Preparazione e mindfulness per la (tras)formazione digitale

Formazione come leva strategica di cyber resilienza

Prof. Paolo Spagnoletti

LUISS

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

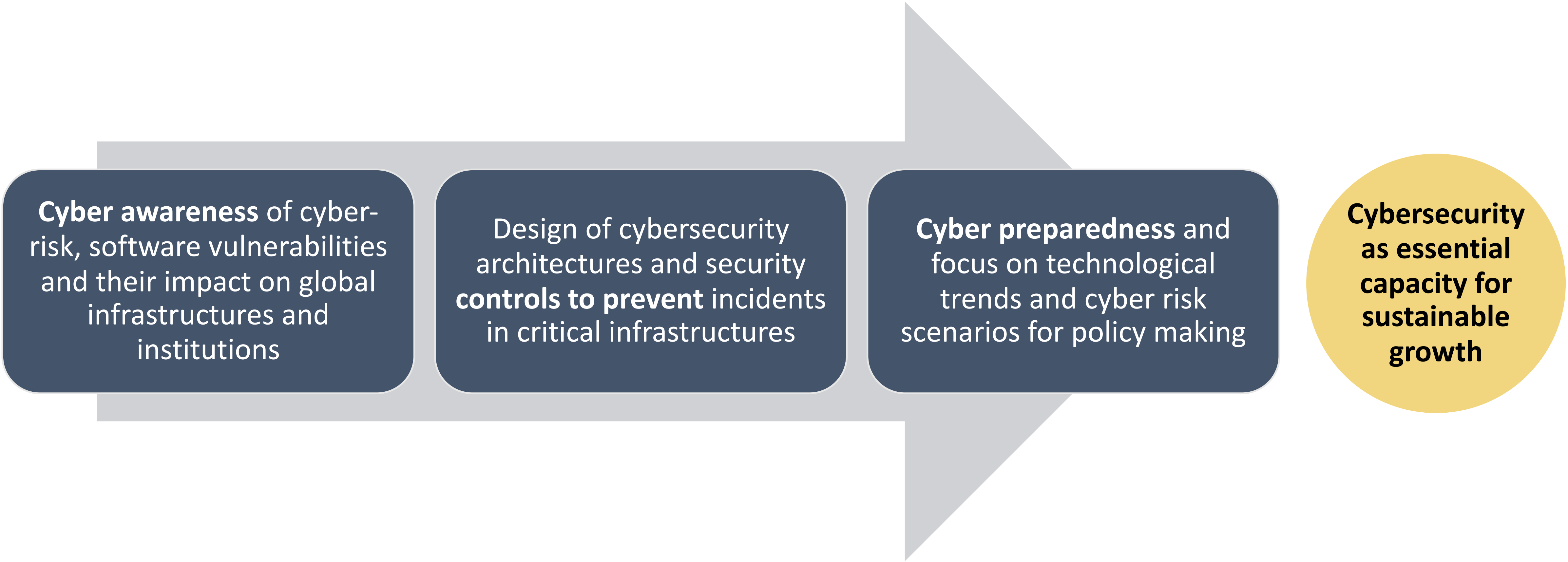
Agenda

- Capacità organizzative per la cyber resilienza
- Metodi e modelli educativi

Capacità organizzative per la cyber resilienza

Requisiti per la formazione e il training

Il valore della cyber resilienza



Cyber awareness of cyber-risk, software vulnerabilities and their impact on global infrastructures and institutions

Design of cybersecurity architectures and security **controls to prevent** incidents in critical infrastructures

