Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERI
SECURITY AND RIGHTS IN T

Secure and TRaceable Identities in Distributed Environments (STRIDE)

Silvio Ranise

Jun 6, 2023

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Partenariato Esteso – Piano Nazionale di Ripresa e Resilienza (PNRR)
(Extended Partnership — Recovery and Resilience Facility, RFF)

- **SEcurity and RIghts in the CyberSpace (SERICS)**
- Extended Partnership in *Area 7 - Cybersecurity: new technologies and protection of rights*
- Proposer: **University of Salerno**
- Coordinated by **CINI Cybersecurity National Lab**
- Total cost: **116 M€** (funding **114 M€)**
- Start: **Jan 1, 2023**
- Duration: **3 years**

cini consorzio interuniversitario nazionale per l'informatica

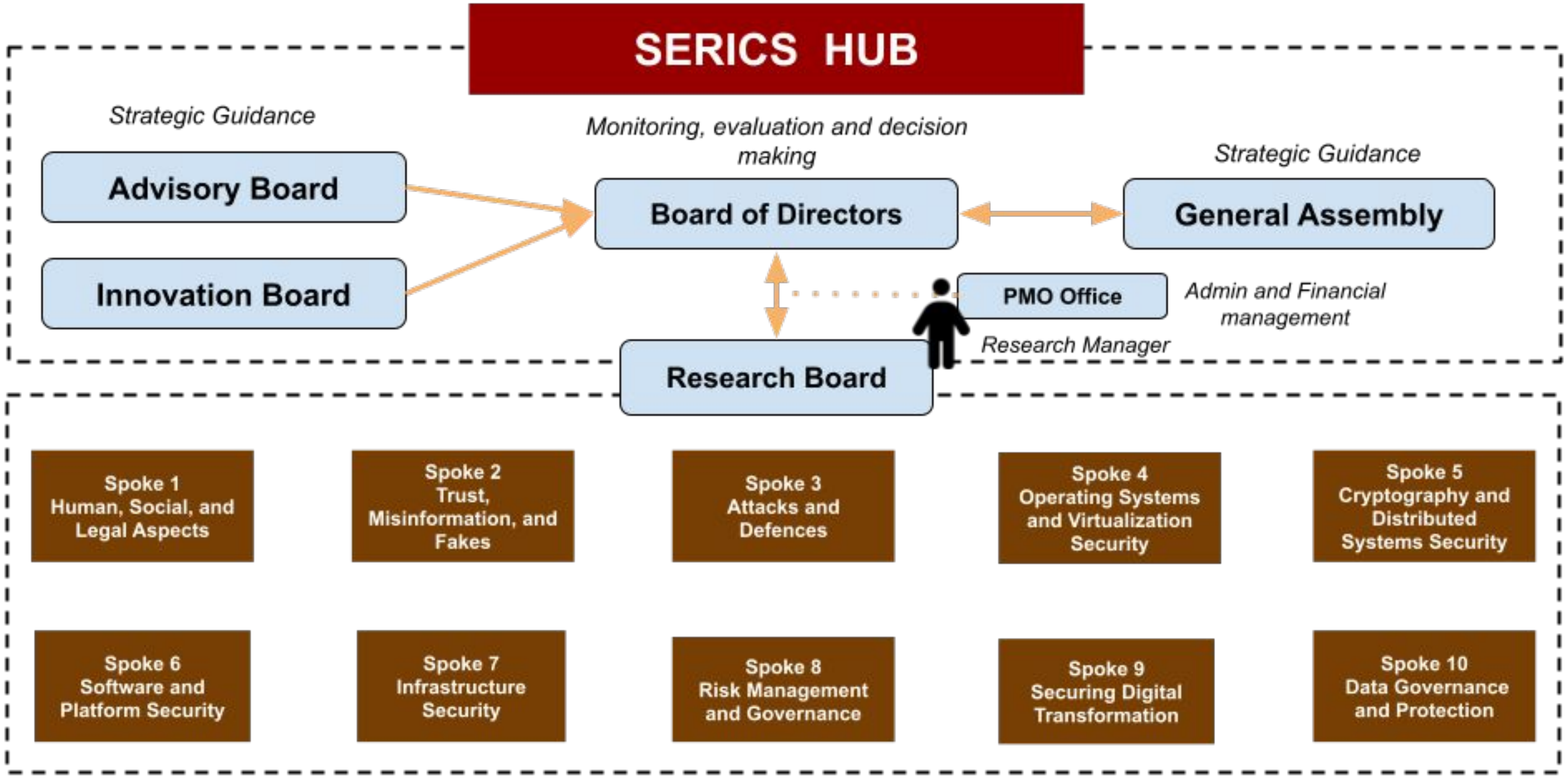
CYBERSECURITY NATIONAL LAB

Overview

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS Hub & Spokes



SERICS HUB

Strategic Guidance

Advisory Board

Innovation Board

Monitoring, evaluation and decision making

Board of Directors

Strategic Guidance

General Assembly

PMO Office

Admin and Financial management

Research Manager

Research Board

Spoke 1
Human, Social, and Legal Aspects

Spoke 2
Trust, Misinformation, and Fakes

Spoke 3
Attacks and Defences

Spoke 4
Operating Systems and Virtualization Security

Spoke 5
