), the content transmission mode, and the identity of the source, whether human or artificial.

For this reason, automated verification systems cannot currently provide certain results and can at most provide a probabilistic indication after a verification process (fact-checking) carried out by human operators. Such strategies have multiple limitations, the most obvious is certainly non-timeliness. To fill this gap, the proposed research activity is aimed at the study and definition of new solutions that exploit artificial intelligence methods to support: the detection of polarizing topics on which an attacker could engage a fake news dissemination mechanism; the study of anomalous content dissemination dynamics; the real-time recognition of fake news by jointly analyzing heterogeneous information flows, coming from sources characterized by different levels of reliability; and the realization of secure systems, even from "adversary" attacks. Activities should also include analysis of legal aspects and safeguarding user privacy.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 12. Formal methods for system security

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** Università degli Studi di Firenze

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:**

**Contact person:** [Rosario Pugliese](#)

### Description

This research activity will address the foundations of computer systems, software, or hardware to devise formal languages and methods for rigorously specifying and reasoning about the security properties of such systems, in addition to their functional correctness. The application of formal methods to security has emerged over recent decades as a well-established research area, and many related tools are applied in practice with increasing success to improve the security of real-world systems. This research activity embraces various possible topics and can be customized based on the candidate's preferences. Relevant to this activity are different kinds of security properties (e.g. authentication, confidentiality, and integrity), approaches (e.g. access control and information flow control), and system abstraction levels (e.g. design, configuration and implementation). One possible aim is to develop formal languages and methods for the specification and management of authorisation policies configured to enforce access control. A few challenges are: proving policies' correctness wrt high-level properties; defining correct-by-construction techniques to synthesise policies from high-level properties; developing formal analysis techniques to estimate the effects of the run-time interference between policy evaluation and system components' behaviour; determining the impact of policy changes, due to their maintenance and evolution over time, on systems components' behaviours.





Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



### 13. Security of 5G infrastructure and its evolution to 6G

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** Università degli Studi di Roma "Tor Vergata"

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <http://dottorati.uniroma2.it>

**Contact person:** Giuseppe Bianchi

#### Description

The emerging network infrastructures for cellular systems referred to as 5G and its evolution 6G are characterized by very high complexity and extreme diversification both in terms of network technologies (different radio accesses, including non-natively cellular accesses such as WiFi and Bluetooth, different infrastructure and transport technologies) and in terms of supporting computing systems (multi-access edge cloud, core cloud, continuum cloud). Such heterogeneity emerges in terms of multiple stakeholders and verticalization of services through so-called network slicing capabilities and has led to an impressive increase in the attack surface. The proposed project aims to address the security, privacy, and availability challenges emerging in the various functional and technological domains of the 5G architecture (radio interface, Multi-access Edge Computing, transport infrastructure, virtualized core network functions, management, and orchestration), covering, in particular, the aspects of continuous security verification and control (e.g., DevSecOps) through all the different phases of the 5G+ technology lifecycle (think, build, test, run&update). Special attention will be paid to the security aspects of 5G location systems and the protection of interfaces between network functions and the development of tools for assessing vulnerabilities at the protocol level.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 14. Well-founded cybersecurity techniques

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** Università Ca' Foscari, Venezia

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:**

**Contact person:** [Riccardo Focardi](#)

### Description

This project is part of the "Foundational Aspects in Cybersecurity" curriculum and concerns the use of formal methods applied to cybersecurity in order to improve the state of the art of system and network security. In particular, the PhD student will use formal verification techniques and tools in various application areas that the research group in Cybersecurity of Ca' Foscari actively deals with such as, for example: correctness of programs, secure compilation, security of Web and networks, security of embedded systems. The research aims to find new attacks and propose innovative solutions based on solid foundations and formal proofs of correctness, and will possibly be carried out in collaboration with the University spin-offs.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 15. Innovative and practical cybersecurity solutions for systems and infrastructures

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università Ca' Foscari, Venezia

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:**

**Contact person:** [Flaminia Luccio](#)

### Description

This project is part of the "Software, System, and Infrastructure Security" curriculum and concerns the study of innovative techniques for the security of software, hardware and communication systems. In particular, the PhD student will develop cybersecurity techniques and tools in various application areas which the research group in Cybersecurity of Ca' Foscari actively deals with, such as, for example: the correctness and protection of software, identification, Web and network security, embedded systems security, usable security. The research aims to find new attacks and propose innovative solutions with a practical impact, and will possibly be carried out in collaboration with the University spin-offs.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 16. Software security: analysis and verification of properties

