Via Europa 18
San Donato Milanese, 20097, MI
Italy
+39 340 818 6441
stefano.longari@polimi.it
Website
LinkedIn
Scholar Scopus

Stefano Longari

Curriculum Vitae

Last updated: March 18, 2026

I have been a RTDa (fixed-term researcher) at Politecnico di Milano since 2023, within the Department of Electronics, Information and Bioengineering (DEIB). My core research interests focus on the security of cyber-physical systems and critical infrastructures, particularly in automotive, satellite, and industrial environments. My work addresses the identification of novel threat scenarios targeting innovative cyber-physical infrastructures and the development of detection methods for such threats, including but not limited to approaches based on machine learning algorithms. In addition, I pursue a secondary research direction on social engineering and the impact of AI on it over the past decade. I am the instructor of the course "Human and Physical Aspects of Security", offered jointly to Politecnico and Bocconi students, which covers threat modeling, cyber-physical systems security, and social engineering. I have also served as a lecturer and teaching assistant for Ph.D. and master's level courses on a wide range of cybersecurity topics, and I coordinated an industrial specialization program in cybersecurity. I act as a reviewer for several Q1 academic journals, have served on the program committees of multiple international conferences, and currently advise three Ph.D. students and have advised or co-advised more than fifty master's theses.

Contents

Overview

Current Role: Junior Researcher (RTDa) at Politecnico di Milano *since May 2023*

Scientific Productivity: Author of 9 journal papers (7 with Q1 ranking) and 19 peer-reviewed conference papers (2 with A* ranking). Author of 2 patents.

Based on Google Scholar: h-index 9 citations 416

Based on Scopus: h-index 8 citations 250

Fundings: Task leader for the *AHEAD* european project, participant of the *SARIL* and *KEEPER* european projects. Local PI for the *SOCRATE* project funded by ASI, and participant to the *MICS* PNRR project. PI for an industrial contract on satellite cybersecurity. Won a Funded Ph.D. position from ACN.

Academic Roles: Chair and member for the master *thesis examination boards* of Politecnico di Milano and member of *thesis examination boards* for Bocconi. Coordinator of the *Security Specialist specialization degree* (equivalent to an academic master) for CEFRIEL and Politecnico di Milano. Organizer of the OWASP Italy Day 2023 conference.

Worked as PC of 9 cybersecurity-related conferences, amongst which ACSAC and DIMVA.

Reviewer for 13 Q1 journals and transactions.

Invited Talks: Various presentations at industrial events, HackInBo, and Hardwear.io.

Advisor Activities:

Currently advisor of 3 Ph.D. students in Computer Science and Engineering.

Advisor or Co-advisor of over 50 Master Theses for the Computer Science and Engineering Master.

Advisor of ∼10 Master Theses for the Cyber Risk Strategy and Governance Master.

Teaching Activities: Course instructor for 1 Ph.D. course, 2 Master courses, and various industrial courses:

Ph.D.: Advanced Research Topics in Cybersecurity.

Master: Human and Physical Aspects of Security course for Politecnico di Milano and Bocconi.

Master: Emerging Topics in Cybersecurity Course for Bocconi.

Research Interests

My research spans approximately seven years, beginning with my Ph.D. studies, which initially focused on automotive cybersecurity. I concentrated on securing vehicle on-board systems, specifically targeting vulnerabilities and intrusion detection mechanisms within the Controller Area Network (CAN) protocol. This early work involved creating real-world datasets, publishing *machine learning-based IDS frameworks*, and identifying *novel threats* and attack surfaces.
Building upon this foundation in automotive security, I have broadened my expertise into the wider domain of Cyber-Physical Systems (CPS). My current research encompasses diverse fields, still including the automotive one, but expanding to industrial robots, railway infrastructure, e-vehicle charging solutions, satellite systems, and critical infrastructure resilience. Across these domains, my main interests are *attack detection and threat modeling*, exploring threats emerging from integrating novel technological solutions into existing systems.
Additionally, I am participating in various projects addressing emerging cybersecurity challenges involving AI-driven social engineering, covert communication channels utilizing Large Language Models (LLMs), and vulnerabilities within federated learning systems.

