Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Defending the Future: Research, Innovation and Resilience

The contribution of the SERICS Extended Partnership to national cybersecurity: Scientific achievements, new visions and solutions to the most pressing challenges.

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

SCIENTIFIC RESEARCH, SECURITY AND RESILIENCE FOR THE NATIONAL DIGITAL SYSTEM

Through education, technology transfer and the promotion of a cybersecurity culture, the SERICS Foundation works to create a more innovative, resilient and aware digital ecosystem.

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

BOOK INDEX

PREFACE

This volume is addressed to policymakers, businesses, public administrations, and all those who, in various capacities, are engaged in building a safer, fairer, and more trustworthy cyberspace.

The invitation is to consider the results presented here not as an end point, but as the beginning of a shared journey toward a digitally resilient Italy and Europe, in which security is a right for all and an enabling factor for the sustainable and inclusive development of our society.

I would like to thank the editors, the contributors, and everyone who made this project possible. May the reading of these pages inspire new paths and collaborations, and provide useful guidance for anyone wishing to take part in shaping the future of research, security, and digital freedom in Italy.

In February 2022, with the National Recovery and Resilience Plan, Italy made a far-reaching strategic choice: to invest in building a national ecosystem of excellence for cybersecurity research and innovation. This decision resulted in the creation of the Extended Partnership PE 14 - SERICS (Security and Rights in the CyberSpace), an unprecedented initiative that brought together the country's best academic, scientific, and industrial expertise around a common mission: strengthening Italy's ability to address digital security challenges in an increasingly interconnected and vulnerable world.

Extended Partnerships, promoted by the Ministry of Universities and Research (MUR) with Notice No. 341 of March 15, 2022, represent one of the most innovative tools of the PNRR for research: broad, multidisciplinary collaborations capable of leveraging complementary expertise on issues of national strategic importance. Within the overall framework, 14 priority themes have been selected, covering areas crucial to the country's sustainable development, competitiveness, and resilience: from artificial intelligence to energy, from health to telecommunications, and including cybersecurity.

SERICS stands out in this landscape for its breadth of vision and its ability to integrate the technological, legal, social, and economic dimensions of cybersecurity, transcending traditional disciplinary fragmentation. The project is not simply a research program, but a true national ecosystem: over a hundred partners, including universities, research institutions, and businesses, coordinated by the SERICS Foundation, have worked for nearly three years through a hub-and-spoke governance structure, with the hub coordinating overall activities and ten thematic spokes addressing the most pressing and complex cybersecurity challenges.

From human, social, and legal aspects to the fight against misinformation; from advanced attack and defense techniques to operating system and virtualization security; from post-quantum cryptography to the protection of critical infrastructure; from risk management to data governance in the age of artificial intelligence: SERICS has built bridges between fundamental research and practical applications, promoting a model in which the protection of infrastructure and data goes hand in hand with the protection of individual and collective freedoms.

The numbers speak volumes about the impact of this initiative: over 1,500 scientific publications in international journals and conferences, dozens of prototypes and technology platforms developed, new vulnerabilities discovered with global resonance, patents filed, spin-offs launched, and structured collaborations with leading national authorities. But what makes SERICS truly distinctive is not just the quantity of results, but their quality and, above all, the ability to translate research into concrete im-

VINCENZO LOIA

President of the SERICS Foundation

pact for the country.

This collection of contributions documents this extraordinary journey with a twofold objective. On the one hand, it clearly and rigorously highlights the scientific, technological, and operational results achieved in the various areas of intervention. On the other, it offers an integrated vision of future challenges, indicating research and application paths that can guide national policies and the strategies of institutions, businesses, and academia.

The added value of SERICS lies precisely in this holistic approach. Cybersecurity is no longer considered a purely technical issue, but a common good that encompasses fundamental rights, economic sustainability, social resilience, and national competitiveness. Each project and each result presented in this volume has been conceived as part of a broader ecosystem, designed to generate lasting value for citizens, businesses, public administrations, and institutions.

Looking to the future, the challenge will be to consolidate and expand this ecosystem, transforming it into a permanent strategic asset for the country. The threats continue: from the advent of quantum computing to generative artificial intelligence, from the protection of increasingly interconnected infrastructures to the management of digital sovereignty in a complex geopolitical context. But the solid foundation of expertise, collaborations, and results built through SERICS represents the best starting point for successfully addressing tomorrow's challenges.

This volume is aimed at policymakers, businesses, public administrations, and all those who, in various capacities, are committed to building a safer, fairer, and more reliable cyberspace. We invite you to consider the findings presented here not as a point of arrival, but as the beginning of a shared journey toward a digitally resilient Italy and Europe, where security is a right for all and an enabling factor for the sustainable and inclusive development of our society.

I thank the editors, contributors, and all those who made this project possible. May reading these pages inspire new paths and collaborations, and offer useful guidance for anyone who wants to participate in the future of research, security, and digital freedom in Italy.

INTRODUCTION

ALESSANDRO ARMANDO

Chair of the Scientific Committee

ROCCO DE NICOLA

Vice-President of the Foundation

Digital Security as a National Strategic Challenge

Increasingly sophisticated cyberattacks, large-scale disinformation campaigns, hybrid threats combining physical and digital dimensions, and a crisis of trust in critical infrastructure and communication systems: these are just some of the scenarios that test the resilience of our country and of Europe as a whole. Cybersecurity has now become a fundamental element in guaranteeing the protection of citizens' fundamental rights, the continuity of essential services, and the competitiveness of the national system in the global landscape.

Within the framework of the National Recovery and Resilience Plan (PNRR), the Ministry of University and Research announced a call for the selection of fourteen Extended Partnerships as new research policy instruments. These were conceived to overcome the fragmentation of interventions, encourage structured collaboration between universities, research bodies, and industry, and concentrate resources on major challenges of strategic relevance for the country. Cybersecurity was identified as one of these priority areas, due to its direct impact on digital sovereignty, national security, and the protection of fundamental rights.

In this context, the proposal for the establishment of the SERICS Extended Partnership was launched, coordinated by the University of Salerno at the initiative of the National Cybersecurity Laboratory of the National Interuniversity Consortium for Informatics (CINI). Leveraging a consolidated body of scientific expertise and long-standing experience in coordinating universities and research bodies, the Laboratory facilitated convergence toward a unified proposal aligned with the strategic priorities of the PNRR. The proposal, structured into ten thematic Spokes, addressed the main cybersecurity challenges in a coordinated and systemic manner, from hardware to software, from the protection of critical infrastructure to the safeguarding of digital rights, and from artificial intelligence to the social dynamics related to disinformation. Following the selection process for the fourteen Extended Partnerships, which saw the SERICS proposal approved for funding, the SERICS Foundation was established, with its headquarters at the University of Salerno.

An Ecosystem of Excellence for Cyberspace Security

The multidisciplinary and integrated approach is one of SERICS' distinguishing features: rather than responding to threats with isolated technical solutions, SERICS promotes a holistic vision of cybersecurity as a common good, capable of integrating technological, legal, economic, and social dimensions.

A key element of this openness and knowledge transfer process is represented by the Open Calls, a tool envisaged from the Partnership's design to extend the impact of SERICS beyond the perimeter of the founding partners and to foster the integration of the entire national cybersecurity research ecosystem into the project. The Open Calls made it possible to fund research and innovation projects proposed by entities outside the Partnership—universities, research bodies, startups, SMEs, and other

ecosystem actors—selected through competitive procedures based on scientific excellence, industrial relevance, and alignment with SERICS' strategic objectives.

SERICS involved over one hundred entities, including universities, public research organizations, and industrial partners, mobilizing diverse and complementary expertise across the national territory. The scale of the initiative is reflected in its numbers: dozens of research projects launched, hundreds of researchers involved, thousands of hours of specialized training delivered, and new technological platforms developed and already tested in real-world contexts. This critical mass made it possible to address cyberspace vulnerabilities systemically and to identify solutions transferable to businesses, public administrations, and citizens. The project's Spokes embody this broad and articulated vision.

Spoke 1 explored the human, social, and legal aspects of cybersecurity, recognizing that a secure digital space is first and foremost one in which fundamental rights are guaranteed and human behavior is adequately considered in the design of protection systems. Regulatory frameworks, governance models, and training tools were developed to support businesses and public administrations in compliance and in the protection of fundamental rights.

Spoke 2 addressed the challenges posed by disinformation and fake news, phenomena that erode collective trust and threaten societal informational resilience. Using an advanced technological toolkit that includes AI-based monitoring platforms, deepfake detection tools, and models for assessing source credibility, this Spoke developed an innovative SIEM for Cognitive Security, extending cybersecurity principles to the protection of the information ecosystem.

Spoke 3 focused on attacks and defenses, developing advanced techniques to detect and counter increasingly sophisticated threats. The research produced tools based on deep learning and large language models for software vulnerability detection, malware analysis, and the protection of AI systems themselves against potential manipulation. Particularly noteworthy is the development of the open-source SecML-Torch library, which has become a reference point for the international scientific community in evaluating the security of machine learning algorithms.

Spoke 4 was dedicated to operating system and virtualization security, which are fundamental to protecting cloud-native architectures and 5G networks. It developed elastic cyber ranges and digital twins of complex cyber-physical infrastructures, enabling high-impact discoveries such as vulnerabilities in the TCAS aircraft collision avoidance system, which received international recognition.

Spoke 5 addressed cryptography and distributed systems security, with particular attention to digital identity, producing innovative solutions for protection against telephone scams and developing post-quantum cryptographic schemes.

Spoke 6 tackled the gap between theoretical models and real-world implementations in software security, developing tools for the formal verification of embedded systems and for LLM-based phishing detection.

Spoke 7 focused on the protection of critical infrastructure, discovering new microarchitectural vulnerabilities in the Spectre family affecting millions of devices and developing solutions for securing cyber-physical systems in the energy, transport, and healthcare sectors.

Spoke 8 explored governance issues and developed innovative methodologies for cyber risk management, financial contagion modeling in the event of systemic attacks, and platforms for automated incident response.

Spoke 9 concentrated on developing technological and methodological solutions to ensure security, trust, and resilience in digital transformation processes, including strategic sectors such as finance, public administration, healthcare, and quantum communications.

Spoke 10 addressed challenges related to the secure and responsible management of information in an increasingly digitalized context, characterized by the widespread adoption of cloud computing and artificial intelligence. Its goal was to ensure privacy, control, and regulatory compliance throughout the data lifecycle, while balancing security and functionality.

From Research to Impact: Concrete Results for the Italian National System

The value of SERICS is measured not only by the scientific contributions produced, but above all by its ability to transform scientific discoveries into techniques and tools that enhance the resilience of the national system. SERICS has interpreted research as an instrument for impact, generating knowledge with the explicit aim of translating it into skills, tools, guidelines, entrepreneurial initiatives, and public policies.

Among the most significant results are the establishment of the CybeRights Interuniversity Research Center, a permanent structure ensuring continuity in research on the legal and social dimensions of cybersecurity, and the development of advanced platforms for monitoring online disinformation, some of which have already led to entrepreneurial initiatives such as the spin-off based on the IDA platform.

The discovery of new microarchitectural vulnerabilities in modern processors—three new attack vectors in the Spectre family—had global repercussions, affecting tens of millions of devices and prompting the release of official security bulletins by ARM, as well as the assignment of CVEs. In the critical infrastructure domain, vulnerabilities discovered in the TCAS aircraft collision avoidance system using the ARTIC cyber range were officially recognized and disclosed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

In the area of digital identity and cybercrime prevention, CallTrust represents an innovative solution to counter telephone scams based on vishing and spoofing, designed for integration into a federated model compliant with eIDAS 2.0. In cryptography, the CROSS digital signature scheme and other contributions to post-quantum cryptography have fueled international discus-

sions on the standardization of quantum-resistant algorithms.

Additional results include advanced tools for protecting microservices and implementing DevSecOps practices, methodologies for securing 5G networks and O-RAN architectures, frameworks for secure data management in distributed cloud environments, and solutions for protecting smart grids and industrial control systems.

In the field of training and awareness, innovative initiatives such as the CyberTour were implemented. This series of nine itinerant events promoted cybersecurity culture across several Italian cities, with particular attention to the needs of public administrations and small and medium-sized enterprises. To further support the dissemination of digital culture, the CybeRights Observatory provides open-access training resources, including the Legal Breviary of Cybersecurity.

The SERICS Cybersecurity Academy operated as a cross-cutting instrument for capitalizing on the expertise developed by the Spokes, with the objective of transferring specialized knowledge to professionals, public administrations, and businesses. Coordinated by the Hub and developed in close collaboration with the Spokes, which contribute both content and teaching, the Academy ensures scientific coherence and continuous updating in line with the Partnership's overall governance.

In parallel, SERICS complemented research activities with a structured technology transfer service aimed at fostering dialogue with industry and supporting the transition of innovations toward the market. Through multidisciplinary support pathways for research teams, startups, and spin-offs—integrating expertise in intellectual property, mentoring, market analysis, and business advisory—the Partnership promoted the valorization of scientific results and the dissemination of an entrepreneurial culture within the cybersecurity community.

Structured collaborations, either established or under development, with key national cybersecurity authorities—ACN, AGID, the Data Protection Authority, and AGCOM—ensure continuous dialogue between the research community and the country's operational needs, facilitating the translation of scientific results into policies and practical tools. The involvement of industrial partners in validating the developed solutions further reinforces the link between research and application.

Towards a Resilient and Inclusive Digital Future

The strength of SERICS lies in its ability to act as a value multiplier, catalyzing expertise, generating synergies, and transferring knowledge to the national system. From the creation of spin-offs and joint laboratories, to the filing of patents and the establishment of permanent research centers, the legacy of SERICS is destined to extend well beyond the duration of the initial project.

Looking ahead, the challenge will be to consolidate this collaborative ecosystem and transform it into an increasingly strategic asset for the country, capable of combining security, innovation, and rights in a constantly evolving digital world. From the advent of quantum computing to the new frontiers of generative artificial intelligence, from the protection of increasingly interconnected critical infrastructure to the management of digital sovereignty in a complex geopolitical context, challenges are numerous. The solid foundation of expertise and collaboration built through SERICS provides a strong basis for addressing them successfully.

This booklet presents a summary of the main results achieved, organized by thematic Spoke. Each section outlines the reference scenario, the challenges addressed, the main outcomes, and an in-depth focus on a particularly significant result, illustrating the concrete impact of the research activities. The aim is to offer policymakers, businesses, public administrations, and stakeholders an overview of the potential of SERICS' results, fostering dialogue and collaboration to translate research into innovation and security for Italian and European society.

In this spirit, the SERICS Foundation invites all interested stakeholders—innovative companies, public administrations committed to digital transformation, investors attentive to cybersecurity, and international partners—to join this collective journey toward a safer, fairer, and more reliable cyberspace, where technology serves people and digital security becomes both a fundamental right and a driver of the country's economic and social development.

THE FOUNDATION

The SERICS Foundation – Security and Rights in CyberSpace is a public research organization established as the implementing entity of the Extended Partnership “Cybersecurity, new technologies and protection of rights” within the framwork of PNRR (National Recovery and Resilience Plan), with the aim of promoting scientific and technological research on cybersecurity and digital rights, developing innovative strategies to address the challenges of cyberspace and strengthening the resilience of the national system.

The Foundation positions itself as the national reference platform for cybersecurity, acting as a hub for research, innovation, and education capable of integrating scientific, industrial, and educational activities.

It offers advanced training programs through the SERICS Cybersecurity Academy, implements Technology Transfer programs, supports entrepreneurship, and promotes activities aimed at spreading knowledge and awareness on cybersecurity issues. Through an academic–industrial partnership organized into 10 thematic Spokes, SERICS takes an interdisciplinary approach combining technical, legal, and social expertise to develop sustainable solutions for both institutional and industrial contexts.

Simultaneously, it carries out extensive communication and outreach activities to foster dialogue among experts, institutions, businesses, and citizens, and to build a broad base of awareness and competence nationwide.

KEY DATA:

23
PARTNERS FROM PUBLIC AND PRIVATE ENTITIES

54
PROJECTS FUNDED UNDER CASCADE CALLS

113
FUNDING (€ MILLION)

27
RESEARCH PROJECTS

43,8%
FUNDING FOR SOUTHERN ITALY

684
RESEARCHERS INVOLVED

26%
FUNDING FOR RESEARCH CALLS FOR PUBLIC ENTITIES

350
TENURED RESEARCHERS

8%
FUNDING FOR INNOVATION CALLS

134
NEW RESEARCHERS

30%
WOMEN RESEARCHERS

BOARD OF DIRECTORS

The Foundation's governance ensures a solid strategic direction and transparent, efficient operational management.