Cryptography and Distributed Systems Security

Spoke 6
Software and Platform Security

Spoke 7
Infrastructure Security

Spoke 8
Risk Management and Governance

Spoke 9
Securing Digital Transformation

Spoke 10
Data Governance and Protection

SERICS Partnership

Universities and RIs

- CNR
- UniSA
- UniFI
- UniRoma1
- UniCAL
- UniBA
- UniCA
- UniBO
- UniMI
- UniGE
- UniVE
- PoliTO
- CINI
- CNIT
- IMT – Lucca
- SSPA – Pisa
- FBK
- FUB

Companies

- DELOITTE
- ENI
- FINCANTIERI
- ISP
- Leonardo
- TIM

- Very **complex** initiative
- **116 ML**
  - Around **5%** for a new **National Cybersecurity *Academy***
  - **41,3%** destined to the **South** of Italy
  - **18%** devoted to **new researchers**
  - Around **6%** for **Innovation Open Calls**
  - **20%** for **Research Open Calls** (within projects)

© Vemaps.com

- Very **complex** initiative
- **116 ML**
  - Around **5%** for a new **National Cybersecurity *Academy***
  - **41,3%** destined to the **South** of Italy
  - **18%** devoted to **new researchers**
  - Around **6%** for **Innovation Open Calls**
  - **20%** for **Research Open Calls** (within projects)

© Vemaps.com

Academy’s Goals

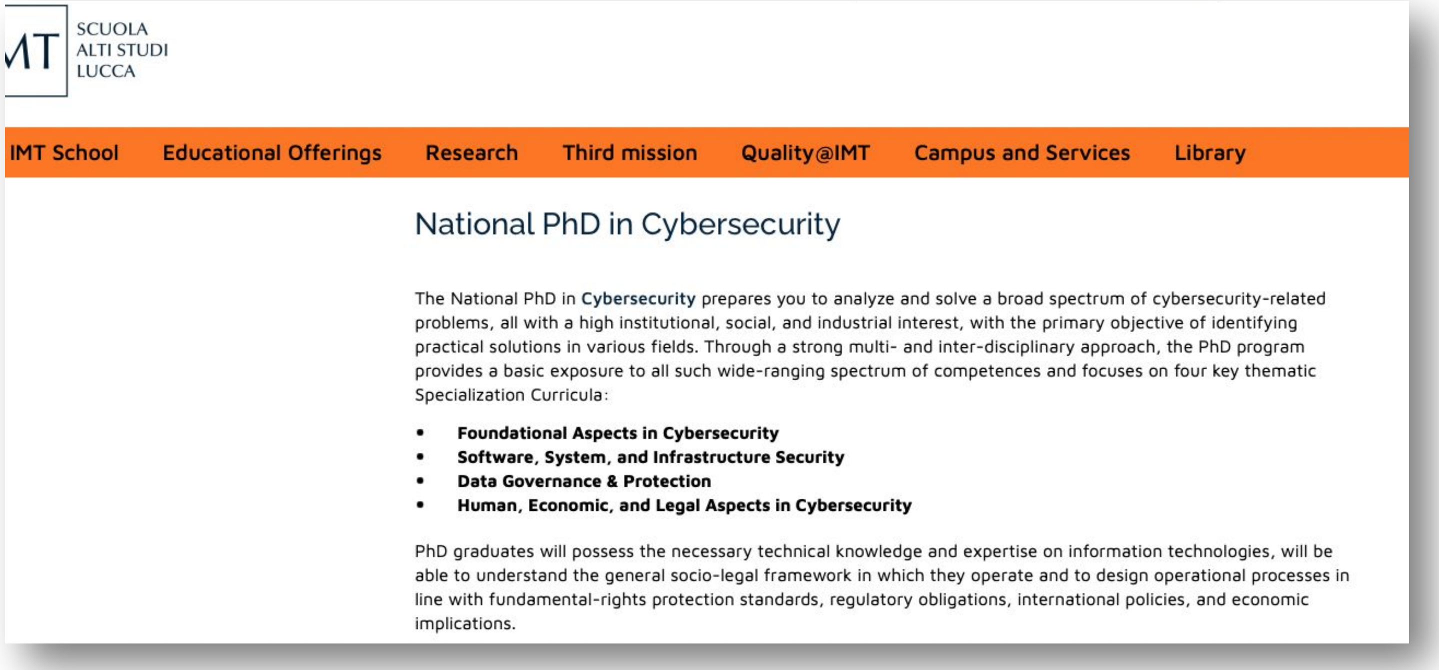
Supporting and implementing a set of activities aimed at improving the resilience and the posture of different categories of people w.r.t. to cybersecurity