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università di Pisa

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:**

**Contact person:** [Cinzia Bernardeschi](#) and [Gian Luigi Ferrari](#)

### Description

The overall topic for the phd project concerns the definition and development of techniques for the analysis and verification of software security. Techniques for ensuring that software is free of bugs and security vulnerabilities, included the disclosure of sensitive data, are of utmost importance, since software vulnerabilities can often be exploited to cause huge damage. Techniques in the scope of the phd project include program analysis based on static analysis (e.g., control flow analysis, taint analysis), abstract interpretation and symbolic execution, supported by constraint solving and SMT. The goals include to significantly extend the power and scalability of currently available techniques to make them applicable to real-world code bases, including concurrent and embedded software, as well as software for IoT systems.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 17. Data protection and privacy in innovative application scenarios

**Curriculum:** Data Governance and Protection

**University:** Università degli Studi dell'Insubria (Varese)

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <http://dawsec.dicom.uninsubria.it/elena.ferrari/>

**Contact person:** [Elena Ferrari](#)

### Description

The project aims to develop new solutions to support data providers to use and share end-users data by respecting users' privacy. The designed strategies will have to consider, on one side, the protection requirements of end-users and, on the other side, the data provider's economic assets (e.g., data utility, costs). This trade-off requires investigating the best-suited data protection policies and related technologies to enforce user requirements. For this purpose, it is expected to use different techniques, varying from AI to support user's requirements specification to anonymization algorithms. The project will target decentralized scenarios to go beyond traditional centralized architectures and application domains characterized by a massive amount of sensitive data (such as IoT). The Ph.D. student will investigate efficient techniques to support the necessary computation and will analyze the security and privacy properties of the developed methods under different attack scenarios.

The potential topics include (and are not limited to): DLT (Distributed Ledger Technology, e.g., blockchain) based services on the support of decentralized data sharing and auditing, risk assessment and data sharing in zero-trust architectures, data protection under normal and emergency situations, privacy preferences and data protection policies' specification and analysis.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 18. Certification Languages for Compliance and Security of Cloud Services

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy

**Funds:** Progetto Europeo H2020 MEDINA (grant nr. 952633) and Istituto di Informatica e Telematica

**Additional benefits:** Possibility of supplementing the scholarship with project funds

**Website:** <https://www.iit.cnr.it/en/marinella.petrocchi/> ; <https://www.iit.cnr.it/en/fabio.martinelli/>

**Contact person:** [Marinella Petrocchi](#) and [Fabio Martinelli](#)

### Description

The adoption of Cloud Computing in the EU is still limited. One reason for this is lack of security and transparency that customers perceive in this technology. Cloud Service Providers often rely on security certifications and compliance to regulations to improve this transparency. In this context, the EU Cybersecurity Act proposes improving customer trust in the European ICT market through a set of EU-wide certification schemes, such as the European Cybersecurity Certification Scheme for Cloud Service (EUCCS) being developed by the European Union Agency for Cybersecurity (ENISA). Unfortunately, the requirements dictated by the certification schemes -EUCCS is not an exception- are defined in natural language. They need to be translated into a machine-readable representation, which facilitates their processing. This project aims to automatically transform the natural-language specification of cloud security certification frameworks, like EUCCS, into machine-readable expressions, by leveraging Natural Language Processing techniques. Ultimate goals are: a standardized way to technically approach the requirements of a security certification scheme; a framework and working language to express requirements as automatically actionable controls; the reduction of the operation workload for technical staff related to (cloud) security certification processes; the adaptation of the framework to data usage policies for checking compliance to regulations, as the EU Data Act and similar.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 19. Cognitive characterization of fake media and media manipulation

**Curriculum:** Data Governance and Protection

**University:** University of Siena

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <http://clem.dii.unisi.it/~vip/index.html>

**Contact person:** [Mauro barni](#)

### Description

The diffusion of fake media and the ease with which end-users can create fake media is raising increasing concern, due to the impact that the diffusion of fake media can have on our society. Multimedia forensic researchers have developed several tools to distinguish genuine media from fake ones, and to identify various forms of media manipulations. Yet, detecting fake media and media manipulations is not enough to prevent the diffusion of fake news and the use of manipulated media for disinformation campaigns; it is necessary that the malevolent use of the manipulations is also identified. The next challenge in media forensic, then, is to link the detection of asset manipulations to the purpose of the manipulations and the role that the assets and their manipulations have in the context wherein they are used. In the above framework the goal of this project is twofold: i) to build suitable cognitive models to study the affective impact that media manipulations and the use of fake media have on the users; ii) to develop a pool of automatic techniques to link the manipulations of a media asset to the intended meaning of the manipulations. Depending on the background of the PhD candidate, research may focus more on cognitive aspects (qualifying the research for the "Human, economic and legal aspects in cybersecurity" curriculum) or on technological aspects (better suited to the "Data governance and protection" curriculum)



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 20. Human and socio-legal dimensions for a better-safe Cyberspace