Vincenzo Loia - President
Appointed by Università degli Studi di Salerno

Marco Conti
Appointed by the General Assembly upon nomination by Consiglio Nazionale delle Ricerche (CNR)

Rocco De Nicola - Vice-President
Appointed by the General Assembly upon nomination by the Public Research Bodies and Higher Education Institutions with Special Statute serving as founding members

Giorgio Giacinto
Appointed by the General Assembly upon nomination by the Public Research Bodies and Special Statute Institutions serving as founding members

Alessandro Massa
Appointed by the General Assembly upon nomination by the private legal entities serving as founding members

Angelo Ientile
Member appointed by Ministero dell'Università e della Ricerca (MUR)

SCIENTIFIC COMMITTEE

The Scientific Committee brings together academic and public-research experts with advanced competencies in cybersecurity, digital rights, and technological innovation.

For State and Non State Universities

Alessandro Armando
Chair of the Scientific Committee
Università di Genova

Francesco Buccafurri
Università della Calabria

Danilo Caivano
Università degli Studi di Bari Aldo Moro

Michele Colajanni
Alma Mater Studiorum Università di Bologna

Stefano Di Carlo
Politecnico di Torino

Giuseppe Fenza
Università degli Studi di Salerno

Riccardo Focardi
Università Ca' Foscari Venezia

Davide Maiorca
Università degli Studi di Cagliari

Leonardo Querzoni
Sapienza Università di Roma

Pierangela Samarati
Università degli Studi di Milano

Andrea Simoncini
Università degli Studi di Firenze

For public research bodies and Higher Education Institutions with Special Statute

Giuseppe Bianchi
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)

Alessandro Biondi
Scuola Superiore Sant'Anna di Pisa

Gabriele Costa
IMT - Scuola Alti Studi di Lucca

Elena Ferrari
Consorzio Interuniversitario Nazionale per l'Informatica (CINI)

Fabio Martinelli
Consiglio Nazionale delle Ricerche (CNR)

Silvio Ranise
Fondazione Bruno Kessler (FBK)

Marina Settembre
Fondazione Ugo Bordoni (FUB)

PARTNERS

Established through the commitment of its founding members, the Foundation collaborates with numerous academic, industrial, and public institutions, forming a public–private extended partnership capable of addressing the challenges of cybersecurity.

Universities and Special-statute Institutes

Research Bodies

Companies

AUXILIARY BODIES

Advisory Board

Rocco De Nicola - Chair
Delegated by the President of the Board of Directors

Gianluca Ignagni
Chief of Staff, ACN – National Cybersecurity Agency

Giuseppe Lupoli
ARMAEREO Directorate – General Secretariat of Defence / National Armaments Directorate

Stefano Mannino
President, CASD – Centre for Higher Defence Studies / University level Institution

Agostino Santoni
Vice President, CISCO South Europe

Filippo Trifiletti
Director General, ACCREDIA – The Italian National Accreditation Body

Innovation Board

Daniele Alì
Head of Cyber Centre of Excellence, FINCANTIERI

Roberto Barbieri
Head of Global Cyber Defence & Operations, ENII

Paola Girdinio
START 4.0 Competence Centre

Luca Iuliano
Engineering Director, TELSY

Leonardo Querzoni - Presidente
CYBER 4.0 Competence Centre

Fabio Ugoste
Information Security Officer, INTESA SANPAOLO Group

Gianluca Vannuccini
Director of the Information Systems Department, Tuscany Region

10 SPOKES

10 spokes, each responsible for coordinating thematic areas that drive research and innovation across the cybersecurity landscape

SPOKE 1 — **Human, social and legal aspects**

SPOKE 2 — **Disinformation and Fake News**

SPOKE 3 — **Attacks and defenses**

SPOKE 4 — **Operating System and Virtualization Security**

SPOKE 5 — **Cryptography and Distributed Systems Security**

SPOKE 6

Software and critical infrastructure security

SPOKE 7

Critical infrastructure security

SPOKE 8

Risk Management and Governance

SPOKE 9

Securing Digital Transformation

SPOKE 10

Governance and Data Protection

Spoke

Human, social and legal aspects (CNR)

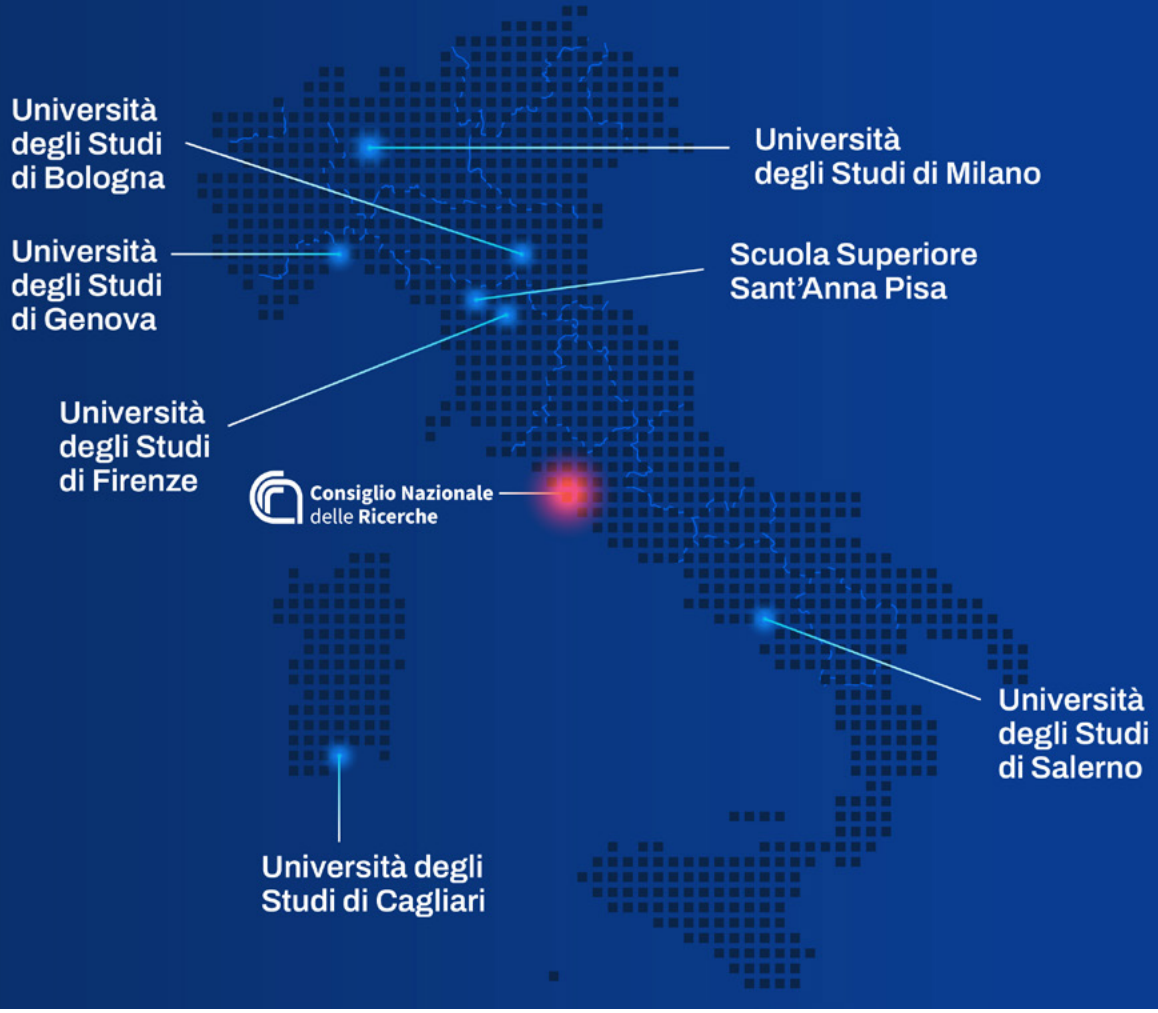
1

Coordinator

Fabio Martinelli
Consiglio Nazionale delle Ricerche

Consiglio Nazionale delle Ricerche

In the broader context of the changes affecting our society, and particularly in the area of security and the response to cyber attacks, it is essential to address the challenge of building a reliable cyberspace, combining robust technological systems with appropriate human behavior, in the belief that a safe digital space is, first and foremost, one in which everyone's fundamental rights are guaranteed. Starting from the observation that traditional security and trust measures are no longer sufficient in a context where the physical and digital worlds increasingly interpenetrate, the contribution of experts with diverse perspectives (legal, sociological, pedagogical, and technological) is particularly important for defining a holistic and interdisciplinary approach. Aiming to contribute to the implementation and evaluation of new cybersecurity policies that transcend existing measures, the research sought to strengthen the ability to predict and address the risks of a surveillance society, expanding legal frontiers in harmony with technological innovation. The projects integrated legal and technological expertise, achieving results that advance scientific progress and its ability to bring about positive changes in society. The adopted framework identifies and addresses the interconnected legal, social, ethical, and technical challenges of cybersecurity, recognizing that protecting rights in a digitalized society requires a comprehensive understanding of human vulnerabilities, regulatory frameworks, and technological capabilities.



Projects

CYBERIGHTS: Law and regulation for a better-safe Cyberspace

PI: ANDREA SIMONCINI, UNIVERSITÀ DEGLI STUDI DI FIRENZE

DiSe: Digital Sovereignty

PI: FABIO MARTINELLI, CONSIGLIO NAZIONALE DELLE RICERCHE

Spoke 1

CHALLENGES

The CybeRights: Law, Regulation, and Policy for a Better-Safe Cyberspace project addressed a series of complex challenges to build a safer and more just cyberspace. Activities focused on four key areas, representing crucial sectors of our time. The first concerns the definition of rights, rules, and taxonomies for new forms of co-regulation, capable of addressing the needs of regulatory simplification and, therefore, essential for the governance of a rapidly evolving digital ecosystem, both nationally and internationally. The second concerns the analysis of legal and ethical issues related to the protection of fundamental rights in an ever-expanding technological environment, with particular attention to the dynamics of artificial intelligence (AI), misinformation, and the evolution of digital and political rights. The third challenge was the development of learning and continuous training models on legal issues related to cybersecurity, to bridge the skills gap between legal and technology professionals, both in the public and private sectors, with particular attention to two key sectors: public administration and small and medium-sized enterprises. The fourth challenge explored criminal law and geopolitical aspects, considered crucial elements for a new national strategy for preventing and repressing cybercrime. The Digital Sovereignty (DiSe) project explored a further area, digital sovereignty, analyzing the legal and security implications of emerging digital technologies. It was supported through an Open Call by the Enforcement and Monitoring of Data Sovereignty Policies (EMDAS) project at the University of Naples Federico II.

Specifically, an initial challenge addressed was analyzing digital sovereignty regulations to help define cybersecurity requirements for technological systems. Techniques for semi-automatic policy interpretation and translation were developed, and the socio-economic aspects of data sharing were studied. Another challenge was developing digital sovereignty solutions, particularly for data protection. This work included creating models for managing trust, identity, and data use control, and collecting reliable data for secure AI in the management of cyber threats (such as malware like ransomware). A further challenge was identifying methodologies for developing secure systems capable of dynamically assessing risk levels. The aim is to ensure the confidentiality of computations in distributed environments, create secure and usable technologies, and validate solutions in the laboratory, particularly in the energy and transportation sectors.

MAIN RESULTS

The CYBERIGHTS project was led by the University of Florence in collaboration with five other universities (specifically, the University of Milan "Statale" and the Scuola Superiore Sant'Anna of Pisa, acting as WP Leaders) and the CNR (Institute of Legal Informatics and Judicial Systems, IGSG). Through the Open Call, nine other universities, brought together in the HARD-DISC project, led by the University of Roma Tre, contributed to defining the objectives and implementing the results.

The project's key results demonstrate the effectiveness of its holistic approach, with an impact that extends from the scientific community to professionals and citizens. The deliverables can be grouped into four main thematic areas:

Regulation and governance. A working matrix has been created that maps and systematizes legislation and the role assigned to institutions in protecting cyberspace, including non-European contexts. Technical reports have been produced on the transformation of international and European cybersecurity law, the application of the "security-by-design" principle to AI, and the regulation of risk and misinformation, including from a comparative perspective.

Fundamental Rights and Ethics. The project provided a conceptual framework for fundamental rights in cyberspace, producing technical reports that propose new vocabulary and practical solutions. The dynamics of e-government and e-democracy, the protection of personal data in cross-border contexts, security issues in the healthcare sector, and cyber risk management for intellectual property were analyzed. These findings contribute to a more effective understanding of rights and their dynamics, particularly with regard to the implementation of the principle of equality in a digitalized society.

Training and skills development. The project addressed the need for new professionals with multidisciplinary skills. Plans for new cybersecurity training modules were developed for public and private entities, with a specific focus on compliance for public administration and SMEs. The activation of joint observatories to assess the impact of regulations at the local and regional levels underscores the commitment to strengthening skills and providing concrete support at the territorial level.

Criminal and geopolitical aspects. A major research area has produced reports on the prevention and repression of cybercrime at the national, European, and international levels, accompanied by specific analyses dedicated to the criminological profiles of new vulnerabilities and digital investigations. Additional studies have examined the evolution of cyberwarfare concepts and the legal regime applicable to hostile operations, providing a crucial strategic framework for national security and international diplomacy.

Analysis of the CybeRights findings reveals a clear path from theoretical knowledge to practical applications with a strong focus on action and problem-solving. For example, the report on the protection of rights in healthcare and the report on cyber compliance for public administrations are not just studies, but operational guides that address real and vital issues.

This transformation of research into applicable tools is a key strength of the project. The establishment of joint observatories with national authorities and agencies (ACN, AGCOM, the Italian Data Protection Authority, and AGID) and local and regional public bodies (regions, municipalities, other universities, and research centers) represents a commitment to translating theoretical discoveries into concrete and measurable impact analyses. The project has created the necessary infrastructure for continuous analysis of regulatory dynamics and their impact. This makes CybeRights' results not only of academic interest, but also directly usable by businesses, public administrations, and policymakers.

In this regard, two particularly important results that have already

received significant attention are worth mentioning: the CybeRights Observatory and the CyberTour. The **CybeRights Observatory** provides clear and understandable information to the community on the regulations relating to certain sensitive areas of the technological innovation process. The Observatory also offers free training materials on digital culture and digital citizenship education. These include the "Legal Reference Book for Cybersecurity", a useful theoretical and practical tool for navigating the complex regulations in this area. Constructed in sections and also available in an open-access volume, the Reference Book can be a valuable aid for educational and training activities, necessary for raising awareness of the risks involved in the digital space. To ensure the rapid dissemination of cybersecurity concepts, the **CyberTour**, organized in nine one-day meetings, was launched in collaboration with the SERICS Academy. The first part, a general session, took place in the morning, followed by a special session in the afternoon, specifically dedicated to public administrations and small and medium-sized enterprises.

The Digital Sovereignty (DiSe project), led by the CNR, has achieved a series of significant results, such as:

- A study for the semi-automatic management of security policies and data protection and a comparison of cloud security policies in the EU and US.
- A social and economic analysis of data management with particular attention to cyber security in the energy sector.
- Advanced tools for collaborative and distributed analysis in a secure and privacy-respecting environment through data usage control techniques and applications in the automotive sector,
- Advanced ransomware threat detection tools through explainable AI solutions.
- Dynamic risk analysis systems and for the identification of optimal countermeasures, particularly in the energy sector.
- Methodologies for integrating IT security aspects and system quality (Quality 5.0).

Through some of these services, the cybersecurity observatory has been strengthened (**cybersecurityosservatorio.it**). Specifically, in cooperation with PID and the Start 4.0 competence center, a self-assessment service on the security posture of SMEs has been implemented, leading to the analysis of several thousand companies in Italy.

IN THE **SPOTLIGHT**

The most significant and long-term result of the CybeRights Project is the creation of the CybeRights Interuniversity Research Centre, whose activities will be divided into four main axes: research, teaching and excellent training, consultancy to the public and private sectors in the forms of technology transfer, and public engagement and dissemination.

This initiative represents a fundamental evolution, transforming a limited-term project into a permanent structure. The Center's activities will focus, from a legal, as well as economic, social, and political perspective, on topics such as the impact assessment of the NIS2 Directive, the regulation of quantum technologies, the security of space operations, and cybercrime. Its structure, modeled on the four areas of original research (regulation, rights, training, and criminal and geopolitical aspects), ensures continuity of vision and lasting impact, making the Center a strategic asset for the country and a point of reference for innovation.

This strategic move transforms the project into a value multiplier. The initiative is not a one-off, but the starting point for a collaborative platform that will continue to generate knowledge, education, and impact for years to come.

The network of academic and research excellence has been further strengthened by a strong partnership with Italian authorities and agencies (particularly through the Framework Agreement concluded with AGCOM and the close collaboration on numerous projects, starting with the development of regulatory sandboxes, with ACN) operating in the field of cybersecurity, thus ensuring constant dialogue between the research community and the concrete needs of the country's system.

