Course Syllabus for
Electrical and Information Engineering PhD or Industry 4.0 PhD
(years 2022-23 /2023-24)

Course title	**Emerging methodologies and technologies for the Cyber Security**
Scientific Discipline Sector	ING-INF/03
Hours of instruction	20 hours
CFU	2 CFU
Semester	Second semester
Goal	The course illustrates the emerging methodologies and technologies for the cyber security, with particular focus on (i) Internet, wireless and mobile networks, (ii) Cyber-Physical Systems and Social Internet of Things, (iii) Digital Service Chains, (iv) advanced mechanisms for data protection, user authentication, and access control, (v) Blockchain and examples.
Syllabus	Internet security · transport layer security (TLS 1.2, TLS 1.3, DTLS), object security (COSE and OSCORE), emerging AAA systems Wireless and mobile security · IEEE 802.11 security (IEEE 802.11i framework, WPA2, WPA3, personal vs enterprise configurations) · IEEE 802.15.4 security, configure security in real scenario, the IoT use case, protocol configuration, security framework, key management, implicit X 509 certificates · 5G security Identity and access control management and data protection · AuthZ and AuthN services, NIST model, IBAC, RBAC, ABAC, data protection with identity and attribute encryption (ABE, CP-ABE, DMA-CP-ABE) · solutions for federated and cloud-based systems Social Internet of Things and Digital Service Chains · Concepts, definitions, emerging security framework · Blockchain, definitions, technical details, usage · H2020 GUARD, presentation of the cybersecurity framework to guarantee reliability and trust for digital service chains
Bibliography	Scientific papers suggested by the lecturer Slides and support material from lecturer
Examination method	Final examination in class