Luiss
School of Government

Luiss Guido Carli:
Cybersecurity: Understanding Technical, Legal and Management Issues

Prof. Antonio Gullo, Prof. Paolo Spagnoletti

LUISS

Course's details

Course's title	**Cybersecurity: Understanding Technical, Legal and Management Issues**
Length	From Monday 26th April until Friday 14th May - every day from Monday to Friday
Time	9h30 – 13h30 CET

About the programme

Cybersecurity is an essential capacity for the sustainable growth of any digitally-enabled environment. Digital technologies offer new opportunities for achieving economic development and wealth to people and institutions joining the cyberspace. However, a lack of security in digital ecosystems generates pitfalls and social vulnerabilities such as frauds, service breakdowns and disruptions in political and democratic stability. Therefore, building a cybersecurity capacity entails both the protection of digital infrastructures and the defence of national and economic security while ensuring respect for human rights.

There is general agreement that cyber capacity is about achieving resilience against internet-based threats through a broad range of policies which include the creation of national cybersecurity strategies, computer security incident response teams (CSIRT), the strengthening of cybercrime laws, the promotion of public–private partnerships, and improved education and awareness. Moreover, the institutional development of skills and knowledge on cybersecurity technologies and practices positively impact cyber capacity building.

The program on "Cybersecurity: Understanding Technical, Legal and Management Issues" provides an in-depth understanding on the multi-faceted nature of cyber risk in digitally-enabled societies. The course adopts a multi-disciplinary approach to focus on cybersecurity as a key driver for sustainable growth. The international relations, legal, management and engineering perspectives are adopted to analyse the evolution of cyber-threats, the legal frameworks and institutions implementing national and transnational governance on cybersecurity, organizational and interorganizational processes and practices to protect digital assets in businesses and public administrations and advanced technologies to design secure infrastructures and support different phases of cybersecurity operations such as cyber-intelligence and digital forensics.

The course is structured in three weekly modules. Each module is self-consistent and covers a specific objective. The first module focuses on cyber awareness and covers the essentials notions for understanding cyber-risk as a phenomeon that spans from sw vulnerabilities to global infrastructures and institutions. The second module provides a more detailed view on cyber-attacks and cyber-security controls to prevent incidents in critical infrastructures. The third module aims focuses on cyber preparedness and addresses specific legislations, technological trends and practices to improve response capabilities.