Experience

Junior Researcher (RTDa)

Politecnico di Milano (Milan, Italy) *May 2023 — Current*

Research topic: Threat modeling, offensive, and defensive measures for novel cyber-physical systems.
Research group: NECSTLab, System security research group.

Postdoctoral Researcher

Politecnico di Milano (Milan, Italy) *Jun 2021 — Apr 2023*

Research topic: Offensive and defensive security techniques for cyber-physical systems.
Research group: NECSTLab, System security research group.

Research Internship

ESCRYPT GmbH (Stuttgart, Germany) *Oct 2019 — Apr 2020*

Research topic: Development of new security techniques for automotive on-board CAN-connected devices.

Education

Ph.D. in Information Technology, Politecnico di Milano *Jun 2021*
Dissertation title: *On the security of connected automotive systems*
M.Sc. in Computer Science and Engineering, Politecnico di Milano *Apr 2018*
Dissertation title: *On the security of connected vehicles*
Bachelor in Computer Science and Engineering, Politecnico di Milano *Sep 2015*

Publications

Productivity and Impact Metrics

Scientific Productivity: Author/Co-author of 9 scientific publications on journal papers, including 7 top-ranked Q1 journal papers based on SCIMAGO, and 21 peer-reviewed conferences, including 2 top-ranked security conferences, where one work received an award for its value. 26 publication entries on Scopus. 35 publication entries on Google Scholar.

Based on Google Scholar: h-index 11 citations 494
Based on Scopus: h-index 8 citations 290

Peer-reviewed Journals

- Digregorio, G., Saputelli, E., **Longari, S.**, Carminati, M., & Zanero, S. (2025). *Swarm: A Distributed Ledger-based Framework to Enhance Air Traffic Control Security Using ADS-B Protocol.* ACM Transactions on Privacy and Security.
- **Longari, S.**, Cerracchio, P., Carminati, M., & Zanero, S. (2025). *Assessing the Resilience of Automotive Intrusion Detection Systems to Adversarial Manipulation.* ACM Transactions on Cyber-Physical Systems.

- Barelli, R., D'Onghia, M., & **Longari, S.** (2025). *Towards Secure Electronic Voting: a Survey on E-Voting Systems and Attacks.* IEEE Access.
- **Longari, S.**, Jannone, J., Carminati, M., Tanelli, M., & Zanero, S. (2024). *Janus: A Trusted Execution Environment Approach for Attack Detection in Industrial Robot Controllers.* IEEE Transactions on Emerging Topics in Computing.
- **Longari, S.**, Pozone, A., Leoni, J., Polino, M., Carminati, M., Tanelli, M., & Zanero, S. (2023). *CyFence: Securing Cyber-physical Controllers Via Trusted Execution Environment.* IEEE Transactions on Emerging Topics in Computing.
- Nichelini, A., Pozzoli, C. A., **Longari, S.**, Carminati, M., & Zanero, S. (2023). *Canova: a hybrid intrusion detection framework based on automatic signal classification for CAN.* Computers & Security, 128, 103166.
- Maffiola, D., **Longari, S.**, Carminati, M., Tanelli, M., & Zanero, S. (2021). *GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems.* IEEE Transactions on Intelligent Transportation Systems.
- **Longari, S.**, Valcarcel, D. H. N., Zago, M., Carminati, M., & Zanero, S. (2020). CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network. IEEE Transactions on Network and Service Management, 18(2), 1913-1924.
- Zago, M., **Longari, S.**, Tricarico, A., Carminati, M., Pérez, M. G., Pérez, G. M., & Zanero, S. (2020). ReCAN–Dataset for reverse engineering of Controller Area Networks. Data in brief, 29, 105149.

