Curriculum vitae

PERSONAL INFORMATION

Alessandro Cantelli-Forti

5, Piazza dei Martiri, Bologna (BO) – Italy

+39 347, 2651552 +39 050, 3820819

alessandro.cantelli.forti@cnit.it syd@rass.cloud

https://labrass.cnit.it/staff/alessandro-cantelli-forti/

orcid.org/0000-0002-6943-2632

Nationality Italian, United States of America

POSITION Researcher in Cybersecurity and Digital Forensics

RESEARCH VISION

His research aims to make cyber-physical systems capable of accounting for their own failures. That account is currently improvised after the event, reconstructed from records that were never designed to serve as evidence and that an adversary can now forge or degrade well enough to mislead machines and courts alike. He works to turn forensic reconstructability into a measurable design property of ships, vehicles, industrial plant and autonomous systems, specified alongside safety and availability, so that what happened to a system can be established with a confidence that is stated rather than assumed.

PROFESSIONAL AND RESEARCH EXPERIENCE

February, 2012 - to present

Researcher

National Inter-University Consortium for Telecommunications – Radar and Surveillance Systems National Laboratory (CNIT-RaSS), Pisa Activities focus on cybersecurity, digital forensics, incident management, and remediation.

Research projects – Participation in numerous national and European research programmes funded by the Italian Ministry of Defence, Ministry of Economic Development, European Commission, EDA, and ESA. Contributed to the projects *SMARP*, *HABITAT*, *ISAR-SKY*, *X-WALD*, and *INEST*. Served as major contributor or principal investigator in *SCOUT*, *SMART-AESA*, *ISS*, *iFurther*, and *THYRESIA*. – Led the activation of the cyber component of the *SCOUT* project, later selected by CORDIS as a high-impact EU-funded initiative.

Competitive funding – Involved in the preparation and management of over 30 research project proposals since 2014, resulting in 7 successfully funded projects.

NATO and EDA research coordination – Participated in the NATO AFSC Small Scale Study Project IV on “Information Assurance” (AFSC SSS-IA, 2018), which resulted in a letter of appreciation signed by NATO Chief Scientist Dr. Thomas H. Killion. Scientific and technical coordinator of two NATO Science for Peace and Security (SPS) research projects. Since 2020, appointed expert within the European Defence Agency (EDA) CapTech framework, contributing to activities in the Cyber Defence and Simulation Technologies areas.

Ministry of Defence projects – Principal investigator for cyber resilience implementation in two projects funded by the Italian Ministry of Defence: *SMART-AESA* (Leonardo S.p.A.) and *ISS – Integrated Submarine System* (DRASS S.r.l.). *SMART-AESA* addressed cyber risk management in radar systems designed for hypersonic threats; *ISS* developed resilience strategies for the full IT chain in submerged military systems.

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

Judicial technology transfer: court-appointed expert – Digital evidence expert appointed by courts and public prosecutors since October 2012, in criminal investigations involving the *Costa Concordia*, *Norman Atlantic*, *Efe Murat*, *MSC Opera*, *Costa Deliziosa*, the high-speed train accident in Parma (2021), the Audi–Porsche "Dieselgate" case, and the Mottarone cableway tragedy. The *Costa Concordia* investigation ran for four years under the direct coordination of Admiral Giuseppe Cavo Dragone, at the time Commandant of the Italian Naval Academy in Livorno and now Chair of the NATO Military Committee. Related research and expert activities have contributed to scientific publications.

Judicial technology transfer: party-appointed expert – Sole digital forensics and cyber-physical evidence consultant in the proceedings concerning the sinking of the motor yacht *Bayesian*, acting in the same capacity both in the Italian criminal proceeding and in the parallel proceedings before foreign jurisdictions. Scope covers acquisition and interpretation of on-board electronic records, navigation and automation data, and the reconstruction of the digital evidence chain across jurisdictions.