This will include:

- *Training activities*:
  - For trainers
  - For trainees
- *Training materials:*
  - PhD Courses
  - Lectures & Seminars
  - Challenges
- *Training facilities:*
  - Platforms
  - Custom Cyber-Ranges
- *Training evaluation*

PhD National Program on Cybersecurity

- Interdisciplinary PhD Program: technical, regulatory and ethical aspects covered
- 1st year just started
- 25 students selected and enrolled
- 4 weeks of *mis-à-niveau* courses



National PhD in Cybersecurity

The National PhD in Cybersecurity prepares you to analyze and solve a broad spectrum of cybersecurity-related problems, all with a high institutional, social, and industrial interest, with the primary objective of identifying practical solutions in various fields. Through a strong multi- and inter-disciplinary approach, the PhD program provides a basic exposure to all such wide-ranging spectrum of competences and focuses on four key thematic Specialization Curricula:

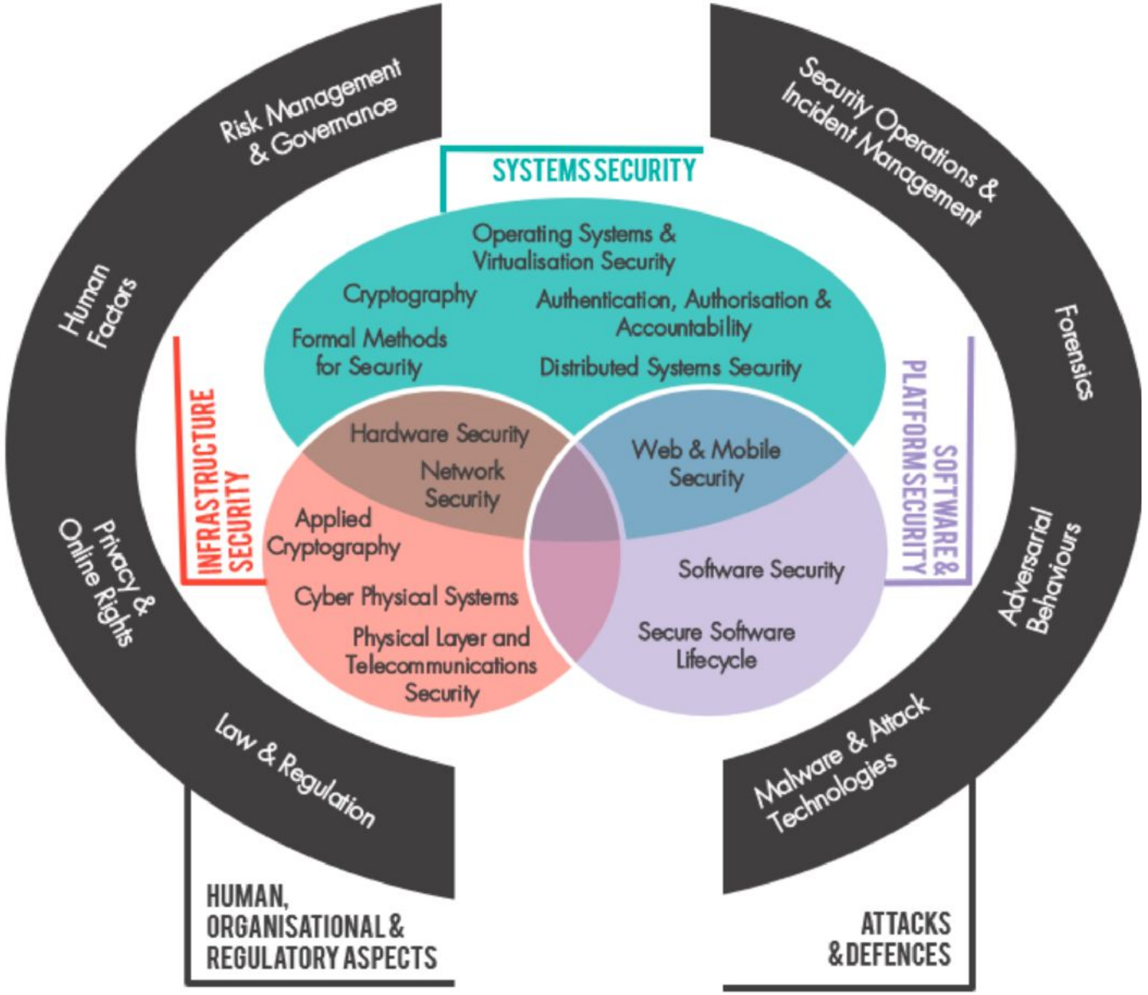
- **Foundational Aspects in Cybersecurity**
- **Software, System, and Infrastructure Security**
- **Data Governance & Protection**
- **Human, Economic, and Legal Aspects in Cybersecurity**

PhD graduates will possess the necessary technical knowledge and expertise on information technologies, will be able to understand the general socio-legal framework in which they operate and to design operational processes in line with fundamental-rights protection standards, regulatory obligations, international policies, and economic implications.