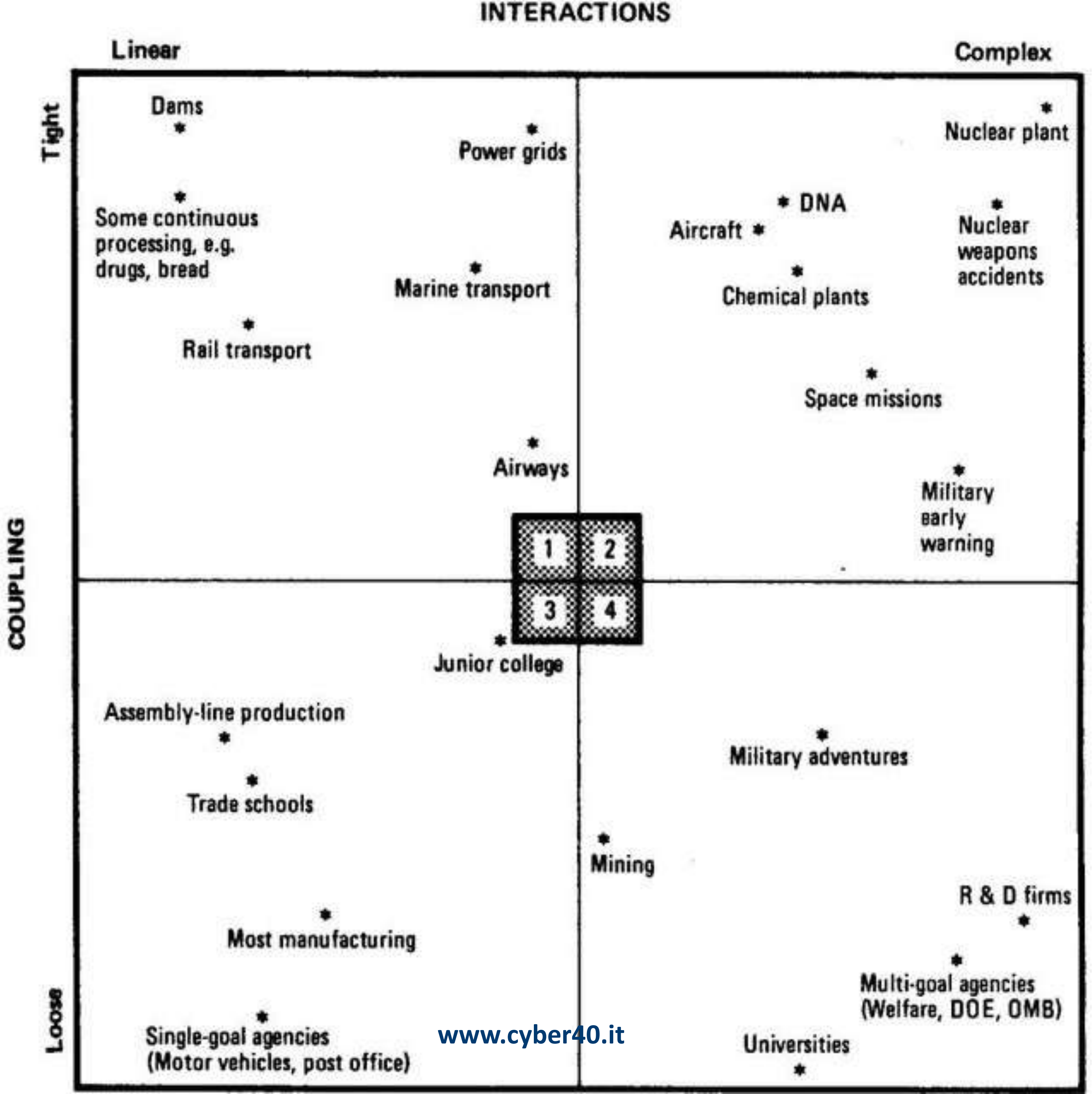
Cyber preparedness and focus on technological trends and cyber risk scenarios for policy making

Cybersecurity as essential capacity for sustainable growth

Normal Accident Theory

- Interactive complexity and tight coupling of technological systems
- Localized failures spread/disrupt/damage larger systems
- System accidents are inevitable or “normal”