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Università di Firenze

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:**

**Contact person:** [Andrea Simoncini](#)

### Description

Cybersecurity, meaning the security of cyberspace, is more than a technical problem and doesn't only focus the protection of data and infrastructures from intrusions. It encompasses all the human, socio-legal and economic dimensions related to the development of the digital world in today societies. This new and complex research field includes five main areas of inquiry. 1) Models of regulation and Authority enforcement for a safe Cyberspace. 2) Ethical and legal aspects of Cybersecurity. 3) Cybercrime and CyberDiplomacy 4) Social and economic policies for cybersecurity 5) Data governance, national clouds and digital sovereignty. All the research areas are to be matrixed over some main foundational and methodological pillars: fundamental-rights protection, the evolving-upcoming global regulation (EU vs US vs China), the socio-economic impact of cyber-regulation, human and social effects of cyber-society. Phd candidates can focus their project on either one or more cross-cutting research areas. Research projects have to be preferentially designed according to a holistic, multidisciplinary, problem-solving approach and should involve public and private stakeholders, implementing innovative technological, legal, ethical and organizational solutions, such as strengthening key competencies, transfer of technologies and knowledge, and the ability to integrate technologies in systems and services.





Finanziato  
dall'Unione europea  
NextGenerationEU



## 21. Methods and tools for the security assessment of critical information infrastructures

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** IMT School for Advanced Studies Lucca

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:** Full board accommodation

**Website:** <https://sysma.imtlucca.it/>

**Contact person:** Letterio Galletta

### Description

Information and communications technologies (ICTs) are increasingly common in our daily activities. Some of the ICT systems, services, networks, and infrastructures form a vital part of our society, providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as Critical information infrastructures (CIIs) as their disruption would seriously impact vital societal functions. Since cyber threats to CIIs could potentially affect the safety of citizens, many of these systems require a high level of security.

Security engineering for CIIs is a multidisciplinary field involving various topics ranging from secure software development and cryptography to embedded systems design and network security. Formal modeling and verification techniques have the potential to provide strong security guarantees and support vulnerability detection tools. However, developing effective formal methods-based tools for CIIs is still open.

This project aims to study new methodologies and tools based on formal methods for the security assessment of CIIs that could support Macro-regional CSIRT in their activities. The research activity could focus on different aspects, such as network security, protocol security, and application security. Also, different verification techniques may be considered, including, for instance, model checking, fuzzing, static analysis, and security testing.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 22. Enhanced soft computing techniques for fake news detection

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Università degli Studi di Salerno

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://www.unisa.it/>

**Contact person:** [Vincenzo Loia](#)

### Description

The spread of fake news through the social media is a relatively new problem. Its importance is witnessed by the attention paid by social network platforms such as Facebook, Whatsapp. Fake news can take several different forms in the social media environment, making even more difficult to efficiently detect and contrast them. An example is offered by clickbait headlines, inducing users to open possibly biased articles to gain money from views. The literature trend in this field is about supervised classification approaches. The interest in deep learning (DL) techniques, such as Recurrent Neural Networks and Convolutional Neural Networks, seems to be dominant. Such DL techniques represent the state of the art. Anyhow, there are still some concerns and open issues. First, fake news still has to be fully understood from a linguistic perspective. In this regard, the fuzzy logic (FL) formalism may help. The contributions to the field using FL are still scarce and not offering a formal response to address the open issues. Secondly, both content- and context-aware techniques should be implemented. Finally, it is worth mentioning the lack of widely accepted benchmark datasets. The currently available resources may not be sufficient to check the effectiveness of new models in a real-world scenario. This research project aims to address the main open issues above, prioritizing the FL formalism to obtain more effective DL variants.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



### 23. Cyber Security and Cyber Intelligence measures for Monitoring, Preventing, and Mitigating Radicalisation Pathways

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Università degli Studi di Salerno

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://www.unisa.it/>

**Contact person:** Giuseppe Fenza

#### Description

The role of the Internet in radicalization has been widely discussed since 1990s. Radicalization is the process of pushing an individual towards more extremist views. Online communities play a central role in spreading radicalization since users may disseminate their radical ideologies, gain support and provide instruction in terrorist activity. Additionally, the homophily property underlying recommendation systems traps the users in radicalization pathways, shifting their opinions along the time from moderate to extreme. An effect of this can be echo chambers, where particular opinions can easily start to be re-shared and reinforced, which could have the gradual effect of causing someone to experience a change in mindset. Therefore, tools for user monitoring are required, such as filter bubbles to track information about users' activities combined with AI techniques that can help discover polarized social groups.