SERICS Thematic Areas

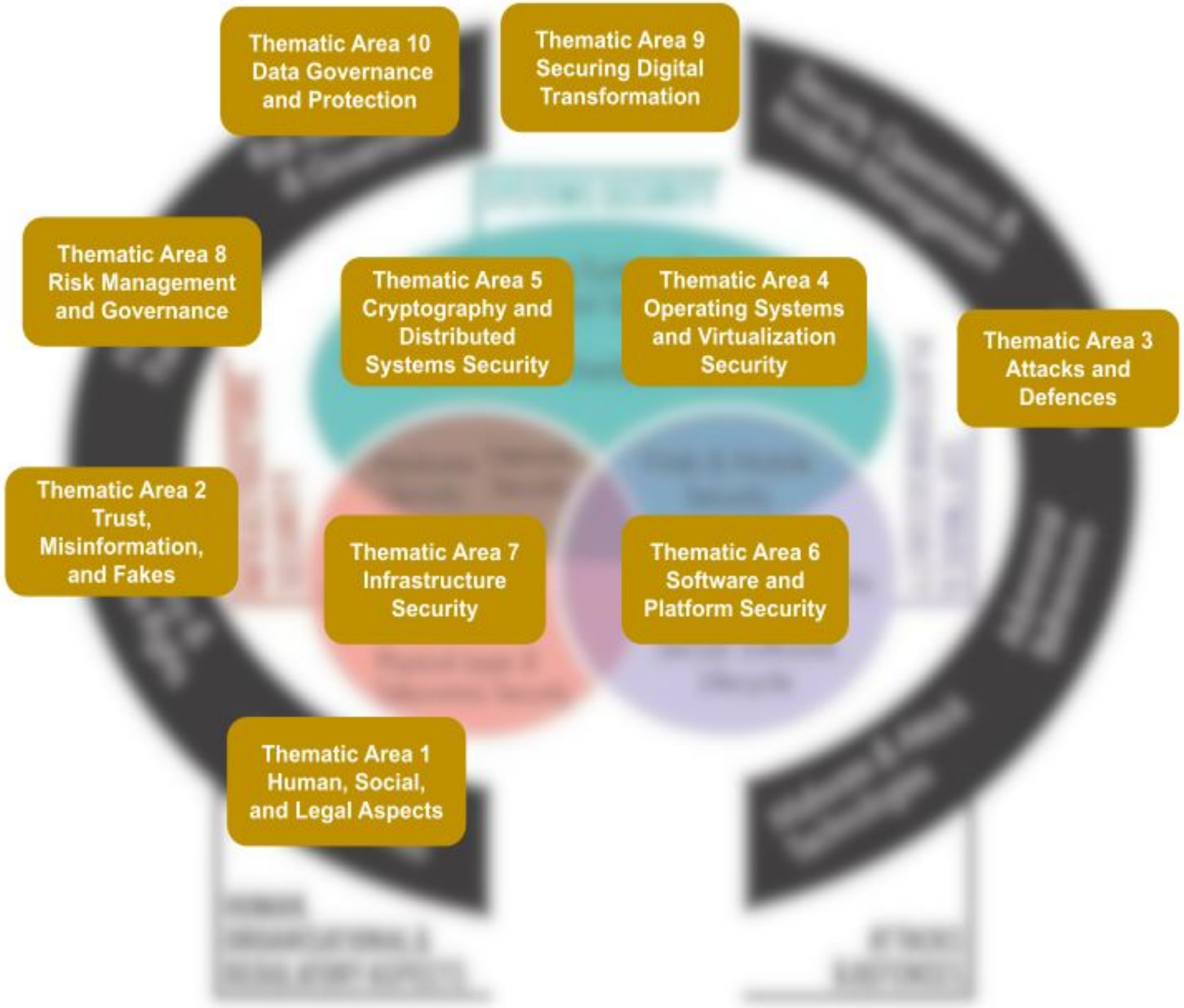
The Cyber Security Body Of Knowledge

https://www.cybok.org/


SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
SOFTWARE & PLATFORM SECURITY
Web & Mobile Security
Software Security
Secure Software Lifecycle
Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

SERICS Thematic Areas

- 10 Thematic Areas
- 27 research projects
- Each Thematic Area managed by a Spoke



Thematic Area 10
Data Governance and Protection

Thematic Area 9
Securing Digital Transformation

Thematic Area 8
Risk Management and Governance

Thematic Area 5
Cryptography and Distributed Systems Security

Thematic Area 4
Operating Systems and Virtualization Security

Thematic Area 3
Attacks and Defences

Thematic Area 2
Trust, Misinformation, and Fakes

Thematic Area 7
Infrastructure Security

Thematic Area 6
Software and Platform Security

Thematic Area 1
Human, Social, and Legal Aspects

	Thematic Area	Spoke / Affiliated	#scholars