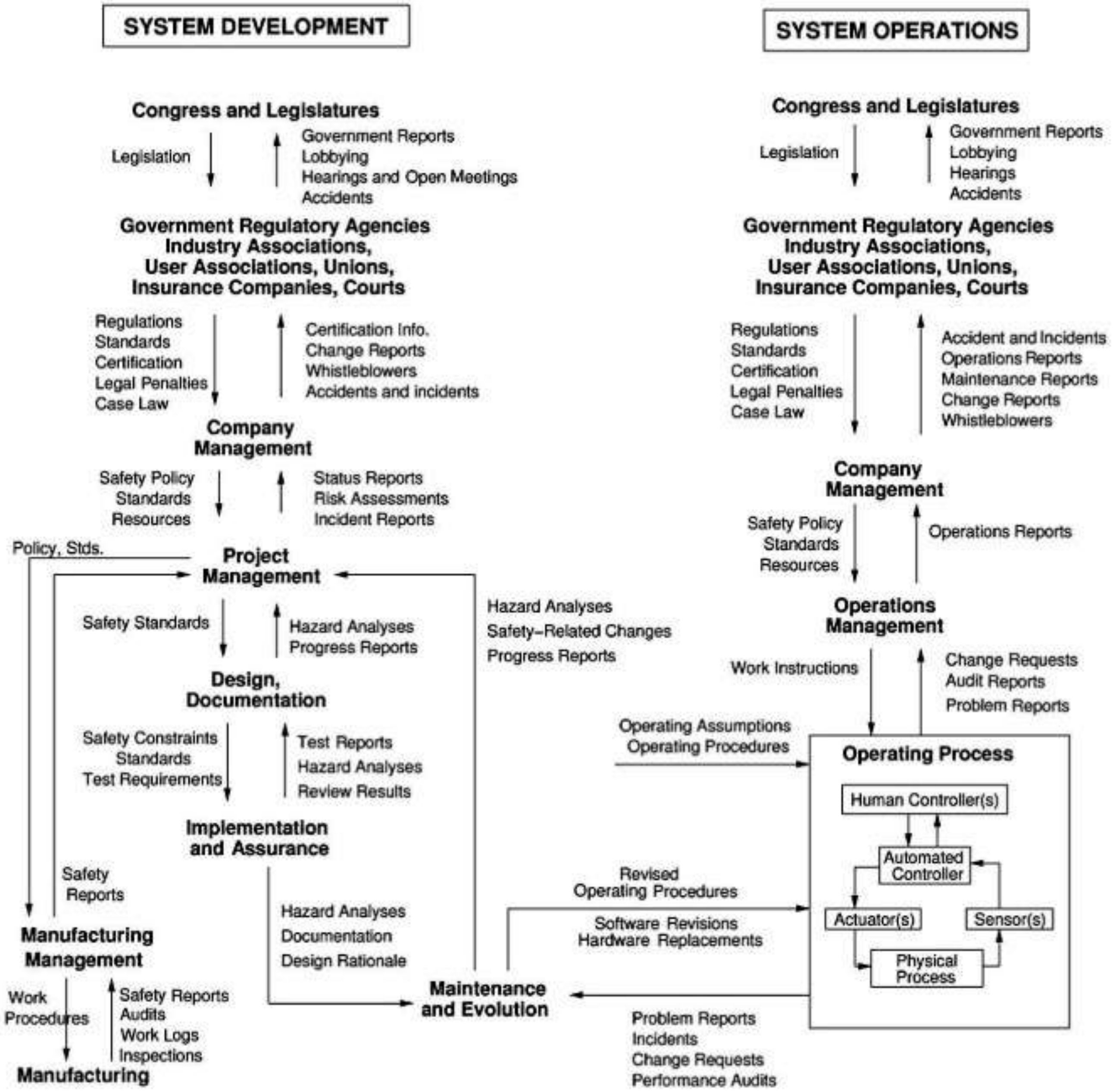
1984



Safety Engineering

- The problem of ensuring safety can be stated as a *control problem* rather than a component failure problem

- accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately controlled or handled



SYSTEM DEVELOPMENT

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and Open Meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal Penalties
Case Law

Certification Info.
Change Reports
Whistleblowers
Accidents and incidents

Company
Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, Stds.

Project
Management

Safety Standards

Hazard Analyses
Progress Reports

Hazard Analyses
Safety-Related Changes
Progress Reports

Design,
Documentation

Safety Constraints
Standards
Test Requirements

Test Reports
Hazard Analyses
Review Results

Implementation
and Assurance

Safety
Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing
Management

Work
Procedures

Safety Reports
Audits
Work Logs
Inspections

Manufacturing

Maintenance
and Evolution

SYSTEM OPERATIONS

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal Penalties
Case Law

Accident and Incidents
Operations Reports
Maintenance Reports
Change Reports
Whistleblowers

Company
Management

Safety Policy
Standards
Resources

Operations Reports

Operations
Management

Work Instructions

Change Requests
Audit Reports
Problem Reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated
Controller

Actuator(s)

Sensor(s)