The goal of this research project is aimed at finding cybersecurity solutions to contain the radicalization phenomenon. The main topics to investigate to achieve the prefixed goal are listed as follows:

- Community detection and network monitoring
- Echo chamber and group polarization detection
- User interaction analysis by fusing network topology with semantic information
- Influential node identification for inter-community polarization analysis
- Dynamic network graph time-evolution analysis.
- Prediction of group polarization evolution.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 24. Cryptographic protocols for the cyberspace

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** Università degli Studi di Salerno

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:** <https://www.unisa.it/>

**Contact person:** Alfredo De Santis

### Description

The project focuses on the design and the analysis of new cryptographic primitives and protocols, suitable for strengthening communication systems and distributed systems, and tailored for the realization of secure, private, and resilient digital infrastructures. The main cryptographic area on which the efforts will be concentrated is secure computation. The research targets are scalable, efficient, and flexible multiparty solutions, secure against powerful adversarial strategies, privacy preserving, and adaptable to a variety of applicative settings. In particular, the project will be developed along two research lines: - two-party and multi-party computation general protocols will be optimized and properly customized to solve specific issues in traditional computational settings, wired and wireless, and in the newest lightweight infrastructures, quickly evolving during the last years - two-party and multi-party ad-hoc protocols will be designed and analyzed, to solve in a more efficient way, compared to the general solutions, basic problems, of interest by themselves and as intermediate steps in complex problems. Regarding the second research line, among the others, attention will be focused on secret sharing schemes, on protocols for secure set operations, and on encryption/authentication primitives, useful for secure computation, especially in lightweight settings. As well as, on applications of machine learning techniques, both as a constructive tool for protocol design, and as a destructive tool for protocol analysis

## 25. Keeping systems, data, and your identity secure

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università della Calabria

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:** <https://people.dimes.unical.it/andreapugliese>

**Contact person:** [Andrea Pugliese](#)

### Description

The project plans to study problems related to different aspects of cybersecurity, with the aim of identifying methodological and technological approaches and solutions to the issues that currently present the greatest interest and criticality (including by studying real case studies proposed by public and private actors and stakeholders) aiming at the definition and development of more secure and reliable processes and infrastructures.

The main topics of the project include:

- methods, techniques and tools for the protection of systems, infrastructure and data;
- methods, techniques and tools for digital identity and accountability.

The student will study and identify, in the above areas, appropriate solutions for the benefit of individual citizens, public institutions and other complex organizations. The student will also develop knowledge and skills that will allow him or her a wide range of professional possibilities, in the public sector (including the National Cybersecurity Agency), in research laboratories, centers of study and expertise, private sectors, and other complex organizations, including through collaboration with inter- and multi-disciplinary teams in cybersecurity - in general, in realities that require professionals with solid scientific, methodological, and technological skills in cybersecurity.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 26. Advanced usage control approaches for data protection

**Curriculum:** Data Governance and Protection

**University:** IIT-CNR

**Funds:** Progetto Europeo E-CORRIDOR e IIT

**Additional benefits:** Possibility of supplementing the scholarship with project funds

**Website:** <https://www.iit.cnr.it/en/fabio.martinelli/>

**Contact person:** Fabio Martinelli

### Description

The focus of the PhD work is about the study of models and architectures for advanced data usage control approaches for protecting data privacy while ensuring a controlled data sharing, as well as achieving digital sovereignty. The PhD work will include the design of a general architecture of a usage control framework able to enforce policies on data and services offering flexing enforcement and obligation management opportunities. The main feature of such a framework will be the capability to promptly react to changes in the access control context while accesses are in progress, according to what specified in the policy itself. Such architecture will be very modular and flexible in order to be easily configurable to be adapted and customized for a number of relevant use cases that will be identified as part of the PhD work. The PhD work will also include the study of the integration of the usage control framework with novel techniques for preserving the privacy of the framework users.



Finanziato  
dall'Unione europea  
NextGenerationEU



## 27. Use of Artificial Intelligence for the protection of Critical Infrastructure

**Curriculum:** Software, System, and Infrastructure Security

**University:** Politecnico di Bari

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://www.poliba.it>

**Contact person:** Eugenio Di Sciascio

### Description

Critical Infrastructures represent a set of technological assets that produce vital activities and services for the country by dispatching Primary Services that, when integrated with each other, enable the interoperability of other services (logistics, health, financial). It becomes critical to secure people from any cyber attack. Using AI techniques, this research proposal aims to investigate and implement new capabilities for the management, detection, and response of attacks that can be handled by such infrastructures. Through the adoption of AI techniques and algorithms, new capabilities for monitoring information flows between the entities involved will have to be developed. To achieve the stated objectives, this proposal uses AI approaches to investigate:

- GEOINT: Geospatial information collected from satellite photographs and areas or from map and terrain data.
- MASINT: Measurement and signature information collected from a range of signatures of fixed or dynamic target sources. (Masints are divided into:electro-optics, nuclear, radar, geophysics, materials, and radio frequency).
- OSINT: Information gathering from open sources. Through the development and adoption of threat intelligence techniques based on AI algorithms, it will be possible to improve cyber vulnerability analysis of critical infrastructure, implementation of attack/defense models, and practices to harmonize emergency response.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 28. Formal Models of Cyber Security

