MISSIONE 4
ISTRUZIONE RICERCA

SECURITY AND RIGHTS IN THE CYBERSPACE (SERICS)

CYBERSECURITY, NUOVE TECNOLOGIE E TUTELA DEI DIRITTI

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Tematica: 7. *Cybersecurity, nuove tecnologie e tutela dei diritti*

Obiettivi *(Sez A dell'Annex 1)*

The security of cyberspace is among the main concerns of governments worldwide. Blocking business
operations, surreptitious control of critical infrastructure services, theft of intellectual property or important information are examples of the threats. Recent campaigns of ransomware and data theft have been the visible events in a series of attacks in every corner of the planet. Cyber attacks raise alarm in the population, damage the economy, and endanger the very safety of citizens when they hit the distribution networks of essential services such as health, energy, transport, i.e,. the critical infrastructures of modern society. In Italy, entire sectors of excellence, such as mechanics, shipbuilding, Made-in-Italy, tourism, cultural heritage, agro-food, and transport, could suffer heavy reductions in their turnover, due to attacks perpetrated in cyberspace by commercial competitors, organized crime, but also by sovereign states. Attacks can compromise the credibility of a company in a short time, or make it operate for a long time in suboptimal conditions, undermining the development of its business and its ability to sell products. A successful attack could destabilize the stock or bond market, plunging entire countries into chaos, or act on the hardware and software components of distribution networks, blocking, for example, gas supplies or the cycle of urban waste. Not only industry but also democracy may be attacked in cyberspace. Fake news are the evolution of attacks based on social engineering: packaged, personalized, and spread in a targeted way through cyberspace, false information tends to confuse and destabilize citizens.
These considerations raise the question of how to defend cyberspace from the threats and attacks that, through malicious cyber actions, perpetrate fraud, steal sensitive and strategic business data, and affect the financial stability, public order, and democratic life of a country.
For this reason, it is particularly important to involve institutions, universities, research centers, and companies in an increasingly intense and integrated way. A country that does not put cybersecurity at the center of its policies of innovation and digital transformation poses a serious risk to its economic prosperity and independence.
The above ones were the starting considerations of the part of the National Research Plan 2021-2027 dedicated to Security for Social systems. After these considerations, the following fundamental objectives were there listed:

- Protecting Data and Services on the Web: Through certification of applications dealing with sensitive data; automated application analysis; analysis of interoperating systems.
- Detecting Malware: Through collection and validation of datasets representative of normal or abnormal behaviors; national database of malicious code, integrated with databases from other countries; tools and methodologies for automated cyberspace surveillance.
- Combating Cybercrime: Through advanced threat intelligence; identification of vulnerabilities in complex
environments; automation of forensic investigations.
- Defending Democracy: Through a multidisciplinary approach to fake news detection; social media monitoring to identify and understand the dynamics of echo chambers; early warning on messages that may be vehicles of false, misleading or instrumental information.
- Defending Artificial Intelligence: Through the detection of data or code injection; robust learning algorithms resilient to attacks, techniques for preserving data integrity in training and in production; approaches to training that guarantee privacy preservation.
- Ensuring privacy: Through homomorphic encryption to directly process encrypted data, techniques for