Physical
Process

Revised
Operating Procedures

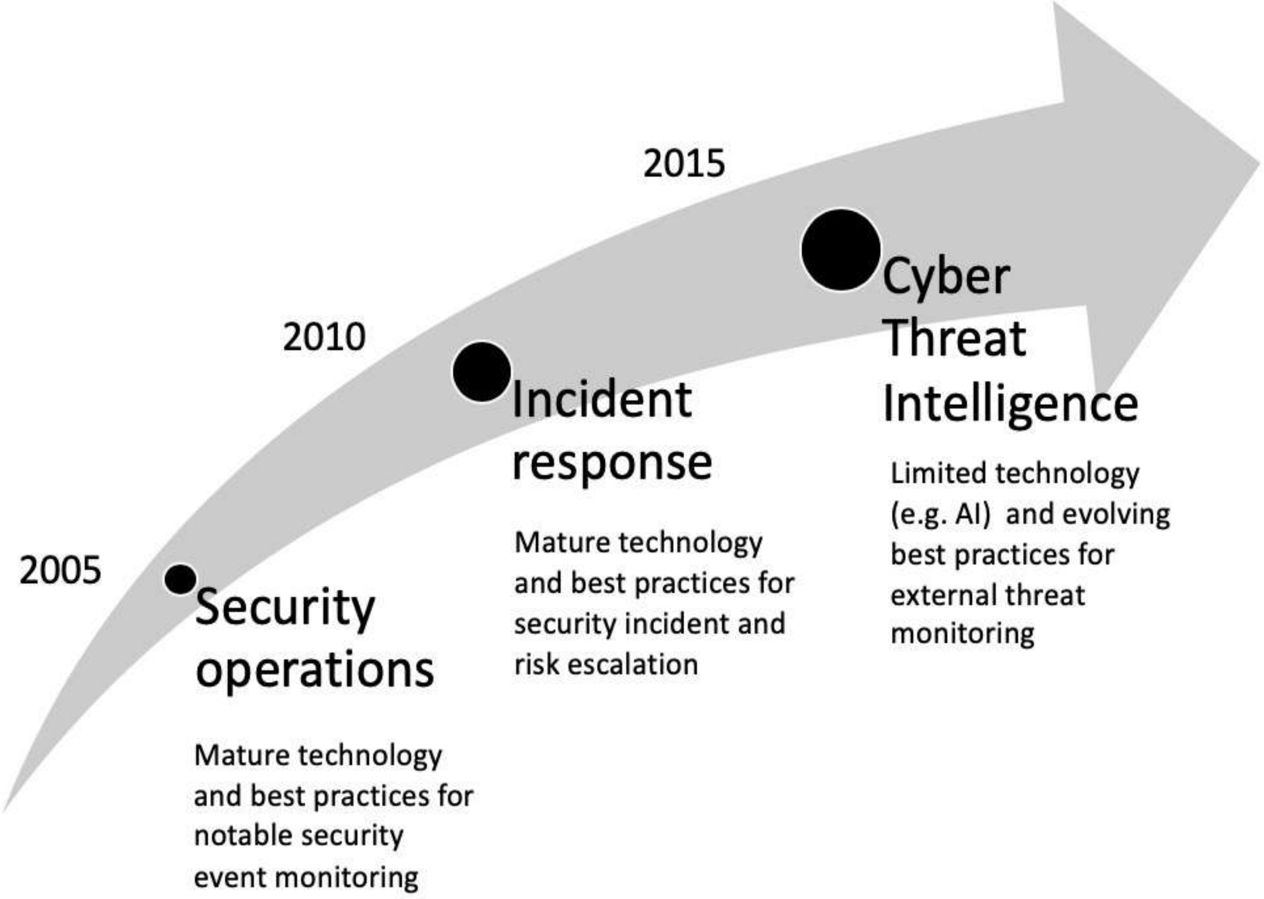
Software Revisions
Hardware Replacements

Problem Reports
Incidents
Change Requests
Performance Audits

Leveson et al. 2009

Le capacità organizzative per la cyber resilienza

- Capacità di prevenire incidenti attraverso controlli di sicurezza a carattere deterrente e preventivo
- Capacità di risposta per ridurre l’impatto di incidenti con azioni che limitano i danni provocati da databreach (es. detection, incident management)
- Capacità di innovazione per adattarsi all’ambiente e alle nuove minacce



Mature technology and best practices for notable security event monitoring

Mature technology and best practices for security incident and risk escalation

Limited technology (e.g. AI) and evolving best practices for external threat monitoring