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** GSSI

**Funds:** Decreto MUR n. 351 del 09-04-2022, lett. b. (borse per dottorati di ricerca PNRR)

**Additional benefits:**

**Website:** <https://cs.gssi.it/emilio.tuosto/>

**Contact person:** Emilio Tuosto

### Description

The ambition of this project is to extend the research on security protocols by explicitly accounting for the “human factor”. In fact, human behaviour is critical in determining the degree of security of an organisation. Many attacks hinge on people’s “misbehaviour”. Many factors contribute to “human misbehaviour” that makes critical assets vulnerable. For instance, people may ignore well-specified practices due to negligence, lack of appreciation of the security risks, or misunderstandings (eg, when or how should a rule be applied). Also, protocols and legal requirements may change over time and their compliance may be compromised by miscommunications.

This project will address the following research questions

RQ1: “How human behaviour should be formally specified and taken into account in the analysis of cybersecurity?”

RQ2: “How to support continuous compliance?”

We will develop mechanisms to specify cybersecurity protocols and their usage (aka ceremonies) modelling human behaviour in terms of non-deterministic and probabilistic system. We will study the robustness of cybersecurity protocols in presence of misbehaving roles.

Human behaviour impacts on continuous compliance. Critical applications eg, in the automotive domain, are continuously enhanced through dynamic over-the-air updates. This poses various challenges related to both safety and security and, specifically, there is an increasing demand of continuous compliance with safety and security standards.





Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 29. Cybersecurity of Complex Systems

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università degli Studi di Genova

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://www.csec.it/>

**Contact person:** [Alessandro Armando](#)

### Description

The candidate will develop one of the following lines of research:

- Application Cyber Risk Assessment: developing automated or semi-automated procedures for assessing the cyber risk exposure of application ecosystems in emerging scenarios, e.g., Mobile, Cloud, Fog, IoT, and any combination thereof.
- Multi-domain Cyber Range and Cyber Resilience Testing of Physical Cyber Systems: definition of a framework for integration between Cyber Range and digital replicas (Digital Twin) of physical infrastructure (e.g., transportation infrastructure) to create multi-domain scenarios for cyber risk resilience testing activities, procedures, and countermeasures against attacks, evaluation of procedures and training of personnel.



Finanziato  
dall'Unione europea  
NextGenerationEU



### 30. Foundations and Methodologies for Secure Programming of CPS

**Curriculum:** Foundational Aspects in Cybersecurity

**University:** Università di Camerino

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <http://micheleloreti.com>

**Contact person:** Michele Loreti

#### Description

Modern software architectures, often referred as Cyber-Physical Systems (CPS), are often composed by a large number of entities that interact with each other and with the enclosing environment to reach local and global goals. Formal tools and methodologies are needed to supporting development of secure CPS. In this project we plan to study a framework that, following a "property driven" pattern and integrated in a "secure by design" approach, permits developing secure CPS. The goal of the project is to develop a methodology that, starting from a formal definition of both "functional" and "non-functional" system requirements, permits checking and refining the expected properties along the whole development process. System requirements will be defined at both global and local level. Global properties identify the overall requirements of a system and typically render the expected emerging behaviour. Local properties consider the behaviour of the single components. Tools will be studied to guarantee that the satisfaction of these requirements is preserved at the different stages of development and that lead to the set of formulas that should be satisfied at runtime. These formulas will be also used to instrument runtime monitors. These will guarantee that in the operating environment, which can differ from the one considered at design time, the behaviour emerging from local and global interactions meets with the requirements defined along the development phase.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



### 31. The Anti-Digital Forensics Cyber Kill Chain

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università di Catania

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:**

**Contact person:** [Giampaolo Bella](#)

#### **Description**

Criminals hardly ever plead guilty, hence Digital Forensics (DF) comes into play as the lawful discipline to gather and interpret evidence in support of a conviction or of an overturning. Coherently with our computerised times, DF vastly relies on computer support through a number of dedicated techniques and tools.

Yet, following the establishment of DF as a routine practice, criminals have tried out novel heuristics and often adopted or developed a new range of tools to counter and, ultimately, evade that practice. For example, wiping off metadata may dramatically influence a verdict, and full-disk encryption on a storage unit may signify that crucial evidence goes unnoticed. In consequence, Anti-Digital Forensics (ADF) is just peeking out and, due to the basic cybersecurity motto that one needs to play as an attacker to develop the best defence, is worth developing with ethical purposes.

This project aims to: establish ADF as a discipline, elicit its requirements and aims, specify its various sub-application domains and, chiefly, advance an ADF Cyber Kill Chain (CKC) as a field reference. While building the ADF CKC is challenging because it requires a vast skillset covering DF, cybersecurity, data protection and programming, it would largely assist DF experts through the development of counter-evasion strategies.