Peer Reviewed Conference Proceedings

- Santorsola, A., Mammone, D., **Longari, S.**, Topputo, F., Mergè, M. (2025, November). An End-to-End GEO Satellite Links Simulation Framework for Cyber Range Applications. In 2025 Security for Space Systems (3S) (pp. 1-11). IEEE.
- Di Gennaro, M., De Lucia, G., **Longari, S.**, Zanero, S., & Carminati, M. (2025). *TimberStrike: Dataset Reconstruction Attack Revealing Privacy Leakage in Federated Tree-Based Systems.* 25th Privacy Enhancing Technologies Symposium (PETS 2025).
- Digregorio, G., Bleggi, F., Caroli, F., Carminati, M., Zanero, S. & **Longari, S.** (2025). *Poster: FedBlockParadox - A Framework for Simulating and Securing Decentralized Federated Learning.* SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2025).
- Mammone, D. and Bossi, L., Carminati, M., Zanero, S., & **Longari, S.** (2025). *Linux hurt itself in its confusion! Exploiting Out-of-Memory Killer for Confusion Attacks via Heuristic Manipulation.* SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2025).
- Panebianco F., and Isgrò, A., **Longari, S.**, Zanero, S., & Carminati, M. (2025). *Guessing As A Service: Large Language Models Are Not Yet Ready For Vulnerability Detection.* Joint National Conference on Cybersecurity (ITASEC & SERICS 2025).
- Balossini, M., Carminati, M., Zanero, S., & **Longari, S.** (2025). *Micro-Mobility Security: A Holistic Approach via Mobile App Analysis.* Joint National Conference on Cybersecurity (ITASEC & SERICS 2025).
- Abbasi, S.M., & **Longari, S.** (2025). *CANPak: An Intrusion Detection System against Error Frame Attacks for Controller Area Network.* Joint National Conference on Cybersecurity (ITASEC & SERICS 2025).
- Giannubilo, D., Giorgeschi, T., Carminati, M., Zanero, S., & **Longari, S.** (2025). *A Deep Learning Approach for False Data Injection Attacks Detection in Smart Water Infrastructure.* Joint National Conference on Cybersecurity (ITASEC & SERICS 2025).
- **Longari, S.**, Galletti, G, Holle, J., & Zanero, S. (2025). *CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN FD.* Joint National Conference on Cybersecurity (ITASEC & SERICS 2025).
- Amico, A., Apicella, V., Bianchini, D., Butera, A., Cesana, M., Digregorio, G., Garda, M., Gatteschi, V., Innamorati, C., Leotta, F., **Longari, S.**, Pizzo, M.R., (2025). *BOTQUAS: Blockchain-based Solutions for Trustworthy Data Sharing in Sustainable and Circular Economy.* Proceedings of the Euromicro Conference on Software Engineering and Advanced Applications (EUROMICRO-SEAA 2024).
- Cestari, R. G., **Longari, S.**, Zanero, S., & Formentin, S. (2024, December). Model Predictive Control with adaptive resilience for Denial-of-Service Attacks mitigation on a Regulated Dam. In 2024 IEEE 63rd Conference on Decision and Control (CDC).
- Digregorio, G., Cainazzo, E., **Longari, S.**, Carminati, M., & Zanero, S. (2024, June) *Evaluating the Impact of Privacy-Preserving Federated Learning on CAN Intrusion Detection.* In proceedings of the IEEE Vehicular Technology Conference Spring (VTC Spring 2024).
- Cerracchio, P., **Longari, S.**, Carminati, M., & Zanero, S. (2024, February) *Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems.* In Proceedings of the 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- Marazzi, M., **Longari, S.**, Carminati, M., & Zanero, S. (2024, February) *Securing LiDAR Communication through Watermark-based Tampering Detection.* In Proceedings of the 2024 Symposium on Vehicle Security and Privacy

(VehicleSec 2024).