Spoke 2

Disinformation and Fake News

Coordinator

Vincenzo Loia
Università degli Studi di Salerno

UNIVERSITÀ DEGLI STUDI DI SALERNO

Digital transformation and ubiquitous access to information have made society more vulnerable to misinformation and manipulation. The current communication ecosystem, dominated by instant content spread on social media, prioritizes speed over reliability. Threats involve not only fake news, but also complex cognitive manipulation techniques based on psychological biases, persuasive strategies, and recommendation algorithms. The advent of generative AI has amplified the risks, producing increasingly realistic and difficult-to-distinguish synthetic text, images, videos, and audio, fueling deepfakes, falsified evidence, and propaganda at minimal cost but with significant economic and social impacts. In addition to these phenomena, there is the coordinated use of bots, trolls, and networks of accounts that amplify messages, polarize debate, and mask the origins of organized campaigns, fostering phenomena such as astroturfing, inauthentic coordinated behavior, and artificial consensus-building. At the same time, AI and machine learning-based detection systems are also becoming the target of adversarial attacks, which undermine their reliability and open up critical scenarios for information security and institutional trust.

In this complex framework, the work of Spoke 2 lies at the intersection of technology, society, and security, with the aim of countering systemic threats that erode information resilience and collective trust.

Projects

DETERRENCE: DEcision supporT SystEm foR cybeR intelligENCE

PI: MAURIZIO TESCONI, CONSIGLIO NAZIONALE DELLE RICERCHE

FF4ALL: Detection of Deep Fake Media and Life-Long Media Authentication

PI: ROCCO DE NICOLA, SCUOLA IMT ALTI STUDI LUCCA

HUMANE: Holistic sUpports against inforMAtioN disordEr

PI: FABRIZIO SILVESTRI, SAPIENZA UNIVERSITÀ DI ROMA

IDA: Information Disorder Awareness

PI: VINCENZO LOIA, UNIVERSITÀ DEGLI STUDI DI SALERNO

Spoke 2

CHALLENGES

The Spoke 2 partners addressed the complexity of information threats, including misinformation and fake news, aiming to strengthen citizens' trust in the media and institutions. The projects shared common challenges, addressed with synergistic approaches, requiring an advanced, effective, sustainable technological and methodological ecosystem centered on expert users and decision-making processes.

A first challenge concerns the reliability of sources and the veracity of content. Automatic analysis of news, posts, and media requires models capable of distinguishing genuine narratives from orchestrated misinformation attempts. The integration of OSINT tools, semantic techniques, and explainable AI has been fundamental to building robust verification and reputation pipelines.

A second set of challenges involved modeling social dynamics in digital contexts. Polarization, account coordination, toxicity, and the role of influential users were analyzed through computational models, simulations, and observations on Twitter (now X), Telegram, and Reddit. These analyses allowed us to detect early signs of misinformation campaigns and develop methodologies not only for debunking, but also for prebunking, anticipating the impact of manipulative narratives. On the technological level, a crucial challenge has been the detection and attribution of increasingly sophisticated synthetic content (deepfakes). On the one hand, projects have pursued passive detection approaches, analyzing multimedia and audio content to establish its authenticity and distinguish genuine from manipulated content. On the other hand, a preliminary analysis was conducted to identify a specific fingerprint for each piece of content, with the aim of attributing its origin to a specific image generator or model.

Another challenge was adapting the models to new or unsupervised contexts. The use of mixture-of-, few-shot, and federated learning allowed us to explore scalable and privacy-preserving approaches in dynamic and decentralized scenarios. The heterogeneity of sources, formats, and languages required multimodal and multilingual solutions. At the same time, to address a well-known critical issue, namely algorithmic bias in generative models and recommendation systems, it was necessary to develop tools for bias auditing, assess socio-political and legal implications, and promote strategies that consider ethical and institutional dimensions. Moreover, the challenge of ensuring system transparency and robustness arose: models must deliver accurate results, make decision-making processes interpretable, and resist manipulation, generalization errors, and unexpected operating conditions, leveraging AI and explainable AI techniques.

Finally, from a monitoring and mitigation perspective, the focus was on the interaction between humans and intelligent systems. A human-in-the-loop approach was integrated to improve model accuracy and actively involve experts, journalists, decision-makers, and citizens in understanding risks and implementing countermeasures.

MAIN RESULTS

IDA – Information Disorder Awareness:

CVES (Cognitive Vulnerability Exploitation Score): A methodology for estimating in advance the risk of manipulation of real events using a dedicated indicator. A patent application has been filed for this method.

IDA (Information Disorder Awareness): A platform for monitoring and analyzing online misinformation, based on AI and data mining. It detects signs of misinformation, tracks its spread, and assesses its risk, providing interactive dashboards. It currently forms the basis of a spin-off company currently under development.

Claim Verification Tool: A prototype methodology that implements an Augmented Generation Retrieval architecture to verify the veracity of online claims in two phases: retrieval from reliable sources and subsequent confirmation or denial.

Propaganda Detection Tool: A prototype that identifies propaganda techniques in texts, using AI and explainability tools (xAI) to understand and validate model decisions.

MSCS (Multifactorial Source Credibility Score): A methodology for calculating a credibility indicator for websites by considering various factors (e.g., bias, advertising, etc.), the verification of which has shownscores consistent with expert human evaluations (e.g., NewsGuard).

Multimodal Manipulation Detection: A solution that integrates computer vision and audio forensics to identify altered content, combining pose estimation, biometric inconsistencies, and fingerprinting of synthetic content generators.

Deterrence – DEcision supporT SystEm for cybeR intelligENCE:

MERMAID: A framework based on a mixture of experts approach, in which the best-fit models are dynamically selected and emerging procedure allows to reduce the overall number of models and preserve specialization and adaptability.

Temporal Dynamics: A methodology for analyzing the dynamics of coordinated online behavior with a multilevel network. It shows that communities are often unstable, with users following fixed archetypes, and that content and structure influence membership.

Automated Detection of Online Hybrid Threats: Scalable Methodologies for Detecting Cross-Platform Information Interference and Manipulation (FIMI). Validation revealed pro-misinformation campaigns and Russian media interferences.

MIPD, Entity Framing, PolyNarrative: Multilingual and multilabel corpora for the study of misinformation, manipulative techniques, entity framing, and narratives on war and climate.

Adversarial Magnification: Super-resolution techniques used as an adversarial attack to fool deepfake detectors. Even small visual changes have a significant impact on the systems' accuracy.

Opinion Dynamics: A method for identifying configurations that generate extreme positions by analyzing polarization and the role of node centrality.

M3DUSA: A multimodal framework that combines text, images, and social structures with flexible fusion strategies. Tests on real-world datasets show superiority over traditional models.

HUMANE – Holistic supports against information disorder:

Theoretical Models. Sapienza University of Rome has studied information diffusion through opinion dynamics models, focusing on political polarization and conspiracy theories. It has also conducted analyses on hypergraphs and simplicial complexes to assess their descriptive capacity for informative and disinformative content.

Attacks and defenses. Sapienza University of Rome analyzed the vulnerability of classifiers to data poisoning attacks, showing that models widely used in the literature can be manipulated by altering the training data. A case study focused on the impact of an attack on classifiers of misogynistic comments on Reddit. In parallel, DanteLLM, a large-scale language model for Italian, was developed, representing a step towards more robust NLP systems.

The University of Milan has analyzed online information disorders and the technological tools used to detect and counter them, adopting a legal perspective with a particular focus on the healthcare and national security sectors and on balancing the rights involved, providing models and guidelines to support public institutions.

Application analyses. The CNR unit has created an NLP framework for sentiment analysis in fake news and models for studying the spread of misinformation on social media. With IMT and Sapienza University of Rome, it has contributed to automated methods for assessing the reliability of online sources. Ca' Foscari University of Venice has analyzed the impact of misinformation in various digital domains and initiated the development of corrective measures based on annotated and updated datasets.

FF4ALL – Detection of Deep Fake Media and Life-Long Media Authentication:

Public datasets. Unique datasets in size and variety have been created and released, including WILD (20,000 images from 20 generators), TrueFake (600,000 real and synthetic images), and VideoDiffusion (3,000 videos from diffusion models). These resources provide solid benchmarks for testing the robustness of the systems.

Frameworks for Deepfake Detection and Attribution. Multimodal frameworks have been developed to attribute content to source generators, leveraging visual, biometric, and acoustic features. Techniques based on 3D facial geometry, mixture of experts, and transformer architectures have improved performance in real-world, compressed scenarios.

Methods for Explainability and Robustness. Training-free methods and explainable AI solutions were introduced to make decision-making processes interpretable. Performance was evaluated against manipulation and adversarial attacks, highlighting the models' resilience and criticality.

Active Protection and Digital Signature Solutions. Fingerprinting and watermarking techniques have been proposed during the generation phase, as well as cryptographic signatures that remain valid after image cropping. Cloud and edge computing applications are also being explored, with a focus on security and interoperability.

IN THE SPOTLIGHT

A prototype platform for countering information disorder has been developed, leveraging industry standards and frameworks (STIX, DISARM, etc.) and integrating existing AI models or those developed within the spoke itself. The solution is designed as a SIEM (Security Information and Event Management) dedicated to cognitive security. Threats involve not only fake news, but also complex cognitive manipulation techniques based on psychological biases, persuasive strategies, and recommendation algorithms. The workflow allows the analyst to define topics of interest and indicators of compromise. The system processes, enriches, and aggregates observables acquired from social media and the web, and returns them in a format accessible to industry analysts. This enables interactive and intelligent monitoring of information disorder and may support businesses, institutions, and media organizations. The solution combines several innovative services: analysis of source reliability, veracity, and authenticity of textual and multimedia content; identification of coordinated campaigns; and advanced authentication and attribution modules for synthetic content, such as generated text and audio-visual deepfakes.

The added value is twofold: on the one hand, the ability to quantify and anticipate the effects of manipulative campaigns, and on the other, the ability to provide decision makers with transparent tools, based on explainable AI, to interpret complex phenomena in real time. The platform is currently being evaluated by the project's industrial partners.

Spoke
Attacks and defenses

3

Coordinator

Giorgio Giacinto
Università degli Studi di Cagliari

The increasing digitalization is leading to an expansion of the attack surface, which in turn results in a greater variety of attacks, both in terms of the techniques employed and the sequence of steps the attacker must take to achieve their ultimate objective. Attack techniques exploit various vulnerabilities, from those inherent in humans linked to the natural tendency to trust, to those inherent in physical devices, communications networks, and software due to design or implementation errors, or related to the complexity of system interactions.

The complexity of attacks varies greatly, often involving sophisticated techniques developed to conceal malicious activity to evade detection by automated security systems. The common thread linking the various attack techniques is their ability to remain invisible to both technological tools and human experts.

Artificial intelligence (AI) techniques have been an effective solution for designing systems to detect and contain cyberattacks for several years. On the one hand, there is a need to continuously update defense systems in response to evolving threats. On the other hand, AI systems that have themselves become targets of attackers must be protected and hardened.

Projects

COVERT: In searCh Of eVidence of stEalth cybeR Threats

PI: GIORGIO GIACINTO, UNIVERSITÀ DEGLI STUDI DI CAGLIARI

GERONIMO: GEneralized Real-time On-line National Internet MOnitoring Infrastructure

PI: FRANCESCO PALMIERI, UNIVERSITÀ DEGLI STUDI DI SALERNO

SOS_AI: Science and engineering Of Security of Artificial Intelligence

PI: FABIO ROLI, UNIVERSITÀ DEGLI STUDI DI GENOVA

CSS: Cyber Social Security

PI: DANILO CAIVANO, UNIVERSITÀ DEGLI STUDI BARI ALDO MORO

Spoke 3

CHALLENGES

Four projects have addressed the challenges of the reference scenario. The **COVERT** (In searCh Of eVidence of stEalth cybeR Threats) project focuses on the study and analysis of attacks that use sophisticated techniques to conceal malicious actions, exploiting the characteristics of programming languages, hiding malicious content within seemingly innocuous digital content, or modifying a program's behavior based on the execution environment. To build effective attack detection tools, AI-based approaches have been developed that enable the processing of a very large number of measurements, identifying even the faintest signs of potential malicious activity.

AI-based approaches have enabled the **GERONIMO** (GEneralized Real-time On-line National Internet Monitoring) project to develop tools for detecting anomalies, attacks, and malicious activity through network traffic analysis at various levels of granularity. The growing number of network-connected devices, which often generate anonymized and encrypted network traffic, requires a careful selection of network traffic characteristics to monitor and the development of specialized machine learning approaches.

Digital tools are creating new types of social, political, and cultural threats that require a reinterpretation of the functions of Prevention, Detection, and Response. The **CSS** (Cyber Social Security) project addresses this challenge through multidisciplinary approaches to risk management, structured along four pillars: I) technological, using AI to detect and mitigate hate speech, deepfakes, cyberbullying, cyber violence, and misinformation; II) ethical-social, balancing freedom of expression and prevention, reducing bias, and protecting vulnerable individuals; III) regulatory, considering various data and system security and protection frameworks such as GDPR, NIS2, the AI Act, and the Cybersecurity Act; and IV) operational and organizational, through governance and cooperation between experts, institutions, businesses, and civil society.

The **SOS AI** (Science and engineering Of Security of Artificial Intelligence) project addressed two open challenges in an integrated manner: re-establishing the theoretical foundations of AI for cybersecurity applications, and the security of AI-based tools and AI-enhanced systems. Indeed, the theoretical foundations of AI were not designed with applications in mind where intelligent attackers aim to intentionally subvert the learning and decision-making processes of an AI-based system, and AI risks becoming the weakest link in the cybersecurity chain. The challenge faced was to develop new algorithmic solutions and software tools for the secure design of AI-based tools.

MAIN RESULTS

The main results of the COVERT project can be summarized in the following points:

- Development of techniques based on deep learning and large language models for the detection of vulnerabilities in source code and for the analysis of other types of cyber threats such as DoS attacks, stegomalware, and malware for Android devices.
- Development of a software tool for analyzing macros within Microsoft Office documents aimed at producing a report on potential malicious actions.
- Identification of vulnerabilities in some operating systems in the implementation of main memory management using ASLR techniques.
- Formal and experimental evaluation of the robustness of tools for static binary code analysis when obfuscation and packing techniques are used and development of new specialized techniques to overcome their limitations.
- Identifying vulnerabilities in template engines used in web application development and in HTTP/3 protocol implementations that may give rise to new cyber threats.
- Development of advanced tools for Cyber Threat Intelligence through the integration of OSINT within SIEM, the development of IDS with innovative machine learning techniques, the creation of attack graphs, and the integration of unstructured information using large language models.
- Threat analysis of industrial control systems through control system modeling and network traffic analysis with machine learning techniques.

The following developments have been achieved within the GERONIMO project:

- Systems based on the federated learning paradigm aimed at correlating traffic generated by different devices for attack detection or traffic flow classification. The TinyIDS system is an IDS designed for installation on devices with low computational capacity. It is based on the TinyML distribution, which implements machine learning techniques that can be run on microcontrollers. Traffic analysis in wireless sensor networks (WSNs) has enabled the development of an epidemiological model of malware propagation.
- Moreover, several approaches based on ML and DNN, as well as on advanced feature selection techniques, have been developed for anomaly detection on time series relating to network traffic.
- A methodology to ensure confidentiality in federated learning workflows used to correlate different traffic flows, leveraging homomorphic encryption. The system was designed to be resilient to adversarial learning attacks.
- A deanonymization methodology based on correlating different flows to detect cyber threats that propagate through anonymized and encrypted traffic.

The Cyber Social Security (CSS) project has developed multidisciplinary methods and tools for managing cyber-social risk, structured along two dimensions: horizontal and vertical.

The horizontal dimension includes the following key areas:

- Cyberbullying, digital harassment through offensive messages, exclusion, or the dissemination of humiliating content.
- Cybercriminal abuse of minors through the production, dissemination, or use of materials that exploit minors or are intended for online grooming.
- Violence against intimate partners and gender-based violence through threats and harassment conveyed digitally through stalking or revenge porn or by exercising remote control, for example by geolocating the victim.

- Cyberterrorism: Adaptation of traditional terrorism to cyberspace, used for attacks, propaganda, and recruitment.
- Dissemination of hate speech and misinformation for manipulative purposes.
- Integrating physical and digital security, with insights into the physical and digital layers.
- privacy and rights, combating mass surveillance and algorithmic discrimination.

The vertical dimension is divided into three operational security units:

- Detection, to identify and predict significant social events in cyberspace.
- Response, to define new intervention and cooperation protocols.
- Prevention, to redefine incident census and mitigation processes considering new critical resources.

In the context of the SOS AI project, the results related to the challenge on "re-founding the theoretical foundations of AI for cybersecurity applications" can be summarized as follows:

- SecML-Torch software library for assessing the security of AI algorithms (https://secml-torch.readthedocs.io/) and for defending AI tools used in multimedia forensics.
- Development of methods for explaining and interpreting AI algorithms in order to evaluate their security and propose appropriate attack mitigation measures, with specific application to the detection of "Windows PE malware"
- Developing a new class of boosted tree ensembles for tabular data applications, such as medical data, that combines high performance with superior robustness, formally demonstrated and verifiable in an extremely efficient way.