March, 2024 - September, 2026

NATO Project Director

Ai4CUAV – Innovative AI-framework to enable the Detection, Classification and Tracking of Killer-Drones

Scientific and technical coordination of the project under the NATO Science for Peace and Security Programme, NATO Partnerships and Cooperative Security Committee. Grant number: G6246 of 22 November 2023. Total budget: 350,000€

June, 2019 - September, 2022

NATO Project Director

Anti-Drones – Innovative concept to detect, recognize and track killer-drones

Scientific and technical coordination of the project under the NATO Science for Peace and Security Programme, Emerging Security Challenges Division. Grant number: G5633 of 12 June 2019. Total budget: 398,014€

June, 2023 - to present

European Defence Agency Governmental expert

Governmental expert of Cyber Defence Capability Technology Area (CapTech)

June, 2024 - to present

European Defence Agency non-governmental expert

Non-governmental expert of Simulation Technologies Area (CapTech)

September, 2020 - June, 2023

European Defence Agency non-governmental expert

Non-governmental expert of Cyber Defence Capability Technology Area (CapTech)

April - December, 2019

Horizon 2020 Scientific Coordinator

ECHO – European network of Cybersecurity centres and competence Hub for innovation and Operations

Full scientific responsibility for the work packages and tasks assigned to Link Campus University, Rome, as a project partner, and for the maritime demonstration case. Funded by the European Commission under Horizon 2020, priority H2020-EU.2.1.1 Industrial Leadership: Leadership in Enabling and Industrial Technologies, Information and Communication Technologies (ICT). Grant agreement number: 830943. Remit covered work packages 1 to 4 and 6 to 9, from cross-sector needs analysis and EU network governance models to the Federated Cyber Range, prototype integration, demonstration cases and exploitation, together with the project's international scientific networking. Four-year contract for 1,440 hours, 72,000€, held from April to December 2019.

July, 2015 – to present

Co-founder of ECHOES s.r.l

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

Co-founder of *ECHOES*, a CNIT spin-off company developing on radar systems

September, 2025 - to present

Adjunct Professor

Universita' degli Studi di Parma, Department of Mathematical, Physical and Computer Sciences. Paid private-law teaching contracts under art. 23 of Law 240/2010, awarded by public comparative selection

Security and Computer Forensics, 48 hours, 6 ECTS, INFO-01/A and IINF-05/A, M.Sc. in Computer Science and in Computer Engineering, first and second year, a.y. 2026/2027

Computer Security, module A: Digital and Network Forensics, 24 hours, 3 ECTS, INF/01 and ING-INF/05, M.Sc. in Computer Science and in Computer Engineering, first and second year, a.y. 2025/2026

May, 2026

Lecturer

Universita' degli Studi di Genova, Ph.D. Programme in Security, Risk and Vulnerability (DIBRIS)

Digital Forensics, doctoral course, 20 hours, 5 ECTS, offered to the *Security & Law* and *Cybersecurity & Reliable AI* curricula, 18–21 May 2026. Taxonomy of forensic disciplines with a focus on network, web and radio-frequency forensics; case studies from maritime environments and critical-infrastructure sensor networks; legal aspects and training for court-appointed experts in civil and criminal proceedings; international investigations, including cases before the International Criminal Court.

October, 2021 - November, 2024

Lecturer

Universita' degli Studi di Genova, Department of Informatics, Bioengineering, Robotics and Systems Engineering (DIBRIS)

Postgraduate specialisation courses delivered to Italian Armed Forces personnel at the *Joint Telecommunications School, Stelmilit* in Chiavari (GE), under the DIBRIS-Stelmilit framework agreement on Cyber Defence and Digital Forensics for 2021–2024

Network Forensics, all four editions, a.y. 2021/22, 2022/23, 2023/24 and 2024/25, 24 hours each. Traffic analysis and data detection techniques, reverse engineering of network protocols and payload reconstruction; from the third edition, incident identification, chain of custody, identification of active and passive subjects, and forensic freezing and imaging of system state

Digital Forensics, both editions, a.y. 2022/23 and 2023/24, 21 hours each. Acquisition of digital data from mass storage, identification of digital evidence sources, network traffic analysis, laboratory, and battlefield digital forensics

November, 2020

Adjunct Professor

Universita' degli Studi di Modena e Reggio Emilia

Management of the Incident Management and Remediation process, 1st-level Master in Cyber Defence Governance held at *Joint Telecommunications School, Stelmilit* in Chiavari (GE), a.y. 2020/2021