Le sfide per una efficace resilienza cyber

FORMAZIONE

- *Pratiche gestionali «agili»* da adattare al contesto
  - Security studies and capacity building; Criminal law and GDPR; Organizational processes and practices; Security economics and behavior; Technologies for data security
- *Agilità* a livello strategico, tattico e operativo
  - Softskills per bricolage, improvisation, hacking (es. design thinking)
  - Enterprise architecture maintenance and evolution (es. scenario modelling)

TRAINING

- *Collective mindfulness* nel controllo delle operation
  - Preoccupation with failure, Reluctance to simplify, Sensitivity to operations, Commitment to resilience, Deference to experience
  - Active defense: digital twins, sandboxes, AI, etc.
- Capacità di *gestione delle crisi*
  - Fragmented coordination
  - Scenario based training for situational understanding

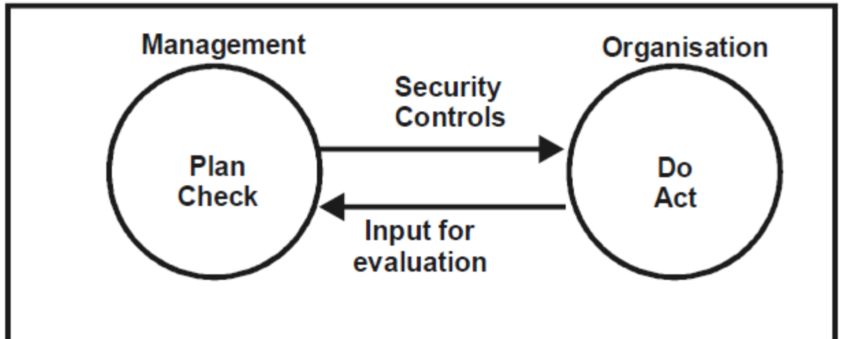


Figure 1.Common stages of an ISMS

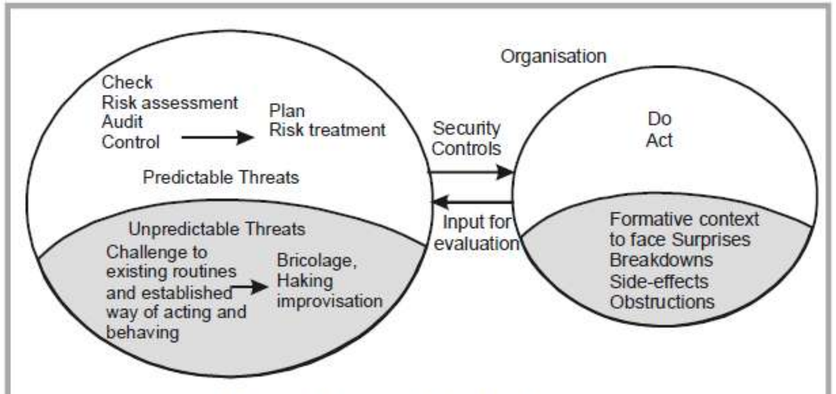


Figure 3.The duality of IS security

Spagnoletti and Resca 2008

Metodi e modelli educativi

Iniziative a confronto

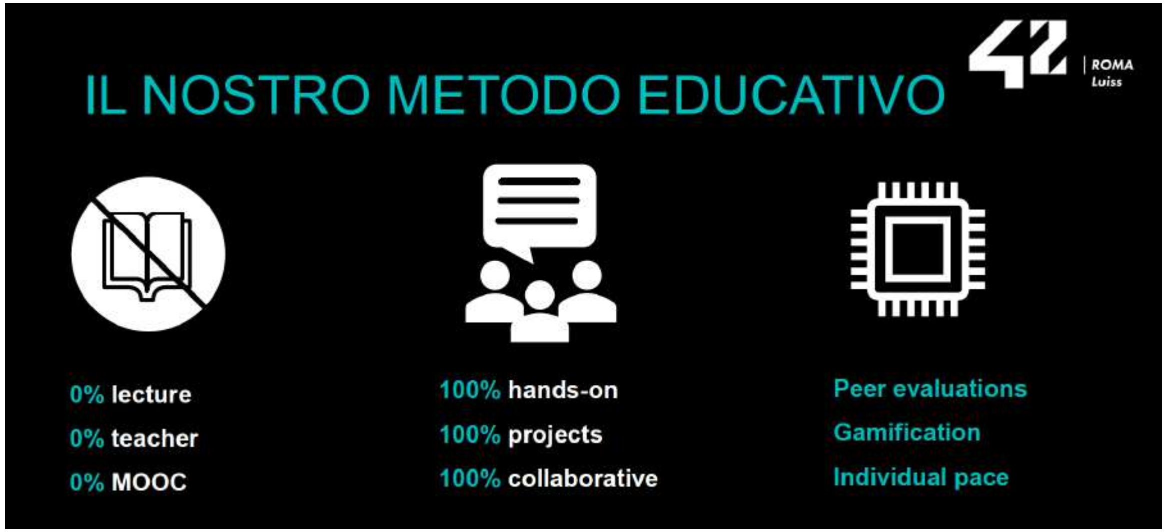
Trends in education

- Enquiry-based learning
- Interdisciplinary
- Design thinking
- Growth mindset
- Continuous assessment

42 Roma Luiss

- il sistema di apprendimento prende spunto dai **metodi Freinet e Montessori**, ma anche dal sistema di educazione finlandese
- applicazioni pratiche, metodologie di problem-solving permettono - a gruppi di età misti - di costruire una formazione personalizzata, puntando sull'auto-appropriazione della conoscenza
- pensiero critico, problem-solving, creatività