Among the key findings **related to the challenge on "Security of AI-based tools and AI-enhanced systems"**:

- development of attacks against AI-based vision systems on board vehicles and their testing in real environments, and of defense and attack techniques against cyber-physical systems that use AI-based modules,
- development of technological tools for assessing the compliance of AI-based systems with the European AI Act legislation,
- Creation of the joint laboratory sAIfer Lab (Joint Lab on Safety and Security of AI, https://www.saiferlab.AI) by two partners of the SOS AI project, the Universities of Cagliari and Genoa.

IN THE SPOTLIGHT

Machine-learning and *deep learning* techniques against attacks that aim to reduce effectiveness in various application contexts. The developed techniques enable companies and public administrations to design robust and effective Artificial Intelligence systems, and contribute to building a solid core of tools for verifying the adequacy of adopted AI systems with respect to functional and regulatory requirements. The SOS AI project has systematized numerous attack scenarios both methodologically and through the creation of the open-source SecML-Torch library, which is continuously enriched with new modules thanks to contributions from the community. The library allows for the highlighting of a machine learning system's weaknesses and vulnerabilities against numerous attack scenarios and provides the designer with useful feedback for making the system robust. This result enables the design of machine learning and deep learning tools capable of detecting cyberattacks characterized by ever-increasing complexity and sophistication.

Spoke

Operating System and Virtualization Security

4

Coordinator

Alessandro Armando
Università degli Studi di Genova

Università di Genova

Cloud and virtualization technologies are profoundly transforming critical infrastructures. Platforms once managed as isolated, vertical systems are now converging into a distributed continuum that integrates computing and communication resources, orchestrated with cloud-native paradigms. The progressive fusion of computing and networking is producing flexible and scalable architectures, yet exposed to new risk areas.

A prime example is the cloudification of 5G: functions traditionally rooted in hardware are dematerialized and redistributed as microservices, seamlessly integrating the radio component with the network core. This approach enables mission-critical services, edge computing, and network slicing, creating an infrastructure fabric capable of dynamically adapting to demand.

The distributed and virtualized nature of these environments, however, brings with it unprecedented complexity. Resilience becomes a fundamental requirement: systems must continue to function even in the event of failures or targeted attacks. The integration of cloud, edge, and core radio opens up new testing scenarios, where security cannot be thought of as an afterthought, but must be natively incorporated into the application lifecycle. The ability to automate, orchestrate, and monitor heterogeneous environments in real time today represents the foundation for building the security of the critical infrastructures of the future.

Projects

SecCo: Securing Containers

PI: LUCA VERDERAME, UNIVERSITÀ DEGLI STUDI DI GENOVA

5Gsec: Security in 5G and beyond

PI: RAFFAELE BOLLA, UNIVERSITÀ DEGLI STUDI DI GENOVA

ARTIC: Affordable, Reusable and Truly Interoperable Cyber ranges

PI: ENRICO RUSSO, UNIVERSITÀ DEGLI STUDI DI GENOVA

Spoke 4

CHALLENGES

The shift to virtualized, distributed, and cloud-native infrastructures raises a multitude of interconnected challenges. One of the most significant is resilience: systems must maintain acceptable service levels even under attack or failure, ensuring operational continuity in highly dynamic scenarios. At the same time, there is a growing need to manage heterogeneous ecosystems composed of microservices, legacy components, and new cloud-native modules, each with different upgrade cycles and requirements.

The complexity of virtualization introduces specific security challenges: shared hardware resources and multi-tenant orchestration increase the potential entry points for compromise. Moreover, the attack surface extends across multiple layers, from the radio access network to the virtualized core, including edge platforms and user devices. Attackers can position themselves at different points in the network—compromised terminals, legacy components, exposed radio interfaces—exploiting the distributed nature of the network to mask malicious activity.

In this context, testing security countermeasures without interrupting operations is a difficult goal to achieve. This makes tools such as digital twins and cyber ranges crucial, capable of faithfully reproducing complex infrastructures and enabling the safe testing of attack and defense scenarios. Microservices, while enabling scalability and agility, also introduce new critical issues: their rapid lifecycle, interdependencies, and internal communications open up attack vectors that are difficult to monitor with traditional tools.

To effectively address these challenges, security must be integrated throughout the entire application lifecycle, from design and development to release and runtime. This means not limiting oneself to ex-post checks, but adopting a preventative approach, with systematic and continuous checks at every stage of the process. The DevSecOps paradigm fits this bill, translating the idea of "security by design" into operational practices: static and dynamic code checks, automatic dependency and container scanning, configuration validation against declarative policies, and, in production, continuous monitoring and rule enforcement. Through automation and constant feedback, DevSecOps reduces the window of exposure, strengthens resilience, and makes protection a native feature of cloud-native systems.

MAIN RESULTS

Results of the SECCO project

The project focused on the security of microservices and DevSecOps flows. Hardening modules were developed and integrated into the development pipelines, with the aim of introducing static and dynamic controls during the release phase. Container security policies were also defined, based on extended formal languages for expressing access and information flow control rules, and their correctness was verified using formal analysis tools.

In terms of threat detection, several innovative techniques have been developed:

A security-by-design methodology for building microservices according to the most advanced protection strategies for the application and the data it manages.

Techniques for detecting and identifying cryptojacking phenomena and large-scale resource theft campaigns.

A taxonomy of covert channels useful for designing countermeasures during runtime monitoring.

Systems for detecting anomalies in TLS 1.3 encrypted communications, integrated with Kubernetes observation tools.

Experiments were also conducted on DoS attacks against containerized microservices, transformer- and autoencoder-based models were developed for threat detection, and automation tools for edge/cloud orchestration were released, aiming to enable scalable and secure deployments.

5GSEC Project Results

The project investigated the security of 5G and next-generation networks, with findings distributed across multiple dimensions.

In the area of 5G privacy and security, the 5Gmap tool has been extended to support NSA architectures, TMSI-based attachment tests, and IMSI/IMEI exposure verification, detecting anomalies in real networks. Advanced testbeds have been developed for localization attacks, such as angular overshadowing and full-frame beaconing, leveraging FPGA hardware for high-precision simulations. At the same time, the ScasDK platform has consolidated its role in SCAS compliance testing, with recognition by national authorities.

The research explored adversarial threats in O-RAN, showing how xApps and rApps can be vulnerable to evasion, poisoning, and manipulated inputs. Runtime defenses and robustness benchmarks were developed. On the physical front, RF jamming attacks were studied and coordinated mitigation models between dApps and xApps were developed.

Significant findings also concern malware propagation in network slices: emulation testbeds have shown that defending a single slice is not enough, and that second-order dynamics can amplify instabilities if defenses are not properly calibrated.

The project also produced:

- A digital twin for secure testing of BGP configurations, tools for distributed hijacking detection, and dashboards for risk assessment at IXPs.
- Security assurance studies on 5G functions (UDM) within NESAS/SECAM.
- methodologies for selective jamming detection in IoT LoRaWAN and solutions based on intelligent gateways and virtualized infrastructures.
- Benchmark of runtime protection tools for 5G containers (Falco and commercial solutions), with extension to NFVCL orchestrators and AI models trained on realistic traffic.
- A testbed for Mission Critical Services in OTA scenarios, which also led to proposals for changes to the 3GPP standards.
- Radio prototypes to counter jamming and increase privacy, together with studies on the integration of post-quantum cryptography into O-RAN interfaces.
- Extending the Arkime platform for 5G traffic parsing and proposing a key escrow-based interception framework that balances privacy and regulatory compliance.

Results of the ARTIC project

ARTIC has developed and made available to the community an open-source cyber range framework that transcends traditional

architectures by adopting cloud-native paradigms. The framework enables the creation of elastic cyber ranges, capable of adapting to both small organizations with limited resources and large-scale exercises on complex infrastructures.

The framework's flexibility is a significant added value for training, allowing for quick and easy hands-on sessions. The project also highlighted the growing role of cyber ranges in testing technological devices and solutions, where it is essential to accurately recreate complex environments, protocols, configurations, physical processes, and sensors, including hardware components. Cyber-physical systems of considerable complexity were recreated, particularly in the maritime and avionics domains.

In the maritime sector, MaCySTe (Maritime Cyber Security Testbed) was developed and released, a specialized version of the framework that supported the development of research activities on realistic scenarios, testing new attacks, assessing resilience and proposing dedicated countermeasures.

In the avionics sector, the framework has been integrated with software-defined radio systems, enabling safe testing of subsystems that use radio frequency communications and are susceptible to wireless attacks. Specifically, it was possible to simulate the Traffic Collision Avoidance System (TCAS), an onboard system that prevents airborne collisions by providing instructions to pilots.

These results have also received concrete validation in the industrial setting, thanks to the direct use by the project's industrial partners, further strengthening the framework's relevance for testing complex cyber-physical systems.

The framework has also been used as a platform for advanced honeypots and complex sandboxes, allowing analysis of how malware or advanced persistent threats can move and propagate in a real-world architecture.

SYNERGIES BETWEEN PROJECTS

The activities of the three projects demonstrate a high degree of complementarity. The hardening and monitoring solutions developed in SECCO find natural application in the 5G environments studied in 5GSEC. The advanced threats explored in 5GSEC can be reproduced and studied in the cyber ranges and digital twins offered by ARTIC, enabling experimental validation in secure environments.

This interaction paves the way for a virtuous cycle: SECCO provides protection mechanisms that can be integrated into DevSecOps workflows, 5GSEC offers realistic and highly critical use cases in the telecommunications domain, and ARTIC provides the ability to simulate and validate scenarios in controlled environments. Together, the projects create an ecosystem capable of strengthening the security of cloud-native infrastructures and next-generation mobile networks, with a direct impact on the protection of Europe's critical infrastructures.

IN THE SPOTLIGHT

Attacks on the aircraft collision avoidance system

Using the ARTIC cyber-range, it was possible to simulate with high precision, but in a controlled environment, the functioning of the Traffic Collision Avoidance System (TCAS) and new attack techniques against it. The simulations demonstrated that a ground-based attacker, with relatively accessible instrumentation, can introduce false radar signals, making the aircraft believe there are non-existent obstacles or concealing real threats. In practice, the attacker can push the pilot into performing unnecessary or even dangerous maneuvers. This discovery, in addition to being reported by the international media, led to the official recognition of two new vulnerabilities (CVE-2024-9310 and CVE-2024-11166) by the U.S. Cybersecurity and Critical Infrastructure Security Agency (CISA) and to an improvement in the security of international air traffic control.

Spoke 5

Cryptography and Distributed Systems Security

Coordinator

Francesco Buccafurri
Università Mediterranea di Reggio Calabria

UNIVERSITÀ DELLA CALABRIA

The protection of distributed systems and the evolution of cryptography are taking place in a landscape characterized by growing complexity and rapid transformation. The need to ensure the theoretical robustness and reliability of cryptographic protocols is made more pressing by the emergence of new attack techniques and the potential impact of quantum computing, which require innovative solutions and the ability to manage the transition. Closely related, digital identity represents a crucial challenge: the secure management of authentication, traceability, and accountability raises questions of interoperability, scalability, and privacy protection, with crucial implications for infrastructures, services, and economic systems. At the same time, distributed ledger technologies and blockchain open up significant opportunities: on the one hand, they raise a number of issues related to security, efficiency, and sustainability, and on the other, they offer applications in complex contexts where transparency and verifiability are essential requirements. In this context, identification and traceability assume a strategic role, emerging as fundamental elements of the security of distributed systems and as development levers for domains of national and international importance. The overlap between theoretical approaches and applied perspectives thus becomes the foundation for building solutions capable of transforming global challenges into opportunities for innovation and strengthening digital trust.

Project

STRIDE: Project Secure and TRaceable Identities in Distributed Environments

PI: FRANCESCO BUCCAFURRI, UNIVERSITÀ MEDITERRANEA DI REGGIO CALABRIA

Spoke 5

CHALLENGES

The STRIDE (Secure and TRaceable Identities in Distributed Environments) project addressed challenges that reflect the complexity of identification and traceability, even in hybrid scenarios that intertwine physical and virtual dimensions.

A specific focus was on digital identity, considered in its various forms and analyzed in both traditional and anonymous forms. The difficulty of combining recognizability, privacy, and traceability has required the development of new solutions capable of ensuring user protection and system accountability. In this context, interest in Self-Sovereign Identity models has grown, which place the individual and the autonomous management of personal information at the center, but which raise complex questions about interoperability, sustainability, and infrastructure governance.

Another crucial challenge concerns blockchain, identification, and traceability. DLT technologies offer powerful tools for security, transparency, and decentralization, but they face challenges related to scalability, reliability of consensus mechanisms, security of smart contracts, and real applicability in industrial and national contexts. Governance and trust remain critical issues for the deployment of these technologies.

Significant attention has been paid to cryptography for authentication and access control, a field complicated by evolving attacks and the prospect of quantum computing. The development of secure and scalable protocols has been a priority, along with the challenge of combining theoretical rigor with concrete industry needs, such as secure access to financial services or the protection of critical infrastructure.

Another innovative area involved hybrid scenarios, where the virtual and physical worlds coexist. Here, the adoption of Physical Unclonable Functions appeared promising for strengthening hardware authentication systems and preventing device cloning, albeit with challenges related to reliability, cost-effectiveness, and integration with distributed architectures.

Finally, the project addressed the broader question of the role of identity in the cyber era, a context in which technological, social, and economic dimensions intertwine. Digital identification and traceability were therefore considered not just technical tools, but paradigms for interpreting the security of complex and distributed systems.

These challenges have demonstrated the need for a multi-perspective approach, based on the combination of different visions, ranging from fundamental research to real-world applications. This synergy has enabled us to transform critical scientific and operational issues into concrete results, outlining solutions that can be transferred to strategic domains, with lasting impact at the national and European levels.

MAIN RESULTS

The STRIDE (Secure and TRaceable Identities in Distributed Environments) project has produced significant results that concretely address the challenges of digital identification and traceability in distributed systems. More specifically, the results achieved by Spoke 5 synergistically address various challenges: from digital identity to advanced cryptography, from distributed authentication to hardware security, from blockchain applications to IoT protection. Some results are highly applicative and transferable, while others represent cutting-edge contributions to international research. This diversity demonstrates how Spoke 5 has successfully integrated theoretical approaches, prototypes, and concrete use cases, producing solutions with significant impact on the scientific community, industry, and institutions, and strengthening Italy's role in strategic areas of digital security.

Digital Identity and Self-Sovereign Identity (SSI).

A key aspect of the project involved testing advanced digital identity models based on Self-Sovereign Identity, developed and validated within the Spoke. The goal was to put the user at the center, allowing them to independently manage their credentials and share only the strictly necessary information, in line with European regulations and interoperability requirements. A significant achievement was the integration of this approach into the TreC Salute platform, which demonstrated how adopting SSI can strengthen trust, privacy, and usability in digital healthcare services. The research also addressed the issue of access control combined with the SSI paradigm and the revocation of verifiable credentials, proposing a new protocol based on Anonymous Hierarchical Identity-Based Encryption that allows for temporary and flexible revocation without compromising user privacy. A further contribution came from the formalization of federated authentication policies: the study showed how apparently secure systems can become vulnerable when they interact, and proposed a new SSI-based protocol to ensure consistency and security in federations.

Authentication and accountability in distributed systems.

A separate thread has addressed authentication and traceability mechanisms in communication scenarios. CallTrust is a federated system designed to counter the combination of caller ID spoofing or outbound call hijacking attacks with vishing techniques. CallTrust reduces the risk of telephone fraud, a problem of great social and economic importance, by relying on a federated trust model compliant with eIDAS 2.0.

Encryption and access control.

Spoke 5 has developed cryptographic tools and methodologies for data protection and secure access management in distributed scenarios. CryptoAC, an open-source Cryptographic Access Control prototype, demonstrates how end-to-end protection can be ensured in cloud-native microservices architectures and zero-trust scenarios, combining security and efficiency. This achievement is complemented by the design of a methodology and system for penetration testing cryptographic protocols, designed to systematically evaluate the robustness of solutions and promptly identify any vulnerabilities.

Post-quantum cryptography.

The advent of quantum computing has made it a priority to develop algorithms resistant to future attacks. CROSS, a code-based digital signature scheme that combines efficiency and security, stands out as a competitive alternative to algorithms currently being standardized. Alongside CROSS, the

Spoke partners have contributed to new primitives such as post-quantum ring signatures and MiRitH, a scheme based on the MinRank problem, expanding the range of cryptographic solutions to strengthen the resilience of digital infrastructures and fueling the international debate on the standardization of post-quantum cryptography.

PUF and hardware authentication.

In hybrid scenarios where the physical and digital worlds intertwine, an innovative approach to Physical Unclonable Functions (PUFs) based on multilevel optical techniques has been developed. These solutions exploit the intrinsic variability of materials to ensure unclonable hardware authentication mechanisms, with potential application in several practical scenarios. Research on optical PUFs is complemented by studies on quantum PUFs and lightweight implementations, paving the way for a new generation of authentication tools rooted in the physicality of devices.