May, 2019

Lecturer

Universita' degli Studi di Modena e Reggio Emilia

Forensic Engineering: case study Cyberacademy Advanced Training Course in Cyber Security, a.y. 2018/2019

March - May, 2014

Adjunct Professor

Universita' degli Studi di Napoli «Parthenope»

Network Security 2nd-level Master, a.y. 2013/2014

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

March - May, 2013

Adjunct Professor

Universita' degli Studi di Napoli «Federico II»

Network Security 2nd-level Master, a.y. 2012/2013

April, 2016 - July, 2017

Guest Lecturer in Digital Forensics applied to industrial accidents

Guest lecturer for EMAIIF (Marine Accident Investigators' International Forum), MAIB (Marine Accident Investigation Branch, United Kingdom), and DIGIFEMA (Direzione Generale per le Investigazioni Ferroviarie e Marittime, Italy) about naval safety and information security at University of Cranfield (UK) and at Southampton UK Ministry Offices.

EDITORIAL AND PEER-REVIEW ACTIVITY

27 November, 2025 - to present

Associate Editor

IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Computer Society. Member of the Editorial Board. Handling editor for submissions in digital forensics, cyber-physical and critical-infrastructure security, and adversarial/AI-enabled attack and defence, at a sustained rate of about 3 manuscripts per month. Responsible for desk screening, reviewer recruitment, and recommendations to the Editor-in-Chief.

2024 - to present

Programme Committee member

36th USENIX Security Symposium (USENIX Security '27), Denver, CO, USA, 11–13 August 2027.

5th Workshop on Active Defense and Deception (AD&D 2026), co-located with the 31st European Symposium on Research in Computer Security (ESORICS 2026), Rome, Italy.

IEEE LCN Special Track on Maritime Communication and Security (MarCaS), IEEE Conference on Local Computer Networks: 2nd (2024), 3rd (2025) and 4th (2026) editions.

Workshop on Operating Systems and Virtualization Security (OSVS), co-located with the IEEE European Symposium on Security and Privacy: 1st edition (EuroS&P 2024, Vienna) and 2nd edition (EuroS&P 2025, Venice).

Journal reviewing

Reviewer for *IEEE Transactions on Aerospace and Electronic Systems* (IEEE), *Computers & Security* (Elsevier), *International Journal of Information Security* (Springer), *Pervasive and Mobile Computing* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *The Journal of Supercomputing* (Springer), *Journal of Marine Engineering & Technology* (Taylor & Francis), and *SoftwareX* (Elsevier).

EDUCATION AND TRAINING

October 2015 – 29 April 2019

Ph.D. Program in Information Engineering, Engineering Ph.D. School "Leonardo da Vinci"

Final grade: excellent

University of Pisa

Doctoral research project: Developing innovative cybersecurity techniques for protection of critical infrastructure

Ph.D. Thesis: Mitigation and Incident Management Methodologies for Critical Infrastructure Protection

November 2017 – October 2018

Research internship at WebLab Laboratory, Department of Engineering "Enzo Ferrari"

University of Modena and Reggio Emilia

Conducted as part of the Ph.D. scholarship

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

September 2013 **Summer School on Computer Security & Privacy, Department of Electrical and Electronic Engineering** Certificate awarded

University of Cagliari

Final Examination Building trust in the Information Age

15 July 2011 **Integrated Bachelor's/Master's Degree in Computer Science Engineering** Final grade: 97/110 (ECTS A – excellent)

University of Genoa

Final Thesis Study and analysis of a data link between subsystems of a skywave HF-OTH radar

August, 2001 **Academic Plus English Language Program** Final grade: A+

UCSD, University of California, San Diego

SOCIAL AND INTERPERSONAL SKILLS

Collaboration in heterogeneous teams across academic, research, industrial, and consulting environments, both public and private. Experience in military, ministerial, and judicial settings, including technical litigation and research related to complex national or international incidents. Engagements with stakeholders from EU countries, NATO, Eastern Europe, and the Middle East (including contexts affected by crises), applying adaptability and technical-institutional communication in regulated, organizationally and geopolitically complex environments.