protecting federated data infrastructures in international data spaces; data anonymization to ensure that the user cannot be re-identified; a secure multi-party computation.
● Preparing for Quantum Computer attacks: new cryptographic systems whose level of security is quantifiable with respect to cryptanalysis, considering both quantum and classical devices; analysis of the usability of quantum-based cryptographic systems and key generation and distribution methods for general-purpose computing devices; guaranteeing interoperability between quantum cryptographic systems and classical ones.
● Defending Hardware: Through national methodologies to fully control the entire hardware supply chain, from design to the manufacturing process, to maintenance, till dismissing; vulnerability-tolerant national architectures that guarantee predefined security levels, even in potentially vulnerable systems.
It must be said that the above objectives were concentrating on cybersecurity as an engineering discipline. But cybersecurity is not just that. A distinctive feature of our proposal is keeping the focus also on what is considered the "weak link" in the overall security of cyberspace: the human being. Real and effective security of cyberspace is guaranteed not only by a sound and robust technology, but also by an equally sound and robust regulation of human behaviors. And this requires a deep involvement from those who understand non-technical motivations, forces, and incentives - economists, sociologists, lawyers, and other experts - to create a holistic perspective that can anticipate and guide effective real-world strategies. This reality creates an environment that is rich in collaborations, partnerships, and new forms of commercial and academic working relationships – yet at the same time is deeply challenging due to fundamental differences in research culture, methodology, and approach. This is the additional challenge of the project that is however central to its success: to reach this aim, the following objectives are crucial:
● Rights, Rules, and Authorities for a safe Cyberspace: Creating a national network for tech lawyers and a Cybersecurity Regulation Archive (combining and harmonizing laws, ethical codes, soft-law, doctrine, jurisprudence on Cyberspace); contributing to International and EU multilevel co-regulation of Cyberspace and to the regulation of cross-border protection of private rights.
● Legal and Ethical Issues for Cybersafety: Digital privacy and online rights; regulation of E-government and E-democracy; Development of secure, privacy-proof, and reliable methodologies for digital sovereignty; cybercrime and cyber diplomacy.
● Lifelong Learning and Education on Cybersecurity Regulation: Training models and methods for Cybersecurity education and for data governance; Cyber-compliance for Public Administration and for Small and Medium Enterprises.

SCIENTIFIC OBJECTIVES

The starting point to structure the SERICS project has been the CyBoK, a comprehensive Body of Knowledge
designed with the help of major internationally-recognised experts to map the Cybersecurity knowledge space. Figure 1a summarizes the 21 knowledge areas introduced in the CyBoK that have been the basis for structuring this proposal. In fact, we have used to define the 10 Thematic Areas (TA) of SERICS that are used to structure the ten Spokes of the proposal. The thematic areas have been identified after a long confrontation with a large group of Italian researchers representing the different approaches to cybersecurity. The names of the thematic areas and their main objectives as described below. Figure 1b represents pictorially the coverage of the knowledge areas by SERICS thematic ones.

Thematic Area 1: Human, Social, and Legal Aspects

The main objective of TA 1 is to investigate how to create a compelling and secure Cyberspace by combining sound technological systems with strong and robust regulation of human behavior. This will be based on an innovative ecosystem where experts in technology, law, ethics, sociology, and education will bring together to create a process that, through a holistic perspective, can anticipate and test new cybersecurity policies. In particular, TA 1 will cover and produce new knowledge on regulatory, legal and ethical aspects of CyberSpace.
Detailed objectives of TA 1 can be classified into five macro-categories. The first category deals with rights, rules, definitions, taxonomies, and authorities aimed at creating new forms of co-regulation for cyberspace. The second category analyzes legal and ethical issues for cybersafety, such as fundamental rights related to this new ecosystem. The third category encompasses lifelong learning and education models on legal issues of cybersecurity. The fourth category comprehends cybercrime and cyber diplomacy as important and crucial elements of a new national strategy by developing the knowledge on this issue to the academic and general public. The fifth category includes digital sovereignty, even for computations and technologies based on Artificial Intelligence, and cloud, fog, and edge computing, and their applications in specific sectors, like those concerned with energy and transport.
Thematic Area 2: Misinformation and Fakes
This TA aims to design and develop innovative solutions to identify and manage information disorder threats that come alive through fake news and deep fake spreading. These malicious actions, leveraging people's cognitive bias, generate citizens' disapproval and media and institutions untrust. The project will utilize a multidisciplinary approach leveraging open source automation achieved through Intelligence Analysis, recent advancements in Artificial Intelligence, and knowledge from political and geopolitical sciences. Firstly, it aims to check news content's truth and the reliability of news sources. The objective is to implement text and multimedia content analysis methodologies to detect meaningful patterns to be used for finding disinformation attempts. Moreover, the analysis of Social Media communities will give evidence of the cognitive vulnerabilities of participants and threats related to fake news spread. The objective is to design an early alerting system for debunking false information by leveraging the syntactic integrity of contents and patterns related to disinformation flows. The resulting framework aims to generate people's awareness about risky behaviors associated with sharing questionable content. Moreover, the framework will support experts and security officers in decision making by adopting a human-in-the-loop approach.
Thematic Area 3: Attacks and Defenses TA 3 aims to analyze emerging attack methodologies and develop advanced methods for detecting attacks and identifying guidelines for the design of computer systems guaranteeing reduced vulnerabilities for new attack categories. The detailed objectives can be divided into four macro categories: (i) Development of advanced tools for malware analysis and software analysis aimed at identifying vulnerabilities that could be exploited by malware; (ii) Development of tools for network traffic analysis able to identify communications related to ongoing attacks; (iii) Development of machine learning systems that are robust to attacks and through which it is possible to extract knowledge aimed at creating more advanced tools for a timely analysis of attacks and their early detection; (iv) Analysis of the "human factors" involved in an attack with the development of tools for the analysis and correlation of information from OSINT (open sources intelligence) and the defense and prevention of attacks based on social engineering techniques.