- **Longari, S.**, Pozzoli, C. A., Nichelini, A., Carminati, M., & Zanero, S. (2023, June). *Candito: improving payload-based detection of attacks on controller area networks.* In International Symposium on Cyber Security, Cryptology, and Machine Learning (pp. 135-150). Cham: Springer Nature Switzerland.
- **Longari, S.**, Noseda, F., Carminati, M., & Zanero, S. (2023, June). *Evaluating the Robustness of Automotive Intrusion Detection Systems Against Evasion Attacks.* In International Symposium on Cyber Security, Cryptology, and Machine Learning (pp. 337-352). Cham: Springer Nature Switzerland.
- Avanzi, D., **Longari, S.**, Polino, M., Carminati, M., Zanchettin, Tanelli, M., & Zanero, S. (2023). *Task Aware Intrusion Detection for Industrial Robots.* In Proceedings of the Italian Conference on Cyber Security (ITASEC 2023) (pp. 1-16). CEUR.
- de Faveri Tron, A., **Longari, S.**, Carminati, M., Polino, M., & Zanero, S. (2022, November). *CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks.* In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 711-723).
- **Longari, S.**, Penco, M., Carminati, M., & Zanero, S. (2019, November). *Copycan: An error-handling protocol based intrusion detection system for controller area network.* In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy (pp. 39-50).
- **Longari, S.**, Cannizzo, A., Carminati, M., & Zanero, S. (2019, December). *A secure-by-design framework for automotive on-board network risk analysis.* In 2019 IEEE Vehicular Networking Conference (VNC) (pp. 1-8). IEEE.

Awards

- Best Paper Runner Up, Securing LiDAR Communication through Watermark-based Tampering Detection. 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- Best Paper Honorable Mention, CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks. 2022 ACM SIGSAC Conference on Computer and Communications Security.

Patents

- Sistema di controllo in tempo-reale implementato mediante computer per il controllo di un sistema o dispositivo fisico (Computer-implemented real-time control system for controlling a physical system or device), International application ref: WO2023002321A1. Numero di pubblicazione italiano: IT202100018998A1. **S. Longari**, A. Pozone, M. Tanelli, S. Zanero. Published 2023. 01. 26.
- Submitted: Verfahren zum Erkennen eines Angriffs auf einen zu sichernden Busteilnehmer, Überwachungseinheit und Bussystem (Method for detecting an attack on a to be protected bus node, monitoring system and the bus). Registration number: DE 102022207911.6. **S. Longari**, J. Holle. Registered on 01.08.2022.

Fundings

European Projects:

AHEAD: *AI-informed Holistic EVs integration Approaches for Distribution grids* *2024 — 2028*

Role: Task Leader.

SARIL: *Sustainability And Resilience for Infrastructure and Logistics networks* *2023 — 2026*

Role: Participant.

KEEPER: *Key Code based on Nanomaterials to Protect Services and Products* *2024 — 2027*

Role: Participant.

Other open calls:

SOCRATE: *Satellite Operations Cyber Range Evaluation* *2023 — 2025*

Founding source: Agenzia Spaziale Italiana
Role: Local PI.

MICS: *Made in Italy Circolare e Sostenibile* *2023 — 2025*

Founding source: PNRR
Role: Participant.

ACN Cybersecurity Ph.D. positions: *funded Ph.D. position on satellite cybersecurity* *2026 — 2028*

Founding source: Agenzia per la Cybersicurezza Nazionale

Role: Proponent.

Industrial contracts:

Satellite Cybersecurity: *development of Intrusion Detection Solutions for intra-satellite networks* *2024 — 2025*

Founding source: D-Orbit
Role: PI.

Academic Roles

Specialization Degree Coordinator:

Security Specialist *specialization degree ("Master universitario di primo livello").* *2022 — Present*

Organizers: CEFRIEL and Politecnico di Milano
Number of students: ∼20
Length: 2yrs.