42ROMA



IL NOSTRO METODO EDUCATIVO

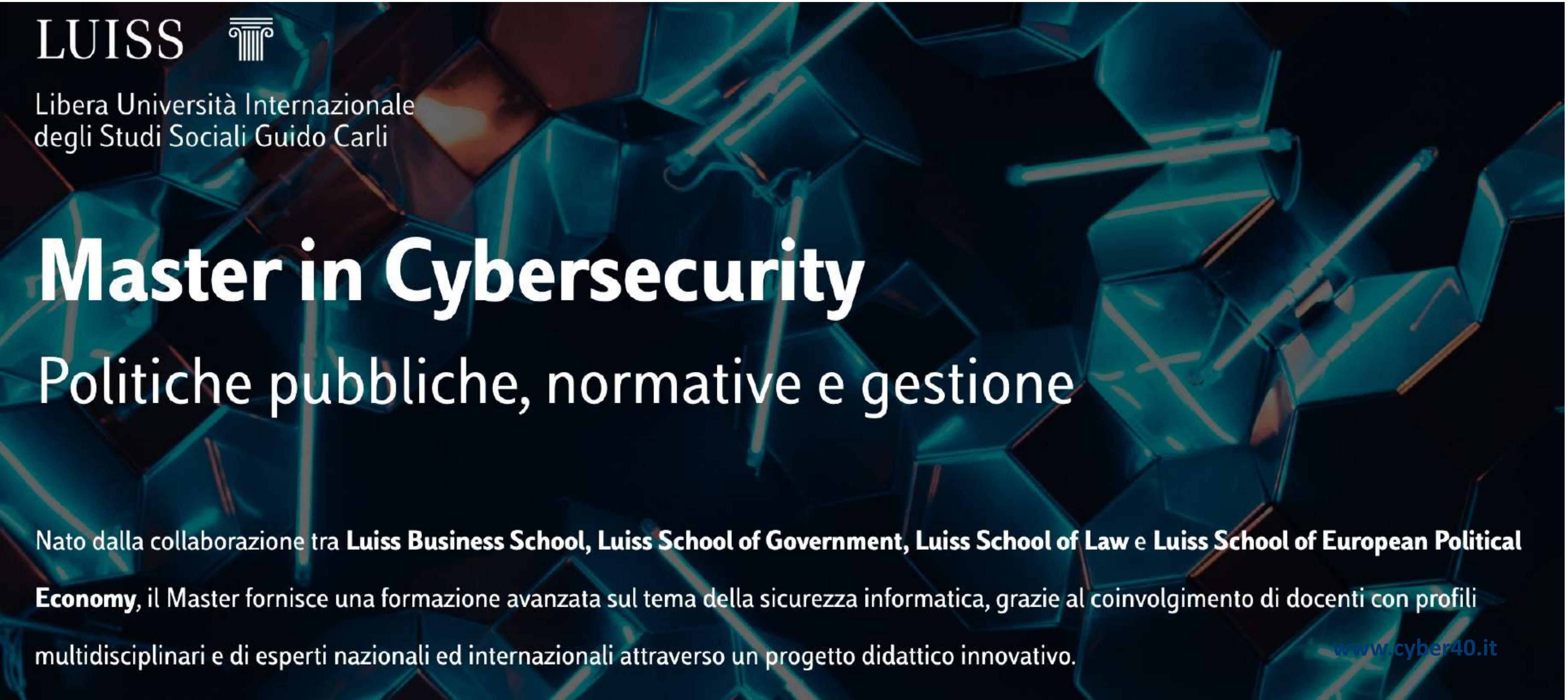
42 | ROMA Luiss

0% lecture
0% teacher
0% MOOC

100% hands-on
100% projects
100% collaborative

Peer evaluations
Gamification
Individual pace

VI edizione, 200+ domande di ammissione, 60% background scienze sociali, gender balance, corsi di specializzazione collegati (es. NFT), 90% lavorano entro 3 mesi