1	Human, Social, and Legal Aspects	**CNR**, UniBO, UniCA, UniFI, UniGE, UniMI	45
2	Trust, Misinformation, and Fakes	**UniSA**, CNIT, CNR, IMT, UniCA, UniMI, UniRoma1, UniVE, ENI	44
3	Attacks and Defences	**UniCA**, CNR, SSSA, UniBA, UniCAL, UniGE, UniRoma1, UniSA, UniVE ENI, LDO, TIM	54
4	Operating Systems and Virtualization Security	**UniGE**, CNIT, CNR, CINI, FBK, FUB, IMT, UniCAL, UniRoma1, UniSA, Fincantieri, LDO	52
5	Cryptography and Distributed Systems Security	**UniCAL**, CNR, FBK, PoliTO, UniCA, UniSA, Deloitte, ISP	38
6	Software and Platform Security	**UniVE**, IMT, UniBA, UniCA, UniFI, UniRoma1, UniSA, Deloitte	32
7	Infrastructure Security	**PoliTO**, CNR, CINI, FUB, IMT, SSSA, UniCA, UniGE, Deloitte, LDO, TIM	52
8	Risk Management & Governance	**UniBO**, CNIT, CNR, PoliTO, UniBA, UniFI, UniGE, UniMI, Deloitte	58
9	Securing Digital Transformation	**UniRoma1**. CNR, UniBA, UniCA, UniGE, UniMI, UniSA, ISP, TIM	35
10	Data Governance and Protection	**UniMI**, UniCA, UniFI, UniRoma1, UniSA, LDO	42