Blockchain and DLT.

A graphical language has been developed to describe supply chains, from which smart contracts, interfaces, and access policies can be automatically generated, increasing traceability, transparency, and security in industrial processes. The concept of Non-Fungible Mutable Tokens (NFMTs) has also been introduced, an evolution of traditional NFTs, whose attributes can be updated in a controlled manner through attribute-based access rules: an innovative model for certifying digital and physical assets in dynamic scenarios. Spoke 5 has also contributed to blockchain interoperability protocols, a key prerequisite for the practical adoption of blockchain-based approaches, and explored the use of artificial intelligence to identify and explain vulnerabilities in smart contracts, making distributed applications more reliable and secure.

IoT security and distributed scenarios.

Protecting connected objects has been addressed with REPLIOT, a tool for automatically testing IoT devices for replay attack vulnerabilities. Thanks to its scalable and automated approach, REPLIOT allows for rapid identification of weaknesses and supports manufacturers in the development phase. This achievement is part of a broader trend of automated red-teaming tools for IoT, complemented by advanced intrusion detection and PUFs for low-cost devices, with the aim of strengthening the overall resilience of distributed systems.

IN THE **SPOTLIGHT**

Vishing-based telephone scams, often involving caller ID spoofing, are one of the most widespread forms of fraud today. Citizens are the victims, but the consequences also fall on banks, businesses, and other organizations, which face reimbursement costs, loss of trust, and reputational damage. At the same time, these organizations need to communicate via telephone with millions of users, but current systems do not offer adequate protection. The "Report on Fraudulent Payment Transactions in Italy in the Second Half of 2024," published by the Bank of Italy, shows that payer manipulation fraud is on a worrying and continuing rise.

CallTrust is an innovative solution that allows for real-time authentication of calls between users and "certified" services (banks, public administrations, insurance companies, etc.). The system relies on digital credentials published by the services themselves, which can certify the authenticity of the call. The proposed approach works on both traditional telephone networks and VoIP networks, without requiring any infrastructure modifications. A distinctive element of CallTrust is its integration into a federated model, compliant with eIDAS 2.0, which allows for interoperable implementation of protection even across borders. These features make CallTrust of interest to banks, organizations of various types, but also to governments and institutions committed to strengthening trust in digital communications.

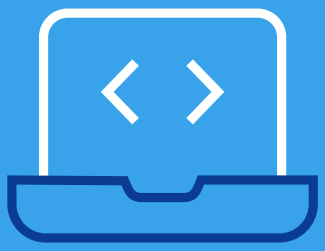
Spoke 6

Software and critical infrastructure security

Coordinator

Riccardo Focardi
Università Ca'Foscari di Venezia

Università Ca'Foscari Venezia



Digital transformation requires ensuring software and critical infrastructure security to safeguard citizen trust, business resilience, and critical services. In this context, the challenge is not only to prevent cyber attacks, but also to bridge the gap between mathematical security models and actual implementations, which often lead to vulnerabilities. Complex digital identity management systems, blockchain platforms, embedded architectures, and OT/ICS systems highlight how even formally correct software can be attacked in ways unpredicted by theoretical models. It is therefore essential to integrate formal methodologies, experimental prototypes, realistic simulations, and empirical validation to increase the security of real systems, ensuring a tangible impact on digital infrastructures and the daily use of technologies by citizens, businesses, and public administrations. This integrated approach includes automated tools, advanced policy languages, static analyzers, explainable machine learning techniques, and continuous security verification frameworks, fostering a culture of active and informed protection and helping to strengthen the trustworthiness of digital systems in critical and strategic sectors.

Projects

SCAI: Supply Chain Attack Avoidance

PI: FLAMINIA LUCCIO, UNIVERSITÀ CA'FOSCARI DI VENEZIA

SWOPS: Securing softWare frOm first PrincipleS

PI: GABRIELE COSTA, SCUOLA IMT ALTI STUDI LUCCA

Spoke 6

CHALLENGES

The challenges addressed by the Spoke 6 research projects reflect the growing complexity of contemporary digital systems and the need to ensure security, reliability, and trust in critical infrastructures, embedded devices, and distributed applications. A first fundamental challenge concerns the gap between theoretical models and real-world implementations. Formal verification tools allow mathematical proof of a system's correctness and security, but the complexity of real-world software and hardware often introduces discrepancies that can be exploited by sophisticated attackers. The challenge, therefore, is designing methods that can connect abstract models to concrete behaviors, providing reliable guarantees even in real-world operational scenarios.

Another challenge concerns data protection, including personal data related to citizens' digital identities. Ensuring that cryptographic protocols are implemented correctly and that any vulnerabilities are quickly identified requires an integrated approach, combining formal analysis, experimental testing, and collaboration with public authorities and software developers. At the same time, the increasing digitalization of industrial infrastructure and OT/ICS systems requires protecting physical facilities from cyberattacks, where even small software errors can have serious consequences for the operation of electricity grids, water systems, or production chains.

The spread of blockchain, smart contracts, and decentralized architectures introduces additional challenges. These systems require sophisticated analytics to detect non-deterministic behavior, unauthorized invocations, or cross-chain vulnerabilities, ensuring security and reliability in a context where transactions have real economic impacts.

In machine learning and artificial intelligence, challenges include both model security and explainability. Understanding how malware detection systems or automatic classification models make decisions is crucial, making the process transparent and allowing analysts to trust the results. Moreover, using federated learning techniques to detect hidden malware in mobile applications requires innovative approaches to preserve model privacy and effectiveness.

The cloud-edge and serverless infrastructure landscape present challenges related to distributed resource management, data security, and performance optimization. Defining and enforcing dynamic access policies in distributed systems is a complex problem, as complex rules must be coordinated across multiple nodes without introducing security vulnerabilities.

Finally, the rapid development of generative AI tools and the increasing automation of software testing raise new challenges in terms of model robustness, reliability, and benchmarking. All these issues require a combination of theoretical research, prototype development, and inter-university and industry collaboration, integrating multidisciplinary knowledge to address digital security holistically.

MAIN RESULTS

ALVIE: Bridging the Gap Between Models and Real Systems. ALVIE represents an innovative prototype for bridging the gap between models and real-world implementations of embedded systems. By interacting directly with the hardware, the system extracts a real-world behavioral model and analyzes it for potential threats. This approach allows for the identification of both known attacks and novel vulnerabilities, providing a systematic method for verifying and certifying the security of embedded microprocessors used, for example, in smart cities. The European CCAT project, which will begin in January 2026, will extend the use of ALVIE to new architectures, increasing its usability even for non-specialist users. A new collaboration with the Polytechnic University of Turin has been launched, again as part of the SERICS partnership, with the aim of exploring the applicability of ALVIE to cryptographic extensions of the RISC-V architecture, paving the way for next-generation formal verification for open-source architectures.

APOLLO: Phishing Detection via LLM. APOLLO is a GPT-4o-based tool for detecting phishing emails and generating explanatory messages that help users understand the risk. APOLLO integrates a pipeline of Large Language Models to produce explanations that improve user understanding and trust. In large-scale controlled studies (N = 750), the system demonstrated exceptional performance (up to 99% classification accuracy) and reduced susceptibility to phishing. The approach combines explainable AI techniques with user behavioral assessments, enabling adaptive and scalable alerts. Validation also involved collaborations with other international academic centers.

Critical OT/ICS infrastructure protection. For industrial systems and critical infrastructure, advanced PLC obfuscation frameworks have been developed, making it more difficult for attackers to understand physical processes. At the same time, distributed monitoring algorithms based on CyTL formal logic have been developed, capable of detecting anomalies and DDoS attacks, increasing the resilience and operational continuity of complex plants. These tools combine qualitative behavioral specifications with quantitative measures, such as time and data volume, to ensure both local and global critical infrastructure security.

Blockchain and smart contracts. The security of smart contracts has been significantly improved thanks to static analysis tools based on abstract interpretation, such as LiSA and GoLiSA. These tools identify non-deterministic behavior and unreliable invocations in Go contracts and decentralized applications. AlgoMove, on the other hand, allows the Move language to be used within the Algorand platform, combining Move's security properties with Algorand's versatility. These prototypes have enabled cross-chain smart contract verification, reducing the risk of fraud and unexpected behavior in public and private blockchains.

Machine learning and malware detection. Advanced approaches have been developed to improve the transparency and reliability of ML-based security models. In particular, explainability in Android malware detection systems has been improved through function call graph analysis. Comparative studies have been conducted between ML models such as GPT and BERT for vulnerability scoring, highlighting the diffe-

rences between generative capabilities and bidirectional text understanding. At the same time, federated stegomalware detection systems allow for the detection of hidden data in app icons without directly sharing sensitive data, thus complying with privacy regulations.

Performance vs. Security in Cloud-Edge and FaaS Systems. FlexiPlace enables multi-service applications to be deployed on cloud-edge infrastructures, taking into account not only functionality, but also security, node availability, latency, bandwidth, and environmental impact. WasteLess is a framework that predictively optimizes provisioning in FaaS environments, balancing cost, performance, and security, with significant savings compared to manual or self-adaptive strategies. These tools, developed within the SERICS partnership, demonstrate how, in real-world scenarios with computational constraints, a balance between resource availability and security is necessary, ensuring systems are secure yet functional and usable.

Policy and access control. The Bart, OWSM, and Strobilus languages, developed within the SERICS partnership, enable the specification of dynamic and collaborative access policies in distributed systems and microservices architectures. These tools formalize complex rules and enable their automatic enforcement, improving the security of enterprise and public infrastructures. Bart, for example, enables the controlled exchange of access to resources between multiple parties, ensuring operational correctness without human intervention.

Generative AI and testing. To increase the reliability and safety of AI systems, benchmarks have been developed for generating test inputs using generative models and search-based fuzz testing techniques. Comparative analysis of different architectures has shown that more sophisticated models produce a greater number of valid inputs, which are more susceptible to errors, especially in complex datasets. Ensuring the reliability and safety of AI systems directly contributes to making the software and platforms on which they operate more secure, strengthening the entire digital infrastructure.

IN THE SPOTLIGHT

ALVIE is an innovative prototype developed by Ca' Foscari University of Venice to verify the security of embedded systems such as the Sancus architecture. Unlike traditional formal tools, which often provide theoretical guarantees that are difficult to apply to the real world, ALVIE interacts directly with the hardware to build a concrete behavioral model of the system. By analyzing this model according to defined threat scenarios, ALVIE is able to identify known attacks and new vulnerabilities, while also producing a precise estimate of the system's security probability. The prototype was selected for the European CCAT project, with the goal of extending its use to various embedded architectures and making it accessible to non-experts. In collaboration with the Polytechnic University of Turin, again as part of the SERICS partnership, we are studying how ALVIE can be applied to the security of cryptographic extensions to the RISC-V architecture, demonstrating how advanced analysis tools can effectively bridge the gap between theory and real-world implementation, increasing confidence in the security of software and devices.

Spoke
Critical infrastructure security

7

Coordinator

Stefano Di Carlo
Politecnico di Torino

Politecnico di Torino

Critical infrastructures are the beating heart of modern society: electricity and gas distribution, water networks, transportation, healthcare, and telecommunications are essential services without which daily life and the economy could not function. Their increasing digitalization, driven by the adoption of IoT technologies, edge computing, and artificial intelligence (AI)-based systems, has improved efficiency and control, but at the cost of significantly increasing the attack surface. In this context, security cannot be limited to data protection alone; it must also ensure service continuity and operational resilience, essential elements for infrastructures that must function without interruption. This tension requires an effort to address new issues: complex, distributed, and highly interconnected systems, including legacy devices that are difficult to upgrade, coexist with next-generation technologies. The simultaneous presence of Information Technology (IT) components, i.e., traditional IT systems, Operational Technology (OT), i.e., industrial control and automation systems, and the Internet of Things (IoT), exposes critical infrastructures to advanced and persistent threats, capable of compromising not only the availability of services but also the physical safety of people. Moreover, the geopolitical and strategic dimension of cyberattacks on critical infrastructures makes protecting these systems a national and European priority.

In this scenario, research plays a fundamental role in analyzing specific vulnerabilities, developing innovative tools for the prevention, detection, and response to attacks, and defining methodologies that strengthen the trust and reliability of digital technologies in the most sensitive contexts for society.

Projects

SANDSTORM: Secure AND Safe infrasTructures fOR cps in the compute continuuM

PI: ERNESTO SANCHEZ, POLITECNICO DI TORINO

SCAR: Securing the third millennium's cyber-CARs

PI: ILARIA MATTEUCCI, CONSIGLIO NAZIONALE DELLE RICERCHE

SCS: Smart-Grid Cyber-physical Security

PI: MARIO MARCHESE, UNIVERSITÀ DEGLI STUDI DI GENOVA

Eraclito

PI: NICOLÒ MAUNERO, CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA

Spoke 7

CHALLENGES

Spoke 7 projects addressed a diverse set of challenges arising from the complex, interconnected, and often legacy nature of critical infrastructure. These include:

Protecting Heterogeneous Systems: The coexistence of Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT) components requires integrated security approaches that take into account both computing networks and field devices, which are often constrained by limited resources.

Advanced Persistent Threat (APT) Management: Attacks targeting critical infrastructures are increasingly targeted and sophisticated, capable of exploiting multiple vulnerabilities along the supply chain. It has been necessary to develop early detection techniques, featuring the use of AI and machine learning.

Resilience and business continuity: Unlike other IT domains, a disruption in critical services can have immediate consequences for citizens and businesses. The challenge has been to design defense strategies that preserve operations even in the event of a partial compromise.

Compatibility with legacy systems: Many plants operate with technologies that are either non-upgradable or lack security patches. Projects had to identify solutions that do not require invasive interventions, favoring non-intrusive monitoring techniques.

AImodels: The integration of intelligent algorithms for anomaly detection raises questions about their robustness to hardware failures and adversarial attacks. It was therefore necessary to develop specific validation and testing methodologies for critical environments.

Automotive Security: Modern vehicles, increasingly connected and autonomous, are themselves critical mobile infrastructure. Projects addressed the protection of electronic architectures and automotive software from attacks that could compromise road safety and user trust.

Hardware security: Long considered a secondary concern, protection at the microarchitectural and physical device levels is now crucial. Approaches have been explored to detect hardware vulnerabilities, develop countermeasures against malicious failures, and ensure the integrity of the computing platform.

Coordinated incident response: Given the distributed nature of infrastructure, it is essential to have mechanisms for sharing information and orchestrating interventions, including among various public and private stakeholders.

Regulatory compliance and governance: the developed solutions must comply with national and European regulations (e.g. NIS2), harmonizing legal requirements with technical needs.

These challenges guided the definition of the methodologies and tools developed in the projects, which range from proactive monitoring to automated response, from cyber resilience analysis to the training of specialized operators, thus paving the way for the concrete results that follow.

MAIN RESULTS

The results obtained from the projects are presented here, organised by initiative and, within each project, by the main sub-themes addressed.

SANDSTORM Project

The project's primary objective is to create an open and secure computing architecture based on the RISC-V processor, covering the entire stack—from hardware to AI frameworks and design tools. SANDSTORM represents a first step toward Italian technological independence from closed foreign solutions, in line with the European Processor Initiative (EPI) and the ambition of making Italy a leading player in the future RISC-V market. The project's main results were:

Hardware architecture and security: A CVA6 RISC-V CPU was enhanced with a cryptographic accelerator capable of performing high-speed 64-bit cryptographic operations. In parallel, a methodology for verifying RTL-level side-channel attacks was proposed and validated with FPGA measurements.

Microarchitectural vulnerabilities: Three new attack vectors have been discovered in the Spectre family that exploit poorly documented hardware mechanisms. These discoveries have already led to an industry-wide vulnerability report (CVE-2024-10929) and will impact tens of millions of devices, including the new AMD/Xilinx Versal chips.

Mixed-criticality systems: Methods have been proposed to ensure the isolation of hardware accelerators in heterogeneous RISC-V-based embedded systems, including mechanisms to isolate bus transactions initiated by accelerators on FPGA-SoCs.

AI robustness: A standardized taxonomy and benchmark for Adversarial Pruning (AP) techniques has been designed and made publicly available for robust and reproducible evaluations.

SCAR Project

The project addresses cybersecurity in road vehicles, considering hardware, software, social, and regulatory aspects. The goal is to strengthen both intra-vehicular (internal networks such as the CAN bus) and extra-vehicular (V2X communications with transport infrastructure) security.The main results of this project were:

Intrusion Detection Systems (IDS): Development of hardware IDS to recognize attacks on the CAN intra-vehicular network and software anomaly detection systems on ROS.

V2X Authentication Protocol: A multi-factor, multi-channel authentication (MFA) protocol for V2X communications has been designed and formally verified, based on challenge-response and the use of a physical channel for authentication. The protocol has been implemented and road-tested, and its potential for transfer to the industrial sector is already being evaluated.

Threat intelligence: An innovative cyber threat intelligence approach has been developed that leverages generative AI models to analyze large amounts of social media data. The goal is to early identify trends, potential threats, and malicious activity that could impact the automotive industry.