Events and Conferences Organization:

OWASP Italy Day 2023 *2023*

Organizers: OWASP Italy and Politecnico di Milano

Program Committee:

- Annual Computer Security Applications Conference, **ACSAC** *2025*
- Italian conference on Cybersecurity, **ITASEC** *2024 — 2025*
- IEEE Security and Privacy Symposium, **IEEE S&P** (Subreviewer) *2023 — 2025*
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment, **DIMVA** *2024*
- Workshop on Re-design Industrial Control Systems with Security, **RICSS** (in conjunction with Euro S&P) *2023*
- Cyber-Physical System Security Workshop, **CPSS** (in conjunction with ASIACCS) *2023*
- Workshop on Automotive Cybersecurity, **ACSW** (in conjunction with EURO S&P) *2022 — 2025*
- Joint Workshop on CPS & IoT Security and Privacy, **CPSIoTSec** (in conjunction with ACM CCS) *2022*
- International Conference on Security for Information Technology and Communications, **SecITC2022** *2022*

Reviewer:

- ACM Transactions on Cyber-Physical Systems, **ACM TCPS** *2025*
- IEEE Internet of Things Journal, **IEEE IoT** *2022 — 2025*
- Elsevier Computer and Security, **COSE** *2019 — 2025*
- ACM Computing Surveys, **ACM CSUR** *2024*
- IEEE Transactions on Automation Science and Engineering, **IEEE T-ASE** *2024*
- ACM Computers and Communication Security, **ACM CCS** (Subreviewer) *2023 — 2024*
- Elsevier Journal of Parallel and Distributed Computing, **JPDC** *2024*
- IEEE Transactions on Intelligent Transportation Systems, **IEEE T-ITS** *2023*
- IEEE Transactions on Aerospace and Electronic Systems, **IEEE TAES** *2022 — 2023*
- IEEE Transactions on Dependable and Secure Computing, **IEEE TDSC** *2022*
- IEEE Transactions on Industrial Informatics, **IEEE TII** *2021 — 2022*
- IEEE Transactions on Information Forensics and Security, **IEEE T-IFS** *2021*
- IEEE Transactions on Emerging Topics in Computing, **IEEE TETC** *2018*

Other Academic Roles:

Academic Advisor for Politecnico's Carreer Service *2025 — Current*
Handle industrial stages proposed to the students of the Cyber Risk Strategy and Governance master.

Academic Cybersecurity Area Referent for MADE Competence Center *2025 — Current*
Organize the future directions of the cybersecurity area in cooperation with the industrial partners.

CPDS Member for the Cyber Risk Strategy and Governance Master *2025 — Current*
CPDS (Joint Faculty–Student Committee) addresses issues and student feedback in the Master's teaching program.

Examination Board Chair *2024 — Current*
Course: Computer Science and Engineering Master, Politecnico di Milano

Examination Board Member *2022 — Current*

Course: Computer Science and Engineering Master, Politecnico di Milano

Examination Board Member *2023 — Current*
Course: Cyber Risk Strategy and Governance Master, Bocconi and Politecnico di Milano

Speaker Engagements

Invited Talks

REDDER Level Up *2025*
Title: Il lato oscuro delle intercettazioni

- Culturstrike *2025*
  Title: Cybersecurity - AI ed il fattore umano
- REDDER Level Up *2024*
  Title: L'anello debole: l'IA punta sugli esseri umani
- Bosch Next Event *2024*
  Title: Challenges in Industrial Cybersecurity
- Hromatka Group *2023*
  Title: Risk and Industrial Security
- HackInBo *2022*
  Title: The CAN Link-Layer, or how we implemented a broken protocol, and can we fix it?
- Automotive Security Research Group *2021*
  Title: CAN Error Handling Attacks and Countermeasures
- Hardwear.io *2019*
  Title: It's easier to break than to patch: a stealthy DoS attack against CAN
- Infosek conference *2018*
  Title: Automotive Security