Focus on

Spoke 5 - Cryptography and Distributed Systems Security

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

Thematic Area		Spoke / Affiliated	#scholars
1	Human, Social, and Legal Aspects	**CNR**, UniBO, UniCA, UniFI, UniGE, UniMI	45
2	Trust, Misinformation, and Fakes	**UniSA**, CNIT, CNR, IMT, UniCA, UniMI, UniRoma1, UniVE, ENI	44
3	Attacks and Defences	**UniCA**, CNR, SSSA, UniBA, UniCAL, UniGE, UniRoma1, UniSA, UniVE ENI, LDO, TIM	54
4	Operating Systems and Virtualization Security	**iGE**, CNIT, CNR, CINI, FBK, FUB, IMT, UniCAL, UniRoma1, UniSA, Fincantieri, LDO	52
5	**Cryptography and Distributed Systems Security**	**UniCAL**, CNR, FBK, PoliTO, UniCA, UniSA, Deloitte, ISP	38
6	Software and Platform Security	**UniVE**, IMT, UniBA, UniCA, UniFI, UniRoma1, UniSA, Deloitte	32
7	Infrastructure Security	**PoliTO**, CNR, CINI, FUB, IMT, SSSA, UniCA, UniGE, Deloitte, LDO, TIM	52
8	Risk Management & Governance	**UniBO**, CNIT, CNR, PoliTO, UniBA, UniFI, UniGE, UniMI, Deloitte	58
9	Securing Digital Transformation	**UniRoma1**. CNR, UniBA, UniCA, UniGE, UniMI, UniSA, ISP, TIM	35
10	Data Governance and Protection	**UniMI**, UniCA, UniFI, UniRoma1, UniSA, LDO	42

Spoke 5 - Cryptography and Distributed Systems Security (UNICAL)

Coordinator: Francesco BUCCAFURRI, Full Professor, affiliated to UNICAL

- *Secure and TRaceable Identities in Distributed Environments (STRIDE)*
  - **PI**: Francesco BUCCAFURRI, Full Professor, affiliated to UNICAL

UNIVERSITÀ DELLA CALABRIA

Spoke 5 - overview

- **Main goal** - support the secure, protected, and accountable *identification* and *authentication/authorization* of entities and actions including objects and humans across physical and virtual domains
- The **distributed nature of cyberspace** requires the use of different **security mechanisms, services and technologies** to achieve the goal, including
  - Cryptography
  - Distributed Ledger Technologies (DLTs), blockchain and smart contracts
  - Anonymous identity, identity protection in distributed environments, self-sovereign identity, process tracing, …

Workpackages

- **WP1** - Cryptographic mechanisms
  - Task 1.1 - Cryptographic solutions for access control
  - Task 1.2 - Cryptographic mechanisms for distributed environments
- **WP2** - Blockchain and other distributed technologies
  - Task 2.1 - Security of blockchain-based solutions
  - Task 2.2 - Identification and access control
- **WP3** - Evolutionary changes and challenges for secure digital identity
  - Task 3.1 - Beyond identity of humans, anonymity, and user-centric management
  - Task 3.2 - Advanced and quantum-safe solutions for digital identity and digital tracing

Selected research topics

- Self Sovereign Identity
  - Verifiable credentials are accepted only if issued by trusted entities: how to know their trustworthiness?
  - Cryptographic mechanisms for the selective disclosure of Verifiable credentials
- PUF-based authentication mechanisms
  - PUF-based identities for IoT devices (in supply chains)
- Cryptographic Solutions for Access Control
  - Privacy preserving storage, transmission, and processing of data in the cloud
- Security testing of Digital Identity Ecosystems
  - National digital identity infrastructures require extensive and continuous testing plans to be conducted automatically

Selected research topics (2)

- ???
- See slide decks in PP