Zero Trust Software Defined Vehicle (ZT-SDV): A new paradigm has been conceptualized that applies the "never trust, always verify" principle to software-defined vehicles, treating every component as untrusted until proven otherwise. The approach combines TEEs, virtualization, containerization, cryptographic attestations, and micro-segmentation, enabling the secure installation of third-party apps and the verifiable execution of dynamic software modules via WebAssembly (WASM) on ARM TrustZone.

Eraclito Project

The project aims to innovate the cyber risk assessment process by moving beyond manual and fragmented approaches and introducing advanced tools and models to automate correlations, identify risks, and assess technological, organizational, and legal impacts. The project's main results were:

Risk Ontology Model: Developing a model to represent and integrate information about users, infrastructure, and impacts, enabling customized multidimensional views for different stakeholders.

Linking technological risks and legal impacts: The correlation between cybersecurity principles (confidentiality, integrity, availability) and the consequences for individuals' fundamental rights.

AI- and ontology-based prototyping tools: Development of tools that leverage inferential rules and LLMs to automate crucial phases such as threat modeling, threat and countermeasure correlation, and vulnerability cataloging. This enables adaptive and dynamic cybersecurity strategies.

SCS Project

The SCS project addresses the cyber and physical security of smart grids, with a particular focus on energy communities and distributed storage systems. The goal is to ensure accurate monitoring and resilience of energy infrastructure against cyber threats and operational anomalies. The main results of this project were:

Anomaly detection algorithm: Development of a method based on autoencoders and physics-informed neural networks that integrates physical laws into AI models, enabling more reliable monitoring of distributed energy resources.

BESS-Set Dataset: Creation of a dataset for the cybersecurity of battery storage systems, already published and made available to the scientific and industrial community.

IEC 62443 Framework: Defining a secure-by-design approach for energy communities, compliant with international industrial security standards.

Industrial Monitoring Tools: Developing a framework for deploying cybersecurity tools in industrial environments.

Attack Impact Analysis: Evaluating the consequences of cyberattacks against energy communities, distribution networks, and electric vehicle charging stations, highlighting vulnerabilities and mitigation strategies.

IN THE **SPOTLIGHT**

One of the most significant findings concerns the discovery of new microarchitectural vulnerabilities in modern microprocessors, related to branch prediction management. The study, conducted by the Scuola Superiore Sant'Anna as part of the SANDSTORM project, showed that little-documented hardware mechanisms, introduced to improve microprocessor performance (such as Bias-Free Branch Prediction and Branch History Speculation), can be exploited to build new Spectre-family attacks capable of bypassing currently standard defenses. The researchers identified three new attack vectors—BiasScope, Spectre-BSE, and Spectre-BHS—and built a practical demonstrator (Chimera) that, using Spectre-BHS, was able to extract data from the Linux kernel at speeds exceeding 24 kbit/s, even with all mitigations active. The impact of this discovery is enormous: several processor families and tens of millions of devices are affected. To understand the impact of this discovery, all new AMD/Xilinx Versal chips are vulnerable. ARM has already released an official security bulletin for Spectre-BSE and BiasScope, distributed patches for the Linux kernel, and assigned the vulnerability CVE-2024-10929. Although ARM has assessed the risk of exploitation as low, the research has demonstrated the possibility of executing complete and functional attacks capable of compromising a real system. Moreover, an additional CVE is being released for Spectre-BHS and Chimera, demonstrating the significance of the discovery. This result highlights how hardware security, long underestimated, is now a key aspect of protecting critical infrastructure and digital services. At the same time, it provides the scientific community and manufacturers with valuable insights for strengthening the resilience of computing platforms, significantly improving the level of protection for the European digital ecosystem.

Spoke
Risk Management and Governance

8

Coordinator

Michele Colajanni
Alma Master Studiorum -
Università di Bologna

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Digital transformation has led to the development of increasingly complex ecosystems, in which multiple digital elements, interacting with cyber-physical systems, support operations of productive and civil services across all states. The adoption of increasingly sophisticated technologies, from cloud to edge computing and artificial intelligence (AI), opens new opportunities but also generates growing cyber risks.

As digital ecosystems are not isolated, a cyber attack can produce cascading effects on the industrial, financial, and social levels, triggering systemic risks that call into question the overall resilience of contemporary societies. In this context, cybersecurity is no longer just about the technical protection of systems but is becoming a topic that encompasses the entire spectrum of policies, regulation, fundamental rights, and global economic relations. It is therefore important to address these challenges and develop risk analysis tools and prevention models to strengthen the safe development of systems, propose quantitative risk management methodologies in critical sectors, and explore the impact of European cybersecurity policies, aiming to develop new cyber risk management skills for citizens, technicians, and legal and political experts.

Projects

EcoCyber: Risk management for future cyber-physical ecosystems

PI: MICHELE COLAJANNI, ALMA MASTER STUDIORUM - UNIVERSITÀ DI BOLOGNA

PROTECT-IT: imPROving The rEsilience to Cyberattacks of distributed ICT InfrastrucTures

PI: ANTONIO LIOY, POLITECNICO DI TORINO

Spoke 8

CHALLENGES

The complexity of the current scenario poses numerous challenges, at technical, managerial and/or regulatory levels.

Predict and model emerging threats. The system design phase must include tools to anticipate potential attacks. Extensions to existing frameworks, enriched with attack patterns and adversary profiles, allow for the simulation of attack paths and attacker success probabilities, providing a scientific basis for comparing architectural security and identifying critical vulnerabilities.

Manage systemic and financial risks. A cyber-attack does not just target a single node; it can spread across interbank networks or industrial chains, amplifying the damage. Cyber risk contagion models that integrate economic and digital dimensions are needed, along with mitigation strategies that combine financial and insurance tools, optimal allocation of security investments, and innovative defense approaches, such as cyber-deception, zero-trust, and reinforcement learning applied to stability controls.

Protecting Industry 4.0 and automation systems. Industrial Automation Control Systems are at the heart of digital transformation, yet remain exposed to critical vulnerabilities. The challenge is to integrate risk assessment methodologies compliant with international standards, including the involvement of asset owners, managing increasing complexity, and adopting tailored countermeasures, as demonstrated by the case study of a gas turbine plant.

Developing resilient technologies for IoT systems. The proliferation of embedded and IoT devices requires real-time monitoring, anomaly detection, and defense against advanced attacks. There is a need to develop hardware-software stacks based on open architectures, integrating remote attestation, intrusion detection, and experimental datasets. A key challenge remains the secure orchestration of network services, through the integration of previously separate SDN virtualization paradigms.

Integrating law, politics and society. European regulations (e.g., the Cyber Resilience Act, NIS2) redefine the roles and responsibilities of businesses and institutions. This creates tensions between national security, the single market, and the protection of civil rights that must be addressed at the technical, legal, and political levels.

Spread awareness and inclusion. A crucial challenge is also cultural: there is a need to raise citizen awareness, develop digital skills, and promote gender balance in technology careers. Only an integrated approach can ensure a truly resilient and democratic cyber-physical ecosystem.

MAIN RESULTS

Ecocyber project has produced significant results on three complementary levels—technical, modeling, and regulatory—which together contribute to strengthening the security of digital and cyber-physical ecosystems. The project began with the risks and security of individual components, developing and testing monitoring and anomaly detection strategies for embedded and IoT systems. It conducted experimental campaigns, produced datasets and software, and developed a new model to ensure the secure orchestration of networked services through the integration of advanced management techniques, previously confined to separate domains (SDN, Data Plane Programmability, Choreographic Programming). A stack was also developed for an architecture capable of ensuring the integrity and confined execution of code, based on open RISC-V components, OpenTitan, remote attestation techniques, and the development of new elements for the Linux kernel. Techniques for real-time detection of malicious instructions on RISC-V processors and for analyzing the reliability of Physical Unclonable Functions in the presence of faults and environmental stress were validated. Formal verification methods have been extended to data-intensive distributed systems.

The project then focused on integrated system components. In the field of Industrial Automation Control Systems, a risk assessment methodology aligned with the ISA/IEC 62443 ZCR 5 standard was proposed, integrating complexity management, specific countermeasures, asset owner involvement, and support tools. Its effectiveness was demonstrated through a case study on a gas turbine power plant. Research was also conducted on a hybrid cyber-robust machine learning architecture, with the aim of evaluating the efficiency of neural network models for supervised and unsupervised learning that are interpretable and robust against adversarial risks, using statistical and quantum mechanics methods. Innovative methodologies were developed to assess and strengthen cybersecurity in critical domains. Digital twin models were applied to industrial infrastructures and quantitative models were used to detect cyber risks and analyze human barriers in incident response. In critical systems, resilient machine learning-based classifiers were designed with output rejection strategies to avoid unsafe decisions. Innovative zero-trust and machine learning models and methods were proposed for the Industrial IoT sector, as well as innovative deception models based on digital twins. In the smart city domain, blockchain-based frameworks were tested for secure monitoring and performance evaluation of smart contracts in safety-critical IoT scenarios. In the modeling component,an extension of the ADVISE Meta framework was proposed by applying it to a public transportation supervision system. This extension allowed for assessing adversary success probabilities and attack paths, by conducting sensitivity analyses, comparing architectures, and identifying vulnerable components. Finally, cyber and financial risk contagion models were presented, along with mitigation strategies that include financial instruments designed to strengthen systemic stability; optimal allocation of cybersecurity investments across network nodes, leveraging cyber-deception and security game theory; and financial control mechanisms based on reinforcement learning.

The EcoCyber project also addressed cyber risks in the legal and political fields, producing significant results in the evaluation and application of European regulatory frameworks for cyber risk management and their impact on global standards and policies, economic relations, and the relationships

between cybersecurity, national security, and surveillance.It also led to the creation of the EU Cyber Resilience Act Interactive Guide, which provides guidance on how this law will operate in practice for economic operators, legal advisors, and technical experts. Finally, the risks associated with data management by law enforcement agencies were explored in depth, highlighting the tensions between security, privacy, and civil rights. Ecocyber project members have organized and collaborated on numerous cybersecurity awareness and digital education initiatives, including those focusing on gender balance.

PROTECT-IT project studied Internet threats by combining a distributed sensor network with AI techniques, automatic defense configuration, and real-time attack detection. An infrastructure was built to collect and share data on suspicious traffic observed by network telescopes and honeypots, developing machine learning methods capable of recognizing hidden patterns, transferring knowledge between networks, capturing the temporal evolution of phenomena, and integrating heterogeneous information. These approaches were used to identify anomalous activity and new threats and to build more explainable and transparent models, while highlighting the limitations and risks of unreliable shortcuts. The distributed platform is now open to other partners who host collection nodes and use the data to develop and test algorithms. Two protection services were developed on this network: REACT-VEREFOO, an automatic reaction mechanism that reconfigures firewalls to block attacks while maintaining essential services, with high guarantees of correctness and speed; and a system for identifying attacks on network nodes in real time (based on root-of-trust for x86 and RISC-V platforms). Generates periodic reports on the software status of nodes, analyzed by an external Verifier, to detect changes or unauthorized software and respond (e.g., node isolation).

IN THE **SPOTLIGHT**

The project developed a platform capable of identifying new types of cyber risks, responding reliably and automatically, and ensuring that network infrastructures are not compromised by malicious software. For the observation phase, a distributed infrastructure was built to collect and share data on suspicious traffic observed by network telescopes and honeypots, increasing visibility into malicious activity originating from cyberspace. Based on this data,AI algorithms were developed to recognize hidden patterns, transfer knowledge between different networks, capture the temporal evolution of attacks, and integrate heterogeneous sources. These techniques enabled the identification of anomalous activity and new threats, with a particular focus on explainable and transparent patterns. At the same time, it was demonstrated that the use of AI should be approached with caution, as models can sometimes rely on unreliable shortcuts. For the reaction phase, an autonomous defense mechanism was designed and implemented that can dynamically reconfigure network firewalls in response to attacks, also thanks to cyber deception initiatives basedonSDN and digital twins. At the same time, a root-of-trust system has been developed that allows for real-time monitoring of the integrity of software running on network nodes. This component is crucial to preventing an attacker from directly compromising routers or other network devices to circumvent the countermeasures in place.

Spoke
Securing Digital Transformation

9

Coordinator

Leonardo Querzoni
Sapienza Università di Roma

The digital transformation of processes across all levels of modern society brings great opportunities, but it also entails risks that may undermine the trust, resilience, and sustainability of digital products and services. In this context, security cannot be seen merely as a technical constraint, but rather as an essential enabling condition for effective, reliable and interoperable digital solutions.

The current landscape presents diverse challenges. In the financial sector, the growing use of Distributed Ledger Technologies (DLTs) and smart contracts opens up more transparent markets while exposing them to the risks of manipulation, scalability, and fraud. As public administration processes digitalize, data protection and secure identity management are becoming crucial to safeguarding citizens' privacy and rights and limiting abuse and unauthorized access. In healthcare, the growth of remote medicine expands the attack surface: compromised medical devices and sensor networks can directly impact patients' health and service continuity. Finally, emerging technologies such as Quantum Key Distribution (QKD) promise high levels of protection, but they still pose challenges related to integration and operational robustness.

Securing these areas means strengthening trust in digital transformation processes and ensuring that innovation can translate into essential, resilient, and sustainable services for society.

Projects

ReQuS: Network for ultra-secure quantum communications

PI: ALESSANDRO ZAVATTA, CONSIGLIO NAZIONALE DELLE RICERCHE

SPEGO: Security and Privacy of E-Government

PI: MAURO CONTI, SAPIENZA UNIVERSITÀ DI ROMA

SmartDeFi: Smart Decentralized Finance

PI: DANIELE VENTURI, SAPIENZA UNIVERSITÀ DI ROMA

SuReCare: Secure Remote Healthcare for a Better Future

PI: LEONARDO QUERZONI, SAPIENZA UNIVERSITÀ DI ROMA

Spoke 9

CHALLENGES

The cross-cutting challenges addressed reflect the security needs of the major sectors involved in digital transformation. The spoke research activities have focused on these challenges to successfully propose solutions that are directly applicable within the reference contexts.

- **Threshold Cryptography:** Threshold cryptography is a cryptographic technique where a secret operation (such as decryption or signature) can only be executed if at least a pre-established minimum number (threshold) of participants collaborates, without any single participant holding the entire secret. This technology is set to become crucial in digital processes to replace single points of vulnerability with distributed and collaborative schemes. The main challenges emerge in scenarios where participants may dynamically join or leave the system. In such cases, the reconfiguration of keys and access policies must be securely managed without a trusted coordinator, while maintaining both forward and backward secrecy, resilience against adaptive adversaries, and scalability in distributed key generation and key refresh processes.
- **AI in Public Administration Digitalization:** Artificial Intelligence (AI) undoubtedly represents a technological revolution that is already profoundly transforming the daily use of IT tools. The integration of such technologies into the decision-making and bureaucratic processes of public administrations poses numerous challenges. The main difficulties lie in designing AI-based architectures to automate procedures, ensure regulatory compliance regarding security and privacy, and guarantee system scalability while minimizing the impact on computational resources.
- **Security of Remote Devices:** Devices used in remote monitoring environments must be securely designed. This is particularly true in the context of telemedicine. New approaches are needed to guarantee the integrity of their software and firmware, along with effective models for managing timely updates when new vulnerabilities are discovered.
- **Coordination of Heterogeneous Infrastructures:** The control and management of large quantities of heterogeneous devices require robust algorithms capable of maintaining system reliability even in the presence of adversarial or malicious behavior.
- **Protection of Sensitive Data:** Personal and health information (PII and PHI), including data collected by remote devices, must be protected from unauthorized access throughout their entire lifecycle, not just during transmission or storage.
- **Risk Management in Complex Ecosystems:** Ensuring the security of an ecosystem composed of interconnected devices, software, and services requires risk management methodologies appropriate to the cyber-physical nature of the context. Such approaches must be consistent with the latest regulations that favor digital transformation, particularly in the healthcare sector.
- **Quantum Key Distribution (QKD) Networks:** The development of metropolitan and inter-metropolitan scale networks capable of supporting QKD faces several technical limitations that reduce the scalability of this technology. Further challenges concern sustainability, costs, and interoperability, as well as the definition of test models and procedures to verify performance and applicability at scale.

MAIN RESULTS

Spoke 9 achieved significant results across all four project areas, contributing to the advancement of security solutions for complex digital scenarios.