Thematic Area 4: Operating Systems and Virtualization Security
Operating Systems (OS) and Virtualization Technologies (VT) are key enablers for existing and emerging
computation and communication paradigms, namely cloud, fog, edge computing and 5G/6G. By leveraging the primitive security mechanisms provided by the hardware, OS and VT offer

key security mechanisms and services (e.g., basic identity management and access control) upon which the security of applications, and henceforth of the whole cyberspace, is rooted. TA 4 is concerned with developing high-level automated security services and innovative security assessment and assurance methodologies to support the secure-by-design development and verification of cloud, edge, and 5G applications. The effectiveness of the proposed techniques will be assessed by stress-testing them in simulated, yet highly realistic attack scenarios, safely run within a platform of federated Cyber Ranges.

Thematic Area 5: Cryptography and Distributed Systems Security
TA 5 is mainly concerned with research activities in cryptography and distributed system security domains.
Given the vastness of these domains and to identify concrete objectives aimed at obtaining long-term results ofhigh technological level and possible impact on the country, TA 5 sees the coexistence of two souls. Among the subtopics (i) cryptographic primitives and protocols, (ii) foundational cryptography and cryptanalysis, (iii) post-quantum crypto, (iv) digital identity, authentication and accountability, and (v) distributed ledgers and blockchain, the two souls are the continuous search for the deepening of knowledge (in all the fields mentioned above), and the plan to apply this investigative approach to applied research goals. During the lifetime of thepresent initiative, this will be achieved by implementing a single unifying project focused on the notion ofdigital identification and tracing, by interpreting this notion also from unconventional perspectives. According to this general objective, the research lines of TA 5 will move along different tracks, stimulating continuous interactions between them and vertical applications of the results on specific application domains.

Thematic Area 6: Software and Platform Security
The first scientific goal of TA 6 is to provide an ecosystem where software developers can easily reason about software security. This will be based on innovative security-aware programming abstractions and new semantic models that will allow to formalize, verify, and certify security properties according to a secure-by-design methodology. The aim is to develop new formal techniques based on secure compilation and secure composition, to reduce the gap between formal models, essential to provide full guarantees of correctness, and actual implementations. The second scientific goal is to provide innovative solutions to protect the software supply chain, including the software management and development process. The aim is to develop new techniques to perform security tests through continuous dynamic analysis and to protect software, detecting malicious activities and preventing or limiting their impact, according to a self-defense paradigm. Test scenarios will be used to validate and experimentally evaluate the proposed techniques.

Thematic Area 7: Infrastructure Security
TA 7 has as its general objective the advancement of infrastructure security technologies. This general goal translates into four specific objectives: (i) Designing and developing an open and nationally available secure computing architecture that will be the starting point for the construction of secure infrastructures that do not suffer from potential risks deriving from the use of proprietary technologies; (ii) Improving the safety of the automotive infrastructure, which, with the massive interconnection and electrification of cars, will become one of the most vulnerable assets in the country; (iii) Improving safety, security, and resiliency of Smart powergrids, which are a fundamental component for optimizing energy use and for achieving the Green deal; (iv) Contributing to the improvement of the security posture of the ITC assets (i.e., networks, IT/OT systems and services) included within the “Perimetro di Sicurezza

Nazionale Cibernetica" (Cybersecurity National Perimeter) by providing ontologies, methodologies, guidelines, best practices, and tools.