ORGANISATIONAL AND MANAGERIAL SKILLS

Coordination of multidisciplinary technical and scientific teams, management of operational projects, and preparation of competitive project proposals funded at national, NATO, and European levels. Work under budget and time constraints in high-responsibility environments, including ministerial, military, and judicial domains. Oversight of academic teaching, research, consultancy, and technology transfer activities.

HONOURS AND AWARDS

2018 Letter of appreciation by NATO Chief Scientist Dr. Thomas H. Killion, for research contributions within the NATO AFSC Small Scale Study Project IV on "Information Assurance" (AFSC SSS-IA).

2024 Winner of the EDA Research, Technology, and Innovation Papers Award 2024, awarded by the European Defence Agency (EDA) at the Hub for European Defence Innovation (HEDI), Paris, 19 June 2024*.

RELEVANT PUBLICATIONS

Accepted, to appear

A. Cantelli-Forti, I. Marasco, H. Alamleh, G. Boschi, M. Colajanni, "Make the Adversary Spend More: Stateful Deception as a Cost-Exchange Primitive for AI-Era Cyber Defense", in *5th Workshop on Active Defense and Deception (AD&D)*, co-located with the 31st European Symposium on Research in Computer Security (ESORICS 2026), Rome, Italy, 18 September 2026

A. Cantelli-Forti, H. Alamleh, "SoK: The Cyber Attack Surface of Unmanned Vehicles (UxVs)", in *2026 IEEE European Symposium on Security and Privacy (EuroS&P)*, Lisbon, Portugal, 2026, doi:10.1109/EuroSP68448.2026.00031

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

V. Rushiti, E. Jajaga, A. Cantelli-Forti, B. Risteska Stojkoska, “A Scenario-Based Evaluation Framework for Drone Detection: Analysis Under Distance, Altitude, and Operational Conditions”, *IEEE Access* 14, pp. 99501–99525, 2026, doi:10.1109/ACCESS.2026.3706245

H. Alamleh, A. Cantelli-Forti, “Defending Against BLE-Based Covert Channels in Crowdsourced Location Networks”, *Computers & Security* 164, 104835, 2026, doi:10.1016/j.cose.2026.104835

A. Cantelli-Forti, G. Longo, F. Lupia, A. Merlo, E. Russo, “Towards the Automated Assessment of Cybersecurity Exercises Using Retrieval-Augmented Generation and LLMs”, in *2026 International Conference on AI x Data and Knowledge Engineering (AIxDKE)*, IEEE, 2026, doi:10.1109/AIxDKE67294.2026.00015

A. Cantelli-Forti, G. Longo, A. H. Oveis, E. Russo, “Insights from Field Experience: Digital Forensics of Event and Voyage Data Recorders in Transportation Systems Accident Investigation”, *International Journal of Information Security* 24 (4), 2025

I. Kurmashev, V. Semenyuk, A. Lupidi, D. Alyoshin, L. Kurmasheva, A. Cantelli-Forti, “Study of the Optimal YOLO Visual Detector Model for Enhancing UAV Detection and Classification in Optoelectronic Channels of Sensor Fusion Systems”, *Drones* 9 (11), 732, 2025, doi:10.3390/drones9110732

A. Cantelli-Forti, G. Longo, F. Lupia, E. Russo, “WEFT: A Consistent and Tamper-Proof Methodology for Acquisition of Automatically Verifiable Forensic Web Evidence”, *International Journal of Information Security* 24 (2), 2025

I. Habibovic, A. Almisreb, M. Hodzic, S. Turaev, A. Cantelli-Forti, “Machine Learning Algorithms and Sensor Technologies for Aging-in-Place Applications: A Review”, *IEEE Sensors Journal*, 2025, doi:10.1109/JSEN.2025.3591931

I. Marasco, A. Cantelli-Forti, M. Colajanni, “Continual Learning for Handling Maritime Data Shifts in Vessel Trajectory Prediction”, in 2025 IEEE 50th Conference on Local Computer Networks (LCN), October 2025, pp. 1–7

H. Alamleh, A. Cantelli-Forti, “Covert BLE Data Exfiltration via Apple’s Find My Network: A Malware Prototype and Defense Strategies”, in 2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), June 2025