The following main contributions were developed in the SmartDeFi project:

- **Advanced Cryptography for Privacy:** New cryptographic techniques were developed to protect data in more flexible ways. This includes methods to allow granular access to encrypted data (functional encryption and predicate encryption), systems to ensure security protocols cannot be manipulated by an adversary (non-malleability), and more efficient zero-knowledge proofs (SNARKs/partial knowledge proofs), also useful for privacy in electronic payments.
- **Artificial Intelligence Security and Vulnerabilities:** An in-depth analysis was conducted on the risks associated with modern AI systems. This includes studying novel attacks (such as poisoning and adversarial attacks) specific to Graph Neural Networks (GNNs) and recommender systems, and developing countermeasures like watermarking (inserting hidden "marks") to protect model intellectual property, as well as systems to detect malware or ransomware.
- **Explainability and Transparency of AI (XAI):** New methods were created to make AI model decisions more comprehensible to humans. A particular focus is on the use of "counterfactual explanations," which show the minimum changes in input data that would have led the model to a different decision.
- **Threat Analysis in Blockchain and DeFi:** The Decentralized Finance (DeFi) and cryptocurrency ecosystem was studied to identify and analyze illicit or manipulative activities. This includes the systematic identification and study of automated bots that manipulate the market (sniper bots), scams such as rug pulls, and deceptive practices like wash trading (fictitious transactions) in the NFT market.
- **Verification and Optimization of Quantum Software:** Methods were proposed to improve the development and reliability of programs intended for quantum computers. This includes creating higher-level programming languages (such as Silq), developing techniques to automatically verify the correctness of quantum circuits, and algorithms to optimize them (for example, by reducing the number of necessary logic gates).

In the **SPeGO** project, concrete results with potential utility for public administration were obtained with **GoTMaT**.

- A dataset of measures was created for training AI models through an automated process of acquiring, cleaning, and structuring data collected from ministerial interfaces.
- An architecture based on Large Language Models (LLM) and Retrieval-Augmented Generation (RAG) was designed and trained to automate bureaucratic procedures in Area 3 (Decriminalization). Although still being developed for a specific use case, the approach is potentially adaptable to different contexts, with the possibility of extension through targeted fine-tuning procedures.

The following results were achieved within the **SuReCare** project:

Low-Level Software Security Analysis: Advanced techniques were developed to find vulnerabilities in software by directly analyzing its binary (executable) code. This includes the use of artificial intelligence models to interpret code function and the development of more effective fuzzing methods (automatic and intelligent testing) to uncover memory management errors and other security flaws.

Development and Evaluation of Federated Learning (FL): The application of distributed machine learning, where data is not centralized, was studied. Workbenches were created to test and compare the performance of FL algorithms and methods were developed to generate "non-identical" (Non-IID) datasets that simulate realistic scenarios.

Security of Emerging Technologies: An in-depth analysis was conducted on specific risks in new technological domains. For drones (UAVs), authentication systems and defenses against attacks (e.g., GPS signal spoofing) were evaluated. For Virtual and Extended Reality (VR/XR), new privacy threats were identified, such as the possibility of extracting voice conversations by analyzing data from seemingly innocuous sensors (e.g., accelerometers).

AI Software Engineering (MLOps and AutoML): The intersection between traditional software development and artificial intelligence was examined. The benefits and security risks of the machine learning model lifecycle (MLOps) and the effectiveness of using automation (AutoML) and data quality in software engineering processes were evaluated.

Security Governance: Security frameworks were developed, based on robust international standards, which capture the peculiarities of the healthcare sector and propose security controls and solutions suitable for meeting the criteria imposed by current regulations.

Finally, the **ReQus** project developed the design of an inter-metropolitan network for quantum key exchange. The project acquired the necessary assets to test this technology in a realistic deployment, which accentuates the implementation complexity, especially for long-distance routes. A portion of this network was subject to implementation, and tests were developed on it to evaluate its performance.

Overall, the results of the Spoke 9 projects demonstrate how the integration of technological, methodological, and regulatory innovation allows for a holistic approach to the challenges of digital transformation, strengthening security in sectors with high social and economic impact.

IN THE **SPOTLIGHT**

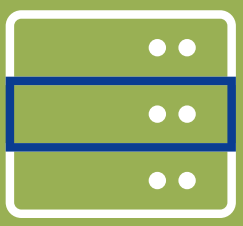
One of the most significant results is the development of a prototype to automate the generation of Area 3 (Decriminalization) measures at the Prefecture of Padua. This result demonstrates how AI technologies can reduce bureaucratic burdens, thereby speeding up processes and reallocating human resources for higher-value activities. The system is designed to run entirely on-premises, thus ensuring full control and security in the management of personal data, a crucial aspect when handling sensitive information. Concurrently, a version integrating "quantized" models is being tested: this choice drastically reduces computing requirements while simultaneously increasing portability and scalability. Thanks to this approach, the developed technology is not limited to the Padua Prefecture but can be readily replicated in other public offices, paving the way for a more efficient, secure, and citizen-friendly public administration.

Spoke
Governance and Data Protection

10

Coordinator

Pierangela Samarati
Università degli Studi di Milano



UNIVERSITÀ
DEGLI STUDI
DI MILANO

Advances in Information and Communication Technologies (ICT) and the availability of a variety of data collections offer the opportunity to easily access and process a huge amount of information, thus obtaining an extremely detailed description of people's behavior and organizational activities.

The availability of these data collections, combined with the vast capacity of modern network and computing infrastructures, clearly offers significant benefits to users, organizations, and society at large. The collection, sharing, and analysis of data, with the contribution of various stakeholders, is a major enabler for an increasingly digitally advanced society. A clear obstacle to realizing this vision is security and privacy concerns.

Data may be sensitive or confidential and therefore not openly shareable. More generally, data may be subject to access and use restrictions (including those arising from data protection regulations). Confidentiality and integrity should be guaranteed even when third parties process or store data.

Without adequate data protection, there is a significant risk of misuse, threatening the privacy of citizens and the confidentiality of companies and institutions.

Project

DGDP: Data Governance and Data Protection

PI: PIERANGELA SAMARATI, UNIVERSITÀ DEGLI STUDI DI MILANO

Spoke 10

CHALLENGES

Providing effective **data governance** and **protection solutions** is essential to the full realization of a modern digital society.

This challenge requires the development of advanced solutions that allow different actors (e.g., individuals, companies, and institutions) to **maintain control over their data** across various information release, sharing, and analysis scenarios. These solutions must also allow for the implementation of restrictions dictated by **data protection laws and regulations** (e.g., the European Union's General Data Protection Regulation) and aim to strike a **balance** between data protection on the one hand and maintaining utility and **usefulness of the information** on the other.

The development of novel solutions must also consider the specific characteristics of private and secure data management in modern and emerging scenarios, enabling, even in these contexts, data sharing, collaborative analysis, and allowing data owners to maintain control.

Technological advances have made distributed computing and data storage architectures easily accessible. **Cloud** architectures offer flexibility and cost-effectiveness (making cloud migration a priority for businesses and public entities), but they pose significant data protection challenges. For example, the number of stakeholders involved in managing information systems who could access confidential information is growing, and the relationships between them are becoming more complex. To prevent these challenges from delaying or canceling the benefits offered by the cloud, it is necessary to develop data protection solutions that take into account the complexity of these environments, allowing data owners to maintain control over shared information.

A further challenge is posed by emerging technologies, essential strategic opportunities for a digitally advanced society (as evidenced by the European Union's Artificial Intelligence Act Regulation). However, these technologies, particularly **machine learning** systems, require access to large amounts of data, exacerbating the risks associated with information sharing. Moreover, these technologies introduce new and unique vulnerabilities and issues. Advanced data governance and protection solutions are therefore needed, developed to specifically address the challenge posed by the spread of **artificial intelligence** (AI).

Finally, in the current context, another challenge is the increased complexity of interactions between stakeholders with different roles who have access to shared data, requiring innovative solutions for data sharing and controlled use.

MAIN RESULTS

Researchers working on the spoke have addressed the challenges presented by the current context by adopting a holistic approach, investigating several aspects of data **governance** and **protection throughout the entire data lifecycle**.

Research activities focused on defining solutions for specifying protection requirements, models, and policies, including data and metadata modeling to express the properties that must be considered when regulating access and sharing. Activities also focused on defining and developing innovative data protection techniques, considering the protection guarantees, and functionality required in various scenarios.

Thanks to this approach, researchers in the spoke have contributed to the development of innovative data sanitization and data wrapping solutions to enable private and secure data management in modern and emerging scenarios, enabling information sharing and collaborative analysis while allowing data owners to maintain control. These solutions have been developed considering data use restrictions resulting from data protection laws and regulations and the needs of companies and public entities.

With **more than 250 scientific articles published** in international journals and conferences, the contribution of the partners involved in the spoke has been broad and varied.

An initial result achieved was the contribution made to the development of essential components for secure data management. This involved the definition of **data and metadata modeling** solutions to express the properties that must be considered in regulating data access and sharing, the related **ontological specifications and reasoning**, and the identification and analysis of protection requirements. One example is a knowledge extraction system based on a combination of context-aware embedding models and zero-shot learning techniques. The system progressively extracts concepts representing the different meanings of the terminology used, a model that can be used to extract concepts for data modeling and ontology specification.

Another achievement by the spoke partners involved the definition of solutions to support the specification and application of data protection requirements, through languages and models that allow for the expression and reasoning of such requirements, as well as supporting the **evaluation and administration of policies**. The goal was to offer flexible, extensible, and expressive models capable of representing the various data protection requirements.

The spoke's main focus has been on the implementation of techniques such as **wrapping** (reversible) and **sanitization** (irreversible), to implement security and privacy throughout the data lifecycle. Specifically, wrapping solutions have been developed that enable data protection during storage and analysis, even in cloud environments. These innovative solutions, leveraging cryptographic techniques, ensure **data protection** for owners in **distributed environments** while also safeguarding their functional utility. Moreover, the solutions developed allow data owners to maintain control, for example by ensuring data deletion even in distributed environments.

The developed solutions also included data sanitization techniques that offer privacy and confidentiality guarantees, measured by appropriate metrics, while maintaining data utility even in innovative scenarios such as those enabled by AI. For example, in the **training** of both supervised (classification) and unsupervised (clustering) **machine learning models**, a solution was developed that, by appropriately reorganizing the data prior to sanitization, allows the required protection guarantees to be met while minimizing the impact on the

utility of the anonymized data.

Thanks to **cascading calls**, the research activities of the partners involved in the **DGDP project** have been stretched beyond the already large network of researchers of the extended SERICS partnership with the **SMIMI project**. The research has focused on evaluating **emerging data management technologies**, studying the application of protection to new data models and modern large-scale management platforms in distributed collaboration scenarios, and ensuring the efficient and effective application (and therefore scalability and applicability) of protection measures, with the aim of reducing the impact on functionality. These activities have led to advances in data protection research in the cloud, Internet of Things, AI, and Quantum Computing fields. Moreover, in the area of industrial research and experimental development, the Innovation Open Call has enabled a private company in Southern Italy to implement the **Privacy-RAG** project, which concerns the development of innovative data protection techniques aimed at mitigating the vulnerabilities of systems that exploit **Large Language Models** in Retrieval Augmented Generation scenarios, leveraging Deep Learning tools and data obfuscation.

IN THE **SPOTLIGHT**

The use of **cloud** architectures offers multiple opportunities: for data storage, for application components, and for the end-to-end management of entire processes. Migration to the cloud is therefore a priority for businesses and public entities. However, these scenarios require solutions that allow data owners to maintain control.

The multiplicity of scenarios to be managed has led to the creation of a **suite of modular solutions** implementing wrapping and sanitization techniques. The developed solutions enable data queries in distributed scenarios involving multiple providers and enable data owners to collaborate, granting each individual selective and controlled access to information. Another solution involves cloud data control, offering data owners the guarantee of data deletion even in distributed environments.

Researchers working on the spoke have also developed a cryptographic-based solution to remove confidentiality constraints that hinder the outsourcing of critical business processes such as internal controls and audit to the cloud.

The developed solutions also allow for the guarantee of confidentiality of sensitive or critical information in contexts of data and **AI model** release.

The results obtained have been presented in leading international journals and conferences in the sector.

SERICS CYBERSECURITY ACADEMY

The SERICS Cybersecurity Academy is a project conceived and implemented by the SERICS Foundation with the aim of strengthening the skills of citizens, students, and professionals in the fields of cybersecurity, digital sovereignty, and data protection. The Academy's mission is to promote a culture of cybersecurity integrated with regulatory awareness and the protection of digital rights. The Academy's activities, launched in October 2024 and continuing until December 2025, are structured along multiple lines of intervention.

LINE 1: SPECIALIZED TRAINING EMPLOYEES AND PROFESSIONALS

During the first year, the Academy has developed a course catalogue of over 15 highly specialised training courses, designed and delivered by university professors and industry experts, for a total of over 35,000 hours of training and more than 1,000 participants.

To contribute to the dissemination of the academy's training offerings, presentation seminars have been held at several SERICS project partner universities throughout Italy since the first quarter of 2025. Specifically, seminars were held at the University of Bologna, the University of Genoa, the Polytechnic University of Milan, La Sapienza University of Rome, the Polytechnic University of Turin, and the University of Salerno.

With regards to the catalogue of courses designed for the training line's target audience dedicated to employees and professionals, the latter have been grouped into 6 different thematic areas as detailed below:Cyber Threats & Defense, Software & System Security, Data Protection & Privacy, Cryptography & Authentication, Risk Management & Evaluation Frameworks, Security of Cloud & Emerging Technologies.

These courses, offered in blended mode (online lessons and in-person sessions, also accessible asynchronously via a dedicated e-learning platform), have involved employees and freelancers from public and private organizations operating in fields such as research, universities, defense, transportation, and ICT. Below is a non-exhaustive list of organizations and institutions receiving SERICS Academy courses: Italian Space Agency - ASI, Ministry of Defense, Bank of Italy, Poste Italiane, ACN, ANAS SpA, Italian Railway Network - RFI, National Institute of Geophysics and Volcanology - INGV, ENAC, Assonave/Fincantieri, University of Genoa, Liguria Digitale, Registro.it, Registrar, Cineca, CSI Piemonte, Insiel, Echolaser.

This line of activity has helped meet emerging labor market needs by strengthening advanced digital skills and encouraging the adoption of innovative cybersecurity management solutions within organizations.

LINE 2: PROMOTION AND SUPPORT OF SPECIALIST DOCTORAL SCHOOLS

From June to November 2025, the Academy provided training activities to support the doctoral programs. These activities, organized in the form of "Summer Schools," were conducted entirely in person, for a total of over 400 hours of training.

The schools represented an important opportunity for discussion and scientific exchange, involving doctoral students and professors from Italian and international universities. The initiative helped create an interdisciplinary collaboration network in the field of cybersecurity, fostering the sharing of research methodologies, best practices, and analysis tools applicable to various technological and academic fields, involving an audience of approximately 300 participants.

LINE 3: PROMOTION AND SUPPORT OF UNIVERSITY MASTER'S DEGREES

To complement the educational offerings offered by universities within the first and second level master's programs, the Academy offered in-depth modules for students focusing on cybersecurity and the protection of rights in cyberspace.

Currently, training courses have been offered in person and/or synchronously online to support the Cybersecurity Management Master's program organized by the Campus Bio Medico University of Rome, for a total of over 100 hours of training. The modules covered both basic and advanced elements of cybersecurity management.

Moreover, the academy has made available on its e-learning platform training modules supplementing the master's program, which can be taken asynchronously. The thematic areas covered the following topics:Secure Software Engineering, Web Security, Network Attacks and Security Strategies, From Cryptography to Stenography.

LINE 4: ENTREPRENEURSHIP COURSES FOR UNDERGRADUATES, RECENT GRADUATES, PHD STUDENTS, AND RECENT POSTDOCS

Particular attention was paid to entrepreneurship programs, designed for undergraduates, recent graduates, PhD students, and recent research doctorates.

The course's goal was to support young people as they enter the workforce, providing skills for defining a company vision, strategic planning, and risk management, with a focus on integrating digital technologies into corporate governance.

Over the course of the project, training courses totaling over 500 hours were designed, including business gaming activities and hands-on workshops. Additionally, the Academy launched an additional program lasting approximately 40 hours, attended by undergraduates, recent graduates, doctoral students, and recent postdocs from the Rome Biomedical Campus.

Below is a detail of the modules that make up the training course:Macroeconomic Scenarios and Change Management,Entrepreneurial Mindset and Risk Management,Business Planning and Financial Sustainability,Problem Solving and Decision-making

The program, designed for young people entering the job market, aims to support them during this phase by providing a comprehensive understanding of the entrepreneurial process, from defining vision and strategy to managing resources and risks, with a particular focus on integrating digital technologies and cybersecurity into corporate governance.

The course's objectives are geared toward acquiring the skills needed to develop a business plan for starting a business, as well as providing knowledge and skills useful for applying techniques and tools for running a business.

Four editions of the course have been delivered to date, and it is still possible to enroll in subsequent ones, for a total of 480 hours of training, including learning paths through gaming activities.

LINE 5: TRAIN THE TRAINERS

The line of activity dedicated to the training of trainers has

foreseen two types of courses:

The first type is aimed at primary and secondary school teachers, focusing on online security and digital education for students, and consists of the following modules: Introduction to digital technology for cybersecurity, Introduction to cybersecurity, Teaching the use of tools for primary and secondary school.