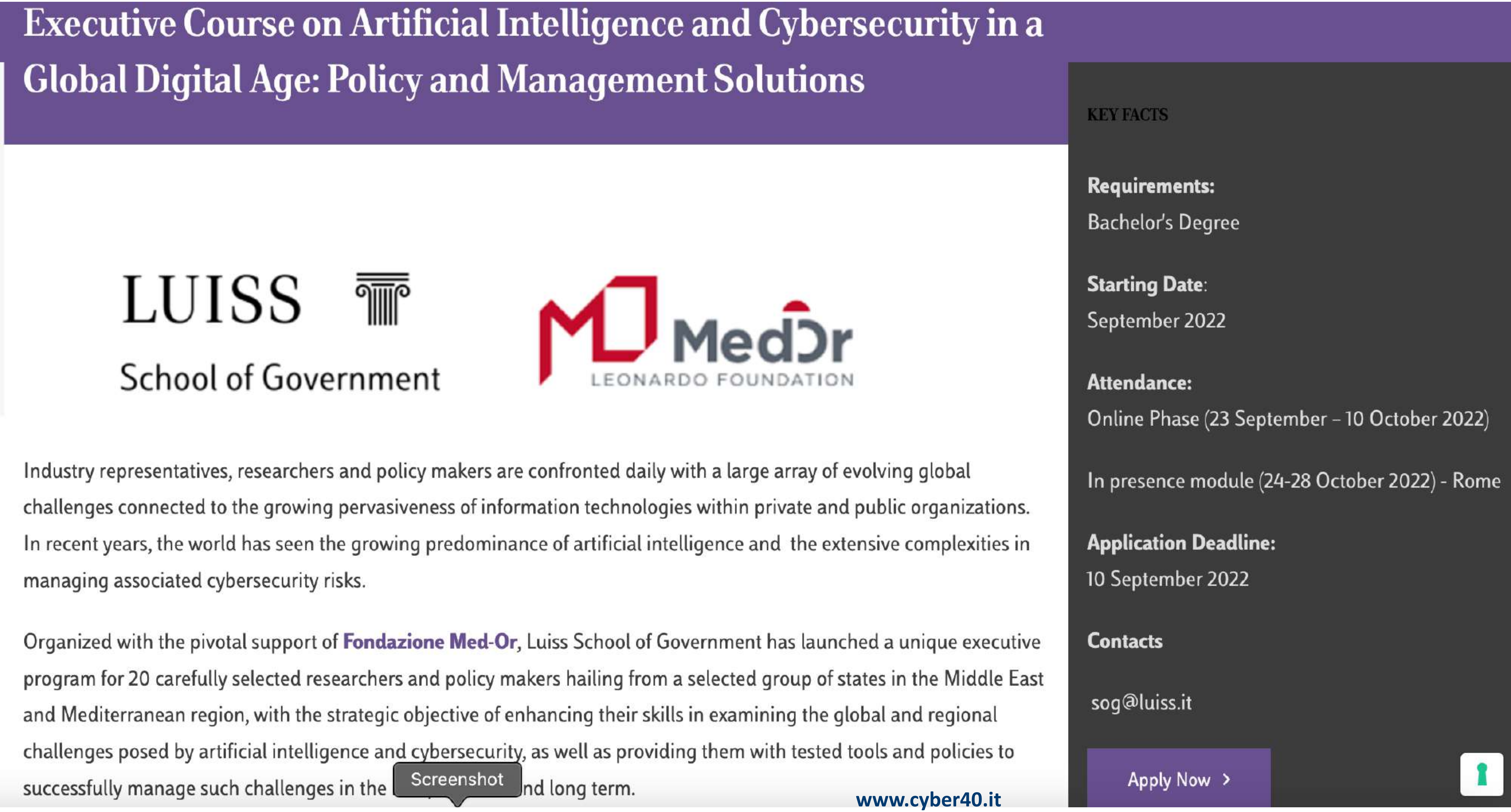
LUISS

Libera Università Internazionale
degli Studi Sociali Guido Carli

Master in Cybersecurity

Politiche pubbliche, normative e gestione

Nato dalla collaborazione tra **Luiss Business School, Luiss School of Government, Luiss School of Law** e **Luiss School of European Political Economy**, il Master fornisce una formazione avanzata sul tema della sicurezza informatica, grazie al coinvolgimento di docenti con profili multidisciplinari e di esperti nazionali ed internazionali attraverso un progetto didattico innovativo.



Executive Course on Artificial Intelligence and Cybersecurity in a Global Digital Age: Policy and Management Solutions

LUISS School of Government

MedOr LEONARDO FOUNDATION

Industry representatives, researchers and policy makers are confronted daily with a large array of evolving global challenges connected to the growing pervasiveness of information technologies within private and public organizations. In recent years, the world has seen the growing predominance of artificial intelligence and the extensive complexities in managing associated cybersecurity risks.

Organized with the pivotal support of **Fondazione Med-Or**, Luiss School of Government has launched a unique executive program for 20 carefully selected researchers and policy makers hailing from a selected group of states in the Middle East and Mediterranean region, with the strategic objective of enhancing their skills in examining the global and regional challenges posed by artificial intelligence and cybersecurity, as well as providing them with tested tools and policies to successfully manage such challenges in the nd long term.

KEY FACTS

Requirements:

Bachelor's Degree

Starting Date:

September 2022

Attendance:

Online Phase (23 September – 10 October 2022)

In presence module (24-28 October 2022) - Rome

Application Deadline:

10 September 2022

Contacts

sog@luiss.it

Finanziato dall'Unione europea
NextGenerationEU