The ADF CKC will be piloted for the sake of validation over data such as multimedial files and environments such as modern car infotainments.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 32. Investigation on GAN- Generated Malware

**Curriculum:** Software, System, and Infrastructure Security

**University:** University of Sannio

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://www.unisannio.it/it/users/visaggio>

**Contact person:** [Corrado Aaron Visaggio](#)

### Description

The co-evolution of malware and malware detection system is a cycle is becoming faster and faster, and requires the development of effective countermeasures in a similar short time. The increasing adoption of machine learning classifiers for automatically recognizing malicious programs and behaviours related to intrusions, spreading, evasion and survival is exposing protection systems to adversarial attacks. Three approaches are mainly used for producing adversarial examples: gradient-based, optimization-based, and Generative Adversarial Networks(GAN). GAN consists of a iterative competition between two components, the Generator and the Discriminator, where the former produces candidate adversarial examples, while the latter evaluates their effectiveness. The evaluation provided by the Discriminator leads the Generator to modify further the original example. The PhD course will focus on three tasks. As first, the candidate should understand how a GAN can be used to modify existing malware, while preserving behavioural properties of the program, i.e. changes to malware shouldn't affect its correct working. As second task, the candidate should study which kind of methods could be able to detect GAN-generated malware and disarms the harming potential of such a malicious creation. As third task, the candidate should design and execute a comprehensive set of experiments for demonstrating the elaborated theses regarding how to recognize the GAN-generated malware.



Finanziato  
dall'Unione europea  
NextGenerationEU



### 33. Application of zero-knowledge techniques to IoT constrained devices

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università di Camerino

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <http://www.leonardomostarda.net>

**Contact person:** [Leonardo Mostarda](#)

#### Description

Zero-Knowledge proofs (ZK-proofs) have become widely adopted in various contexts such as blockchain, finance, voting, ethical behavior and anonymous authentication. This advanced cryptography is capable of proving the correctness of financial transfers, protocol interactions or more generally state updates without disclosing sensitive information. ZK-proofs not only guarantee privacy but also allow trust of a multi-party computation when the entities involved do not trust each other. The application of ZK-proofs is particularly challenging in IoT systems since IoT constrained devices can have limited memory and computation power. These IoT devices require efficient ZK-proofs in terms of space and computation. Although some ZK-proofs techniques can keep the size of data (e.g., by aggregation with recursive proofs) they have not been tailored in the context of IoT constrained devices. The aim of the project is to advance the state-of-the-art of ZK-proofs in the context of IoT constrained devices as an efficient solution for IoT systems integrated with blockchain. Such integration can result in a secure and scalable decentralized IoT system that can see applications in various contexts such as the Industry 4.0 and Smart Cities. The proposed solution will be validated in real industrial scenarios.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



### 34. Hardware implementation of Post Quantum Cryptography algorithms

**Curriculum:** Software, System, and Infrastructure Security

**University:** Politecnico di Torino

**Funds:** DM 351-PNRR: Pubblica Amministrazione

**Additional benefits:**

**Website:** <https://cybersecnatlab.it>

**Contact person:** Paolo Prinetto

#### Description

Over the coming years, with the growing of Quantum Computing, it is expected that Post Quantum Cryptography (PQC) will replace the current public-key cryptography paradigm. PQC leverage on mathematical elements which are not straightforward to implement on standard processor, as well as require non-negligible computational power and resources to be executed. Therefore, the interest in hardware accelerator for PQC is continuously increasing. In 2017 NIST started a standardization process for PQC algorithm. Since then, in the literature, implementation of the different candidate protocols has been proposed, mainly in pure software or through hardware-software co-design methodology. However, very few pure hardware design has been proposed. The PhD work will focus on pure hardware implementation of PQC algorithms, following two main approaches: (i) to build an Application Specific Integrated Circuit (ASIC) to accelerate the requested algorithm. This solution can reach the best performance, but it requires a considerable design effort and relative non-recurrent costs. (ii) to integrate PQC algorithm directly in the processor pipeline with smaller hardware accelerator. This in-pipeline acceleration approach can be evaluated on open Instruction Set Architecture (ISA) processors, such as the RISC-V architecture. The hardware design should minimize resource utilization, in terms of area and power, exploiting parallel and pipelined computations.

### 35. Data protection in emerging scenarios

**Curriculum:** Data Governance and Protection

**University:** Università degli Studi di Milano

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://samarati.di.unimi.it>

**Contact person:** Pierangela Samarati

#### Description

The availability of highly performing systems and services for gathering, storing, and processing data, and of analysis techniques on large data collections, bring great benefits on a personal, business, economic and social level. The collection, sharing and analysis of data, with contributions from different sources and different actors is in fact a great enabling factor for an increasingly digitally evolved society. On the other hand, a strong obstacle to the true realization of this vision is represented by legitimate considerations on data protection. In fact, the (real or perceived) loss of control over data by those who have the authority over them, and the potential compromise of data confidentiality, represent a strong obstacle on the creation of an open framework for information sharing and analysis. The goal of the project is to contribute to the development of advanced solutions enabling the different actors with control over their data in the various data release, sharing, and analysis scenarios. The research can entail investigation in different areas, including: data governance frameworks to support the protection requirements; policy languages and models to express them and techniques for enforcing them; approaches for effective and efficient access to data, offering computation and management functionality, while ensuring the confidentiality and integrity of data and computations; approaches for selective controlled data sharing and release, for the protection of information and computation models in distributed, pervasive, and intelligent scenarios.