This course is aimed at trainers, educators, and teachers, focusing on developing skills in cybersecurity, artificial intelligence, and cyber law, with a particular focus on inclusive education for vulnerable groups. Below is a breakdown of the training modules: Fake News and AI, Addiction and digital, Online aggression, Digital tools for inclusiveness and learning, Digital wellbeing: a space for reflection, Educational strategies for working on digital awareness in the classroom, Cybersecurity and protection, Culture and awareness in the digital world.

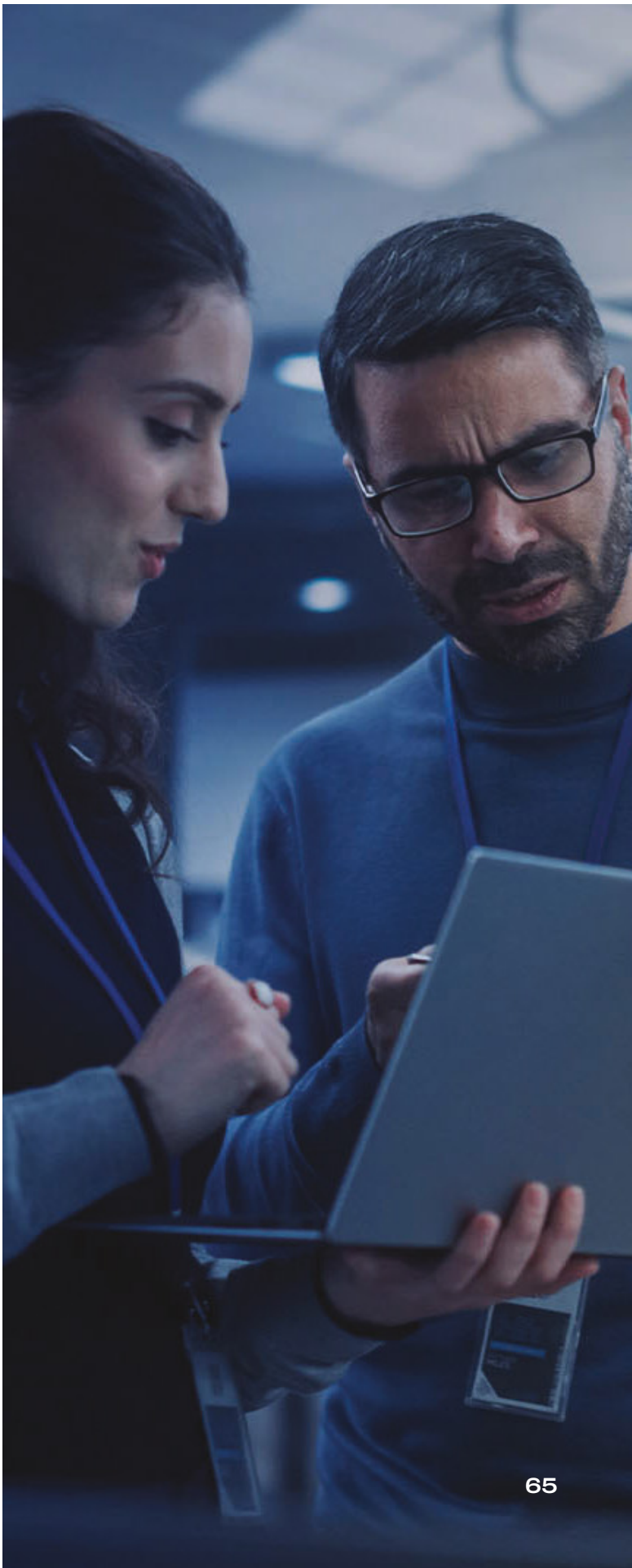
Overall, the courses involved over 300 participants (approximately 150 for each course) and included 1,600 hours of training, combining synchronous lessons, in-person activities, and online modules. These courses helped disseminate knowledge and methodologies useful for strengthening the culture of digital safety in schools and educational settings.

CONCLUSIONS

The Academy's distinctive factors can be summarized in the following drivers:

- **An excellent training offering and a diverse range of recipients** thanks to the design of highly professional and customized training programs tailored to market needs.
- **Multi-channel and integrated approach**, thanks to the possibility of being able to benefit from training in both synchronous (in person and remotely) and asynchronous modes.
- **Highly qualified teaching**, made up of professionals and industry experts from the academic world and/or research centers accredited by ANVUR.
- **High usability of the skills learned**
- **High flexibility** guaranteed by the possibility of using it free of charge and without any minimum training hours requirement.

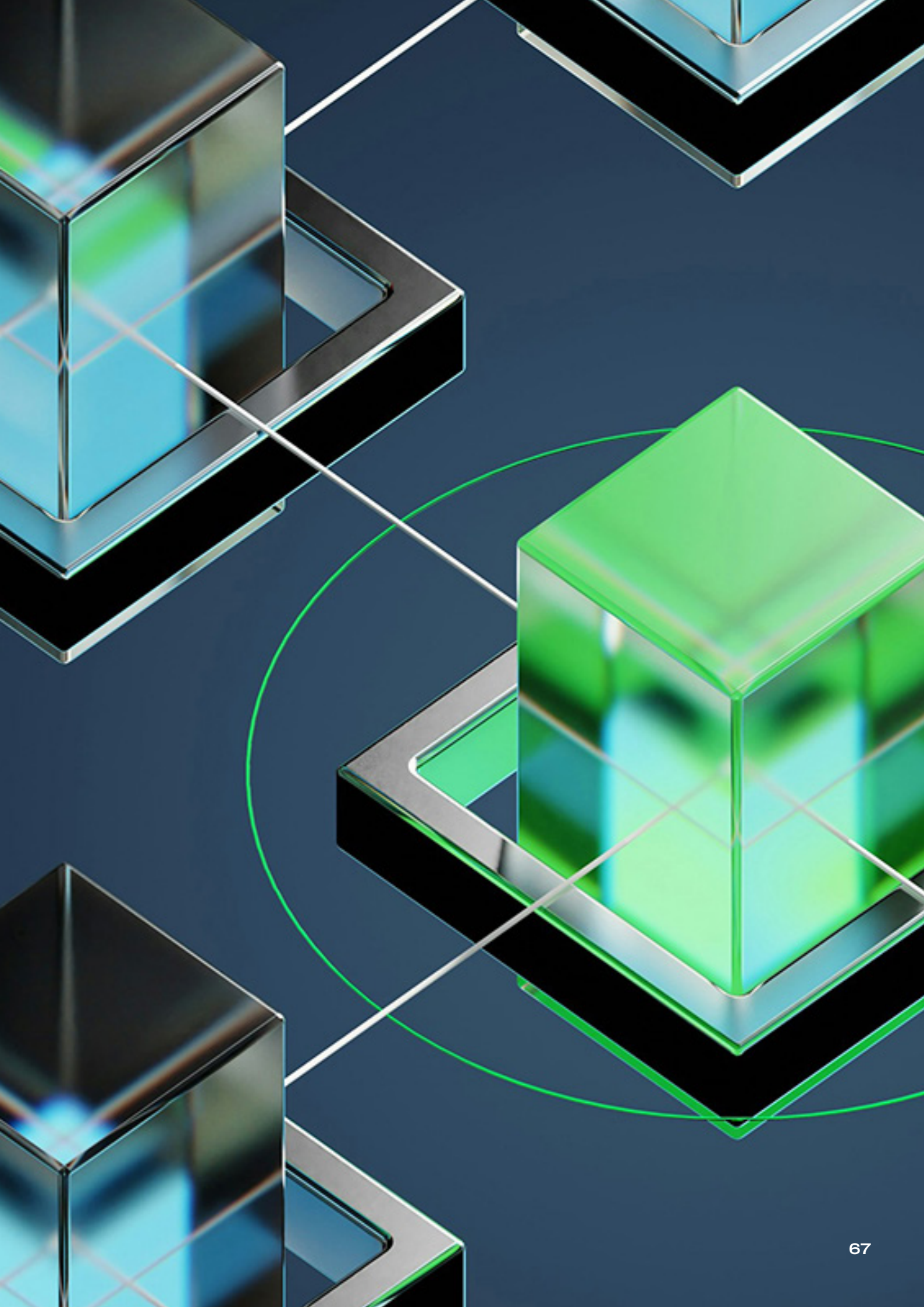
The strategic importance of the SERICS Academy also clearly emerges from the numbers and results achieved during the first year of training provision and summarised below:5 different training lines dedicated to a vast target audience, 9000 hours of free training, 150 teachers, National and international trainers and speakers involved in the design and delivery of training courses, 2,000 participants who benefited from the SERICS Academy training.



TECHNOLOGY TRANSFER

The Technology Transfer service developed within the SERICS Foundation's Extended Partnership was designed to foster cross-fertilization and cooperation between research and industry. The goal is to stimulate the transition of innovation from the research system to the productive system, support the creation and development of startups and academic spin-offs, foster talent discovery, and entrepreneurial culture within the Italian cybersecurity community.

The support model for research teams, spin-offs, and startups adopted a multidisciplinary approach: specialized intellectual property consultants, mentors, market experts, and business advisors helped develop concrete operational support tools. These were complemented by networking opportunities with industrial partners for testing or developing proof-of-concepts, as well as contacts with specialized investors. This approach allowed us to offer structured programs that are consistent with market dynamics.



TECHNOLOGY TRANSFER

INITIATIVES RELATED TO INTELLECTUAL PROPERTY AND PATENTS

The service included two complementary types of analysis: prior art analysis and Freedom to Operate (FTO). The former allowed us to reconstruct the state of the art, map existing solutions in various application areas, and identify unexplored technological opportunities along with emerging drivers. The latter aimed to verify the absence of patent constraints that could hinder the market entry of new technologies, taking into account regional and sectoral specificities.

A total of 30 analyses were conducted, covering multiple cybersecurity areas. The topics explored include cognitive security, cooperative driving, intrusion detection systems (IDS), and the development of Hyper Physical Unclonable Function (HPUF) smart tags. The integration of Software Defined Vehicle architectures and the Zero Trust paradigm was also explored, identifying the main research directions in the smart mobility sector.

Other areas of investigation included IMSI catcher technologies for intercepting cellular signals, the use of artificial intelligence in penetration testing, new watermarking methods to ensure data integrity in healthcare, post-mortem account data management, and the analysis and strengthening of critical OT critical infrastructure security protocols (for physical process control and monitoring systems, such as those in the manufacturing, energy, and transportation sectors) to ensure real-time communication between devices and the reliability and security of critical industrial processes in industrial production and manufacturing SMEs. The protection of AI models integrated into devices in various application areas and the protection of social media content through advanced watermarking systems were also examined.

SUPPORT AND ADVISORY SERVICES FOR RESEARCH TEAMS AND START-UPS

The technology transfer program supported 64 initiatives, including project ideas, research teams, and start-up companies. Of these, 28 initiatives—including informal groups, startups, and spin-offs—participated in a structured acceleration program that combined training and mentoring sessions. All received personalized assistance.

The supported initiatives focus on several key thematic clusters: security of critical infrastructure and OT/IIoT environments, protection of AI models and data, threat intelligence and risk management, connected mobility and software-defined vehicles, compliance of corporate systems with the NIS2 directive and the AI Act, and services for public administration. Additionally, projects related to social media content integrity, embedded device security, cloud-edge, and DevSecOps were supported.

In the OT/IIoT context, projects are emerging that combine network monitoring and anomaly detection for the manufacturing sector, with the goal of reducing downtime and the attack surface along the supply chain. In connected mobility, security-oriented solutions for V2I multi-factor authentication protocols are being observed.

In the telco sector, initiatives have been developed dedicated to identity protection and risk analysis arising from mobile signal interception techniques and the analysis of eSIM vulnerabilities.

The supported teams' technological maturity levels vary. Most initiatives involve activities that straddle the basic research and conceptualization phase and the technology development and validation phase. Some very promising initiatives are already in the demonstration and operational deployment phase.

The coaching methodology was structured into dedicated work sessions and brainstorming sessions aimed at transferring corporate culture, developing critical thinking on the commercial potential of solutions, and demonstrating the importance of customer centricity, competitive dynamics, and building a coherent business model.

The teams were guided in identifying the target market. The lean approach offered a pragmatic Build–Measure–Learn cycle, useful for reducing risk and quickly validating hypotheses.

From an operational perspective, individual co-design workshops were conducted, focusing on the business model. Design thinking sessions facilitated by senior mentors were conducted, working from the core of the value proposition to the construction of the nine canonical blocks of the Business Model Canvas.

Additionally to training and mentorship programs, research groups, startups, and spin-offs benefited from specialized services aimed at strengthening their business proposition, assessing market feasibility, and developing proof-of-concept projects. A total of 52 specialized advisory services were provided, including market analysis, benchmarking, defining go-to-market strategies, seeking investors and partners for real-world trials, scouting for financing opportunities, and financial planning.

OPEN INNOVATION ACTIVITIES, CHALLENGES, EXPERIMENTS, TRANSFER TO COMPANIES

In line with its advisory activities and the discussions initiated within the Innovation Board, a forum for industrial and institutional partners, the SERICS Foundation has developed an open innovation program aimed at connecting the needs of public and private stakeholders with the capabilities of the research community, startups, and spin-offs in the ecosystem.

In this context, the Cybersecurity Technology Challenge was launched to co-create solutions to maintain institutional cybersecurity. Developed in collaboration with the Tuscany Region, the challenge specifically focuses on optimizing web application firewall configurations, the use of artificial intelligence in cyber threat intelligence, and the development of penetration testing methodologies with minimal impact on production systems.

In parallel, six open innovation challenges have been launched, designed to identify agile and rapidly implementable solutions to meet the needs of industrial players, fostering active collaboration between the manufacturing system and the research community. The challenges, designed based on real operational needs identified by major national operators, partners of the SERICS Foundation, aim to facilitate the matching of industrial demand and supply of high-level research, promoting rapid and qualified technology transfer within the SERICS ecosystem.

Researchers do participate in the challenges as "solvers" by formulating proposals (reports, presentations/slides, prototypes, POCs, etc.) relating to the solution to the identified problem, the expected results/feasibility (within 3 months, long-term), and the methods of managing the IP rights (patents, know-how) employed.

In detail, the 6 Open Innovation challenges address critical issues for resilience and competitiveness in different areas:

Cybersecurity & Digital Transformation in Banking: Focused on cloud and mobile operations in the financial sector. Research is underway to develop automated defense solutions, explainable decision support tools (for risk governance), cognitive fraud detection models, and post-quantum cryptography algorithms.

Simple Security: The goal is to optimize data and transaction protection in high-impact services (financial and logistics) while ensuring a fast and transparent user experience. The focus is on data and transaction protection, simplified authentication and privacy mechanisms, and combating digital and cognitive fraud that psychologically manipulate customers.

Maritime Cybersecurity: Onboard Anomaly Detection: Innovative solutions for the timely detection of anomalous behavior and cyber threats on shipboard IT and OT systems, even in multi-ship and multi-fleet environments, with heterogeneous maritime domain data sources, and non-invasive methods, compatible with legacy systems and capable of balancing accuracy and timeliness.

Intelligent vulnerability management in industrial environments: The goal is to reduce the economic and operational impact of risk mitigation activities on large infrastructures. The challenge centers on proposing a prioritization algorithm that sensibly balances intervention costs and residual risk.

Advanced management of enterprise browser plugins: The challenge aims to reduce the risk of security incidents caused by browser add-ons used by thousands of employees at a large industrial operator. The solution must enable the identification and categorization of plugins and enable scanning, monitoring, and selective removal systems.

Industrial IoT System Security: Aimed at large companies operating in critical industrial sectors (energy, aerospace, defense). The goal is to identify modular and scalable cybersecurity solutions for protecting critical sensors, actuators, and automation systems, ensuring interoperability and ease of management in distributed and mission-critical environments.

ECOSYSTEM RELATIONSHIP

Technology transfer activities have helped build a stable channel of dialogue between the research system and businesses, generating three concrete effects. First, the valorization of the results produced by spokes, with their recognition as useful assets beyond the academic sphere. Second, the translation of projects into operational solutions capable of meeting real market needs. Finally, the opening of spaces for technological and training co-development within the national innovation ecosystem.

This approach has enabled the launch of real-world trials of solutions initially developed in the laboratory, in line with the university's third mission: asset protection and market orientation. The design effort and the related transfer and testing efforts aim to shift the paradigm in the relationship between the research world and the production system, enabling scientific research, in the medium term, as a driver of applied innovation and a driving force within a systemic approach.

ACKNOWLEDGEMENTS

Special thanks go to Luca Romanelli, Program Research Manager of the SERICS Extended Partnership, Filomena Annarumma of the Coordination Office for NRRP activities at the University of Salerno, and the SERICS Foundation's technical and specialist support team, Vincenzo Aquino, Teresa Orza, Ilaria Polito, and Silvia Salemi, for their valuable contribution, professionalism, and constant collaboration throughout the development of the project.

We also extend our sincere thanks to the Ministry of Universities and Research for the support, availability, and cooperation, which made the implementation of the project activities possible.