Paper Presentations

- Italian Conference on Cyberesecurity (ITASEC) *2025*
  Paper - CANPak: An Intrusion Detection System against Error Frame Attacks for Controller Area Network
  Paper - A Deep Learning Approach for False Data Injection Attacks Detection in Smart Water Infrastructure
- Italian Conference on Cyberesecurity (ITASEC) *2024*
  Paper - CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN FD
- Symposium on Vehicle Security and Privacy (VehicleSec) *2024*
  Paper - Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems.
  Paper - Securing LiDAR Communication through Watermark-based Tampering Detection.
- International Symposium on Cyber Security, Cryptology, and Machine Learning (CSCML) *2023*
  Paper - Candito: improving payload-based detection of attacks on controller area networks
  Paper - Evaluating the robustness of automotive intrusion detection systems against evasion attacks
- IEEE Vehicular Networking Conference (IEEE VNC) 2019
  Paper - A secure-by-design framework for automotive on-board network risk analysis
- ACM Workshop on Cyber-Physical Systems Security & Privacy (ACM CPS-SPC) 2019
  Paper - Copycan: An error-handling protocol based intrusion detection system for controller area network

Advisor Activities

Ph.D. Thesis Advisor Activities:

(co-advisor) Cyber threat identification and mitigation in the New Space Era. *Bruzzese Luigi* *2026 — Current*
Artificial intelligence for automated cyber threat detection and analysis. *Bossi Lorenzo* *2025 — Current*
On the security of e-vehicle charging infrastructure. *Balossini Marco* *2024 — Current*
Security of Cyber-Physical Systems. *Mammone Daniele* *2023 — Current*
Offensive and Defensive Cybersecurity for Critical Infrastructures. *Digregorio Gabriele* *2023 — Current*

Master Thesis Advisor Activities:

From survey to exploit: systematic security evaluation of open-source space software *Bitetto Mirko* *2025*
Comparison of satellite federated learning algorithms under data poisoning attacks *Forgia Lorenzo* *2025*
Realistic adversarial attacks against traffic sign recognition systems using stickers and graffiti *Bruzzese Luigi* *2025*
A DL Approach for FDI Attacks Detection in SWI *Giannubilo Davide & Giorgeschi Tommaso* *2025*
Exploiting Out-of-Memory Killer for Confusion Attacks via Heuristic Manipulation. *Bossi Lorenzo* *2025*
Evaluating FL Algorithms for Intrusion Detection in the Automotive Domain. *Cardani Federico* *2025*
Enhancing Security in Blockchain-based Decentralized FL. *Caroli Federico & Bleggi Francesco* *2025*
Threat Modeling of Autonomous Vehicle Security: a Case Study on the AIDA Prototype. *Boccia Giuseppe* *2024*
CANdemonium: An Evaluation Test Bed for Objective CAN IDSs Benchmarking. *Azzarà Daniele* *2024*
Implementation of a DNS Filtering System for User-Friendly Online Security. *Zuelli Arianna Luisa* *2024*
Bypassing ARM TrustZone Security: A JTAG-based Approach. *Martelli Vincenzo* *2024*
Towards Effective CAN IDS Validation: Dataset Limitations and Requirements Definition. *Porta Alessia* *2024*
Performance Evaluation of CANdito . *Marelli Giacomo* *2024*
Sandboxing in Space: A Feasibility Study on Application Sandboxing for Small Satellites. *Marra Gabriele* *2024*
Race Conditions Detection in Web Applications: An Analysis Tool. *Paratici Ilaria* *2024*
Novel attack strategies targeting PROFIbus and PROFIsafe Exploiting Error Management. *Alfonsi Alessio* *2024*
CANPak: An IDS against Stealthier Attacks for CAN. *Mehmood Abbasi Sikandar* *2024*
Meeting Proof Protocol: a Protocol for Physical Anchor Systems. *Sironi Mattia* *2024*
Empirical Security Evaluation of Digital Therapeutic Applications. *Gervasio Dario Alex* *2024*
Micro-Mobility Security: A Systematic Approach via Mobile App Analysis. *Balossini Marco* *2024*
CANtera: A novel real-world dataset on advanced CAN attacks for IDSs. *Valencic Jas* *2024*
Evaluation of Graph-based IDS Based on Outlier Detection Methods for CAN-bus. *Balalipour Pedram* *2024*
On the feasibility of Adversarial Attacks against IDSs in Automotive CAN. *Montalbano Ivan* *2024*
Location inference through social media and social relationships. *Rizzi Matteo* *2023*
Panettone: evaluating federated learning implementations of CAN IDSs. *Cainazzo Elisabetta* *2023*
A Blockchain-based framework to enhance air traffic control security using ADS-B protocol. *Saputelli Edoardo* *2023*
A Comprehensive Study of Cyber Threats and Countermeasures in Micromobility. *Rosati Nicholas* *2023*
Exploring gradient-based evasion techniques against automotive intrusion detection systems. *Cerracchio Paolo* *2023*
Towards Secure Electronic Voting : a Literature Review on E-Voting Systems and Attacks. *Barelli Riccardo* *2023*
Securing Lidar communication through watermark-based tampering detection. *Marazzi Michele* *2023*