A. H. Oveis, A. Cantelli-Forti, E. Giusti, M. Soltanpour, N. Rojhani, M. Martorella, “SHAP-Assisted Resilience Enhancement Against Adversarial Perturbations in Optical and SAR Image Classification”, *IEEE Geoscience & Remote Sensing Letters*, 2025

V. Semenyuk, I. Kurmashev, A. Lupidi, D. Alyoshin, L. Kurmasheva, A. Cantelli-Forti, “Advances in UAV Detection: Integrating Multi-Sensor Systems and AI for Enhanced Accuracy and Efficiency”, *International Journal of Critical Infrastructure Protection*, 2025

G. Longo, A. Cantelli-Forti, E. Russo, “Detecting the Unseen: Exploiting Radar–Sonar Sensor Fusion for Visual Detection of Low-Profile Naval Drones”, in *ICT Innovations 2024* (LNCS 2436), 2025

A. H. Oveis, E. Giusti, A. Cantelli-Forti, M. Martorella, “XAI-Driven Resilient Image Classification in the Presence of Adversarial Perturbations”, *IET Radar, Sonar & Navigation* 19 (1), 2025

G. Longo, A. Cantelli-Forti, E. Russo, F. Lupia, M. Strohmeier, A. Pugliese, “Collective Victim Counting in Post-Disaster Response: A Distributed, Power-Efficient Algorithm via BLE Spontaneous Networks”, *Pervasive & Mobile Computing*, 2024

A. Cantelli-Forti, G. Longo, E. Russo, “Work-in-Progress: Consistent and Tamper-Proof Acquisition of Automatically Verifiable Forensic Web Evidence”, 2024 IEEE EuroS&P Workshops (EuroS&PW), pp. 726–730, 2024

A. H. Oveis, G. Meucci, F. Mancuso, A. Cantelli-Forti, “Advancing Radar Cyber-security: Defending Against Adversarial Attacks in SAR Ship Recognition Using Explainable AI and Ensemble Learning”, 2024 IEEE 49th Conference on Local Computer Networks (LCN), pp. 1–7, 2024

A. H. Oveis, G. Meucci, F. Mancuso, F. Berizzi, A. Cantelli-Forti, “Generative AI Threats to Maritime Navigation Using Deceptive ISAR Images”, *IEEE Access*, 2024

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

V. Semenyuk, I. Kurmashev, D. Alyoshin, L. Kurmasheva, V. Serbin, A. Cantelli-Forti, "Study of the Possibility to Combine Deep-Learning Neural Networks for Recognition of Unmanned Aerial Vehicles in Optoelectronic Surveillance Channels", *Modelling* 5 (4), pp. 1773–1788, 2024

B. Ahuja, W. Matta, A. Kumar, A. Cantelli-Forti, "A Novel Data-Fusion Algorithm to Improve the Detection and Tracking of 'Killer' Drones in Urban Environment", 16th ICT Innovations Conference, 2024

V. Semenyuk, I. Kurmashev, D. Alyoshin, L. Kurmasheva, A. Cantelli-Forti, "Development of a Classification Model for UAVs and Birds Based on YOLOv9 to Improve Anti-Drone Systems", 16th ICT Innovations Conference, 2024

A. Almisreb, T. Namas, O. Buyukdagli, A. Cantelli-Forti, E. Jajaga, N. Ismail, "Utilizing Vision Large-Language Models for Automatic Image Annotations: A Comparative Study", 16th ICT Innovations Conference, 2024

A. Lupidi, F. Mancuso, G. Meucci, E. Jajaga, V. Rushiti, A. Cantelli-Forti, "Evaluating Killer-Drone Defense: NATO SPS Project 'Anti-Drones' Field Trials", 16th ICT Innovations Conference, pp. 277–291, 2024

A. H. Oveis, A. Kumar, E. Giusti, M. Martorella, A. Cantelli-Forti, "Adversarial Perturbations in Pol-ISAR Image Classification: A Study on Explanation Consistency and Ensemble Learning", 2024 International Radar Conference (RADAR), pp. 1–6, 2024