Thematic Area 8: Risk Management and Governance
TA 8 aims to contribute to the cyber resilience of future systems and services characterized by increasingly
interconnected digital components that are intrinsically vulnerable as required by the EU through NIS and NIS2, and by the Italian National Agency for Cybersecurity (ACN). To this purpose, it proposes a holistic approach to risk-based cybersecurity that must also include resilience, privacy, safety of organizations, industries, critical infrastructures and related supply chains. This TA includes interdisciplinary competencies that are suitable to face both scientific-technological and legal and political challenges through novel models for continuous evaluation of threats and vulnerabilities but also through the design of self-defensive network components. TA 8 aims also to further the vision that a developed digital Europe requires the protection of fundamental rights and freedoms, the promotion of social awareness and widespread cyber training, as well as the achievement of a gender balance in cybersecurity.

Thematic Area 9: Securing Digital Transformation
TA 9 has the main objective of studying new approaches, methodologies, solutions, and tools that can provide adequate security guarantees for new application scenarios that are emerging today as a consequence of strong acceleration towards pervasive digital transformation. In particular, the researchers involved in the topics of TA 9 will work on four reference scenarios, considered to be of strategic interest for the near future: (i) development of decentralized finance solutions based on secure distributed technologies such as DLTs and smart contracts; (ii) strengthening of data security and privacy properties in services provided by the public administration within e-government programs; (iii) remote healthcare solutions based on personal devices, essential for more efficient management of chronically ill patients or those patients in need of continuous monitoring; (iv) quantum key distribution technologies for critical applications.

Thematic Area 10: Data Governance and Protection
Modern digital society is based, and will increasingly be based, on the gathering, sharing, and analysis of large collections of data, with clear benefits, from the personal, to the business, research, and social domains. The full realization of a digital society based on data can only happen if there is trust in the security and privacy of such data, and therefore if solutions that guarantee correct protection and use of data are available. Data protection laws and regulations impose restrictions that limit the use of data, and individuals, as well as companies, demand compliance with their protection requirements and the assurance of effective protection of their data.
TA 10 responds to this need by empowering the various actors involved in data sharing and using scenarios with control over their data, supporting data sharing in a selective and secure way, at the same time guaranteeing functionality, efficiency, and scalability. The data protection solutions developed within TA 10 will enable and encourage new application scenarios and introduce new opportunities for data sharing, in a controlled way, in compliance with privacy and access restrictions and guarantee integrity of the data and the results of the analyses. TA 10 will therefore contribute to a true and full realization of digital sovereignty.

Partner

N TOTALE SOGGETTI: 24

Proponente: Università degli Studi di Salerno

Partecipanti:

SOGGETTI PUBBLICI

Università

- Università degli Studi di Bari Aldo Moro
- Università degli Studi di Firenze
- Università degli Studi di Salerno
- Università degli Studi di Cagliari
- Università di Genova
- Università della Calabria
- Università Ca' Foscari Venezia
- Politecnico di Torino
- Alma Mater Studiorum - Università di Bologna
- Sapienza Università di Roma
- Università degli Studi di Milano

Organismi di Ricerca

- Scuola Superiore Sant'Anna di Pisa
- Consiglio Nazionale delle Ricerche
- Scuola IMT Alti Studi Lucca

SOGGETTI PRIVATI:

Organismi di Ricerca

- Consorzio Interuniversitario Nazionale per l'Informatica
- Consorzio nazionale interuniversitario per le telecomunicazioni
- Fondazione Bruno Kessler
- Fondazione Ugo Bordoni

Imprese

- Deloitte
- ENI
- FINCANTIERI
- ISP - Intesa Sanpaolo SpA
- Leonardo S.p.A.
- Telsy S.p.A.

Gli Spoke

Spoke n. 1 *"Human, Social, and Legal Aspects"*

Leader spoke: Consiglio Nazionale delle Ricerche

Affiliati allo spoke:

- Università degli Studi di Firenze
- Università degli Studi di Cagliari
- Università di Genova
- Alma Mater Studiorum - Università di Bologna
- Università degli Studi di Milano
- Scuola Superiore Sant'Anna di Pisa

Spoke n. 2 *"Misinformation and Fakes"*

Leader spoke: Università degli Studi di Salerno

Affiliati allo spoke:

- Consiglio Nazionale delle Ricerche
- Scuola IMT Alti Studi Lucca
- Consorzio nazionale interuniversitario per le telecomunicazioni
- Università degli Studi di Cagliari
- Università Ca' Foscari Venezia
- Sapienza Università di Roma
- Università degli Studi di Milano
- ENI S.p.A.