MUR

LUISS
University - Rome

SAPIENZA
UNIVERSITÀ DI ROMA

9 PhD Positions in Cybersecurity with Scholarship

Joint PhD Luiss – Sapienza

Duration: 3 years (Nov 2022 – Nov 2025)

Two of nine scholarships funded by Luiss with NRRP funds

Administrative Headquarters: Sapienza University of Rome

Workplaces: Luiss University, Rome;
Sapienza University of Rome

Visiting research period abroad: up to 12 months

Application deadline:
25 August 2022, 14:00 CEST

Scientific coordinator:
Prof. Leonardo Querzoni, Sapienza University of Rome

Luiss Academic Advisor: Prof. Paolo Spagnoletti

www.cyber40.it

Grazie per l’attenzione

http://www.linkedin.com/in/pspagnoletti

LinkedIn

Letture di approfondimento

Baldoni, R., De Nicola, R. Prinetto, P. (2018) Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici (a cura di), CINI Cybersecurity National Lab https://www.consorzio-cini.it/index.php/it/news-ita/100-eng/eng-laboratori/eng-lab-cyber-security/eng-lab-cyber-security-news/1249-libro-bianco-della-cybersecurity

Baskerville, R., P. Spagnoletti, and J. Kim (2014) “Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response.” Information & Management 51 (1): 138–51. https://doi.org/10.1016/j.im.2013.11.004.

Marchetti R., Mulas R. (2017) Cyber Security: Hacker, terroristi, spie e le nuove minacce del web, LUISS University Press

Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: integrating digital twins in the electric power ecosystem. *Computers & Security*, 102507. https://doi.org/10.1016/j.cose.2021.102507

Severino, P. (2017) La criminalità informatica: nuovi rischi da affrontare e prevenire, http://open.luiss.it/2017/09/08/la-criminalita-informatica-nuovi-rischi-da-affrontare-e-prevenire-lintervento-di-paola-severino/

Spagnoletti, P., and A. Resca. (2008) “The Duality of Information Security Management: Fighting against Predictable and Unpredictable Threats.” Journal of Information System Security 4 (3): 46–62. http://eprints.luiss.it/955/.