Finanziato  
dall'Unione europea  
NextGenerationEU



### 36. Human-centered Framework to integrate trustworthy and cyber intelligence in digital systems

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Università degli Studi di Bari Aldo Moro

**Funds:** DM-351-PNRR: Ateneo

**Additional benefits:**

**Website:** <https://serlab.di.uniba.it/people/danilo-caivano/>

**Contact person:** Danilo Caivano

#### Description

The intelligent systems that pervade our society and interact with users daily, without users being aware of it, need to be regulated, monitored, and constantly analyzed to ensure fair and explainable results and the satisfaction of ethical, security, and privacy criteria. Such systems generate an output that can be, from time to time, a content, prediction, recommendation, or decision that influences the users' behaviors and the environment with which they interact. If the decisions made by the systems are not verified, fair, and explainable, there is a reputational and economic risk to organizations that can impact the security of users and the organization itself. It is therefore important not only to constantly monitor the behavior of such systems to avoid unfair or even wrong outcomes but also to establish metrics that measure the risks and countermeasures to be put in place to mitigate risks to users' security. The European Community has issued several guidelines in recent years to ensure that these systems meet a suitable level of accuracy, robustness, and security. It becomes, therefore, essential to establish an assessment framework that provides a gap analysis, risk assessment, and remediation plan to validate these systems and make them compatible with current regulations.





Finanziato  
dall'Unione europea  
NextGenerationEU



### 37. Design of novel security firmware for modern microarchitectures

**Curriculum:** Software, System, and Infrastructure Security

**University:** Università di Trento

**Funds:** Research funds

**Additional benefits:**

**Website:** <http://www.disi.unitn.it/~crispo>

**Contact person:** [Bruno Crispo](#)

#### Description

Modern microarchitectures implement numerous security mechanisms at the hardware level that are not or only partially exploited by existing software. This doctoral scholarship concerns the study, design, implementation, and validation of new software security services that exploit these new hardware mechanisms. These services, typically running within Trusted Execution Environments (TEE), will complement and/or enrich existing ones (e.g., secure boot, integrity attestation, cryptographic functions, etc.) in order to provide a rich set of security services to operating systems. These services will be designed, implemented, and verified using open and public specifications. The Ph.D. also includes the study of existing secure execution environments in order to assess the causes behind the many flaws and vulnerabilities that have emerged in recent years.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



## 38. Cyber security applied to 4/5G Mission Critical Networks and Applications

**Curriculum:** Software, System, and Infrastructure Security

**University:** IMT School for Advanced Studies Lucca

**Funds:** DM 352-PNRR: Leonardo SpA

**Additional benefits:** Full board accommodation

**Website:** <https://sysma.imtlucca.it/>

**Contact person:** [Mirco Tribastone](#)

### Description

The Ph.D. student will focus her/his activities on studying new methodologies and tools for security assessment and design of secure telecommunications networks in 4/5G technology for Mission and Business Critical applications. This type of communication infrastructure and its applications are a vital asset for all public and private emergency response organizations that use them for their operations. Their disruption or failure can impact the vital functions of these organizations, cause possible loss of life, and possibly impact the safety of citizens and operators.

Formal modeling and verification techniques have the potential to provide robust security assurances and support vulnerability detection tools. However, developing effective tools based on this methodology is still an open issue. The research activity will focus on several aspects, such as the definition of a formal methodology that enables the secure and resilient cyber design of the network solution (access, transport, core network, and applications) also about cloud deployment models, verification of security at the network, protocol and application levels (with particular focus on Police Force use case applications).

In addition, the research activity will consider as reference the specifications, recommendations, and best practices of the main international bodies in the field of communications security and, in particular:

- The 3GPP security standards (Release 16 and later)
- The NIST ZTA (U.S National Institute of Standards and Technology) guidelines.
- European Commission guidelines (EU toolbox for 5G security, NIS directive, ENISA line guide).

Security of open RAN architectures, as specified by the O-RAN Alliance Security Focus Group, will also be the research subject.

Various verification techniques may be considered, including, e.g., model checking, fuzzing, static analysis, and security testing.

The research product will also involve publications of an applied nature on communication solutions developed by Leonardo S.p.A. for broadband 4/5G telecommunications networks.