Spoke n. 3 *"Attacks and Defenses"*

Leader spoke: Università degli Studi di Cagliari

Affiliati allo spoke:

Commentato [BS1]: TIM risulta affiliata allo spoke ma non è tra i partner. Ho inserito Telsy che è una società del gruppo

- Scuola Superiore Sant'Anna di Pisa
- Consiglio Nazionale delle Ricerche
- Università degli Studi di Bari Aldo Moro
- Università di Genova
- Università della Calabria
- Sapienza Università di Roma
- Università degli Studi di Salerno
- Università Ca' Foscari Venezia

- ENI
- Leonardo S.p.A.
- Telsy S.p.A.

Spoke n. 4 "*Operating Systems and Virtualization Security*"

Leader spoke: Università di Genova

Affiliati allo spoke:

- Consorzio Interuniversitario Nazionale per l'Informatica
- Consorzio nazionale interuniversitario per le telecomunicazioni
- Consiglio Nazionale delle Ricerche
- Scuola IMT Alti Studi Lucca
- Fondazione Bruno Kessler
- Fondazione Ugo Bordoni
- Università degli Studi di Salerno
- Università della Calabria
- Sapienza Università di Roma
- FINCANTIERI
- Leonardo S.p.A.

Spoke n. 5 "*Cryptography and Distributed Systems Security*"

Leader spoke: Università della Calabria

Affiliati allo spoke:

Consiglio Nazionale delle Ricerche

- Fondazione Bruno Kessler
- Università degli Studi di Salerno
- Consiglio Nazionale delle Ricerche
- Università degli Studi di Cagliari
- Politecnico di Torino
- Deloitte
- ISP - Intesa Sanpaolo SpA

Spoke n. 6 "*Software and Platform Security*"

Leader spoke: Università Ca' Foscari Venezia

Affiliati allo spoke:

- Università degli Studi di Salerno
- Università degli Studi di Cagliari
- Deloitte
- Università degli Studi di Bari Aldo Moro
- Università degli Studi di Firenze
- Sapienza Università di Roma

- Scuola IMT Alti Studi Lucca

Spoke n. 7 *"Infrastructure Security"*

Leader spoke: Politecnico di Torino

Affiliati allo spoke:

- Consorzio Interuniversitario Nazionale per l'Informatica
- Consiglio Nazionale delle Ricerche
- Fondazione Ugo Bordoni
- Scuola IMT Alti Studi Lucca
- Scuola Superiore Sant'Anna di Pisa
- Università degli Studi di Cagliari
- Università di Genova
- Deloitte
- Leonardo S.p.A.
- Telsy S.p.A.

Commentato [BS2]: TIM risulta affiliata allo spoke ma non è tra i partner. Ho inserito Telsy che è una società del gruppo

Spoke n. 8 *"Risk Management and Governance"*

Leader spoke: Alma Mater Studiorum Università di Bologna

Affiliati allo spoke:

- Consorzio nazionale interuniversitario per le telecomunicazioni
- Consiglio Nazionale delle Ricerche
- Università degli Studi di Bari Aldo Moro
- Università degli Studi di Firenze
- Università di Genova
- Politecnico di Torino
- Università degli Studi di Milano
- Deloitte

Spoke n. 9 *"Securing Digital Transformation"*

Leader spoke: Sapienza Università di Roma

Affiliati allo spoke:

- Consiglio Nazionale delle Ricerche
- Università degli Studi di Bari Aldo Moro
- Università degli Studi di Cagliari
- Università di Genova
- Università degli Studi di Milano
- Università degli Studi di Salerno
- Telsy S.p.A.

- ISP - Intesa Sanpaolo SpA

Spoke n. 10 *"Data Governance and Protection"*

Leader spoke: Università degli Studi di Milano

Affiliati allo spoke:

- Sapienza Università di Roma
- Università degli Studi di Firenze
- Università degli Studi di Cagliari
- Università degli Studi di Salerno
- Leonardo S.p.A.

Dati finanziari (da decreto di concessione)

Costo complessivo: 116.358.089,30€

Agevolazione MUR: 114.499.997,53 €

Bandi a cascata: 41% dei costi di progetto