Co-Advisor of over 20 Master Theses over the years 2018-2025

Teaching Activities

Course Instructor - Ph.D.s:

- *Advanced Research Topics In Cyber Security* *2024 — 2025*
  Politecnico & Bocconi, Computer Science and Engineering & Cyber Risk Strategy and Governance Milan, Italy
  Number of students: ∼10.
  Hours: 30/year.

Course Instructor - Masters:

- *Human and Physical aspects of Security* *2024 — Current*
  Politecnico & Bocconi, Computer Science and Engineering & Cyber Risk Strategy and Governance Milan, Italy
  Number of students: ∼60.
  Hours: 50/year.
- *Emerging Topics in Cybersecurity* *2024 — Current*
  Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
  Number of students: ∼30.
  Hours: 16/year.
- *Social Engineering* *2022 — 2024*
  Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
  Number of students: ∼30.
  Hours: 16/year.

Teaching Assistant - Masters & Bachelors:

- *Cybersecurity Technologies, Procedures and Policies* — *2023 — Present*
  Politecnico & Bocconi, Cyber Risk Strategy and Governance — Milan, Italy
  Number of students: ∼30.
  Hours: 17/year.
- *Informatica B* — *2023 — 2024*
  Politecnico di Milano, Ingegneria Energetica e Matematica — Milan, Italy
  Number of students: ∼250.
  Hours: 25/year.
- *Computer Security* — *2019 — 2023*
  Politecnico di Milano, Computer Science and Engineering — Milan, Italy
  Number of students: ∼200.
  Hours: 10/year.

Non-University Courses:

- *Cybersecurity* — *2022 — Current*
  CEFRIEL & Politecnico di Milano, "security specialist" specialization degree. — Milan, Italy
  Number of students: ∼25.
  Hours: 110/year.
- *Introduction to Industrial Cybersecurity* — *2023 — Present*
  MADE Competence Center per l'Industria 4.0 — Milan, Italy
  Various single-day instances between 2 and 8 hours.
- *Cybersecurity* — *2019 — 2022*
  POLI.DESIGN, Fundamentals of the air transport system — Milan, Italy
  Number of students: ∼20.
  Hours: ∼10/year.

Recorded Courses:

- *Introduction to Industrial Cybersecurity* — *2024*
  MADE Competence Center per l'Industria 4.0 — Milan, Italy
  4 hours of lectures on the basics of security in industrial scenarios.

Other Activities

Seminars on social engineering for WindTre — *2025 — 2026*
Interviews on social engineering for RAI — *2024 — 2026*
Consulting work for RAI Radiotelevisione Italiana — *2024*