Finanziato  
dall'Unione europea  
NextGenerationEU



SCUOLA  
ALTI STUDI  
LUCCA



### 39. Evolutionary application of AI techniques in cybersecurity

**Curriculum:** Software, System, and Infrastructure Security

**University:** IMT School for Advanced Studies Lucca

**Funds:** DM 352-PNRR: Thales Group

**Additional benefits:** Full board accommodation

**Website:** <https://sysma.imtlucca.it/>

**Contact person:** [Rocco De Nicola](#), [Simone Soderi](#)

#### Description

The research project will be in the context of heterogeneous application domains such as critical infrastructure, manufacturing, and public administration, and aims to enable the integration of Artificial Intelligence and Machine Learning algorithms on Cyber Security Intelligence, Cyber Monitoring and Cyber Attack Simulation platforms, and to enrich their analysis and detection effectiveness and to achieve the following objectives:

- implementation of automatic mechanisms for learning behaviors on the network and systems in order to develop advanced correlation rules for early detection of possible attacks and anomalies;
- reduction of alerts generated by monitoring platforms to only significant events that need to be investigated, ensuring full support to cyber operators during the incident analysis activity through the possibility of "navigating" the specific correlation and behavioral investigation path;
- build a theoretical/practical framework that enables mechanisms for predictive analysis of possible cyber attacks towards the assets that need to be protected (simulation, predictive alerting), also through the refinement of AI techniques used in cyber defense to avoid the limitations of current applications about the risk of missing so-called "weak signals"

The study will use an existing complex Security Intelligence /CSOC - Cyber Security Operation Center platform to develop the research project and the various AI and Machine Learning algorithms to be implemented, aiming to realize a demonstrable PoC- Proof of Concept.

Added to this is the need to adequately protect Big Data that is created by cyberinfrastructure (logs, events, network flow, data enrichment, metadata, Threat Intelligence, Data lake, Threat Hunting, etc.). Therefore, the research project will include a specific study to identify and implement quantum/post-quantum encryption techniques appropriate for protecting complex, heterogeneous, and distributed databases such as the analyzed Big Data Cyber.



Finanziato  
dall'Unione europea  
NextGenerationEU



#### 40. Analysis of a highway operator's automated critical IT and OT infrastructure systems and identification of innovative cybersecurity solutions

**Curriculum:** Software, System, and Infrastructure Security

**University:** IMT School for Advanced Studies Lucca

**Funds:** DM 352-PNRR: Autostrade per l'Italia, S.P.A.

**Additional benefits:** Full board accommodation

**Website:** <https://sysma.imtlucca.it/>

**Contact person:** [Letterio Galletta](#), [Massimiliano Masi](#)

##### Description

Critical infrastructure is a system whose destruction, disruption or even partial or momentary unavailability significantly weakens a country's efficiency and normal functioning, as well as the security and economic-financial and social system. A particular type of critical infrastructure is air, sea, rail, and road transport. Although ENISA and the EU Commission have produced several publications and guidelines on critical infrastructure protection for the energy, financial, or maritime transport sectors, a specific guideline for the road transport sector is lacking.

The first objective of this research activity is to define a methodology that enables the design of a system that enables road transport, that is secure from its design or in its re-engineering, that goes to avoid data silos, and that facilitates the exchange of knowledge and expertise among international stakeholders, such as road operators, smart cities, and emergency responders.

The second objective of this activity is to design and implement innovative technical solutions in the area of cybersecurity for the road transport sector, particularly highway tunnel automation and smart road systems. The activity will mainly consider IT/OT/IoT systems that realize the critical infrastructure and services delivered by cloud systems. Special attention will be given to the safety and availability aspects of the systems.



Finanziato  
dall'Unione europea  
NextGenerationEU



#### 41. Development of technologies for automatic recognition of (deep) fake news on OSN

**Curriculum:** Human, Economic, and Legal Aspects in Cybersecurity

**University:** Università degli Studi di Catania

**Funds:** DM 352-PNRR: Ermes Cyber Security S.R.L.

**Additional benefits:** Possibility of supplementing the scholarship with company funds

**Website:** <https://www.dmi.unict.it/~battiato/>

**Contact person:** [Sebastiano Battiato](#)

##### **Description**

The generation and spread of fake news is a social problem with major repercussions on security and privacy, as well as a technique often used by attackers to carry out targeted attacks on companies and institutions. Cases have emerged in which fraud and credential theft attacks have been carried out, starting from fake news, with significant economic losses and social damage. Moreover, attackers are increasingly resorting to AI-based techniques such as Deep Fake and Fake Speech. The purpose of the Ph.D. will be to explore the world of online disinformation and to develop methodologies that analyze texts, multimedia content, and interactions on social networks to detect attacks based on AI-generated synthetic content. These technologies will then be applied to collect information and metadata about the players involved in the attacks (the attackers, victims, and any intermediaries) to facilitate correlations and simplify intelligence functions.