V. Semenyuk, I. Kurmashev, A. Lupidi, D. Alyoshin, L. Kurmasheva, A. Cantelli-Forti, "Developing the GoogleNet Neural Network for the Detection and Recognition of UAVs in a Data-Fusion System", *Eastern-European Journal of Enterprise Technologies* 2 (9), pp. 16–25, 2023

A. Cantelli-Forti, M. Colajanni, S. Russo, "Penetrating the Silence: Data Exfiltration in Maritime and Underwater Scenarios", 2023 IEEE 48th Conference on Local Computer Networks (LCN), pp. 1–6, 2023

G. Meucci, B. Karahoda, A. H. Oveis, F. Mancuso, E. Jajaga, A. Cantelli-Forti, "Naval Cybersecurity in the Age of AI: Deceptive ISAR Image Generation with GANs", 2023 IEEE 48th LCN, pp. 1–6, 2023

Meucci, G., Mancuso, F., Cantelli-Forti, A., AI-Generated Threats to Maritime Navigation using Deceptive ISAR Images, presented at the Hub for European Defence Innovation (HEDI), Paris, 19 June 2024.

*Awarded the EDA Research, Technology, and Innovation Papers Award 2024.

E. Jajaga, V. Rushiti, B. Ramadani, D. Pavleski, A. Cantelli-Forti, B. Stojkoska, O. Petrovska, "An Image-Based Classification Module for Data-Fusion Anti-Drone System", *International Conference on Image Analysis and Processing*, pp. 422–433, 2022

A. Lupidi, A. Cantelli-Forti, E. Jajaga, W. Matta, "An Artificial Intelligence Application for a Network of LPI-FMCW Mini-Radars to Recognize Killer Drones", *Proc. 18th Int. Conf. on Web Information Systems and Technologies (WEBIST)*, pp. 320–326, 2022

A. Cantelli-Forti, A. Capria, A. L. Saverino, F. Berizzi, D. Adami, C. Callegari, "Critical Infrastructure Protection System Design Based on the SCOUT Multitech Security System for Interconnected Space Control Ground Stations", *International Journal of Critical Infrastructure Protection* 32, 2021

A. Cantelli-Forti, M. Colajanni, "Adversarial Fingerprinting of Cyber Attacks Based on Stateful Honeypots", *Proc. Int. Conf. on Computational Science & Computational Intelligence (CSCI)*, 2019

W. Matta, A. Cantelli-Forti, "An Innovative Airport Physical-Cyber Security System (APSS)", *Information & Security* 42 (3), pp. 285–293, 2019

A. Cantelli-Forti, M. Colajanni, "Digital Forensics in Vessel Transportation Systems", *International Symposium on Foundations & Practice of Security*, pp. 354–362, 2019

A. Cantelli-Forti, "Mitigation and Incident Management Methodologies for Critical Infrastructure Protection", Doctoral Thesis, 2019, Published online by the University of Pisa.

A. Cantelli-Forti, "Use of and Issues Regarding Digital Evidence", in *Book chapter, Principles of Forensic Engineering Applied to Industrial Accidents*, pp. 345–354, 2019

© European Union, 2002-2026 | http://europass.cedefop.europa.eu

A. Cantelli-Forti, “Forensic Analysis of Industrial Critical Systems: The Costa Concordia’s Voyage Data Recorder Case”, 2018 IEEE Int. Conf. on Smart Computing (SMARTCOMP), pp. 458–463, 2018

C. Callegari, A. Cantelli-Forti, G. D’Amore, E. de la Hoz, D. E. Santamaría, I. García-Ferreira, G. López-Civera, “An Architecture for Securing Communications in Critical Infrastructure”, *DC-NET*, pp. 111–120, 2016

A. Capria, D. Petri, C. Moscardini, M. Conti, A. Cantelli-Forti, R. Massini, M. Cerretelli, S. Ledda, V. Tesi, E. Dalle Mese, “Software-Defined Multiband Array Passive Radar (SMARP) Demonstrator: A Test-and-Evaluation Perspective”, *OCEANS 2015 – Genova*, pp. 1–6, 2015

Driving licence AB (Italy); C (Texas, USA)

© European Union, 2002-2026 | http://europass.cedefop.europa.eu