

Hacking, Hustle & AI: The business of Cybercrime in the age of Artificial Intelligence.

This talk traces the transformation of hacking from a 1980s–90s hobbyist pursuit into today’s professionalized, monetized cybercrime economy, and then examines how artificial intelligence reshapes both offense and defense. It is organized in three parts.

Part One reconstructs the history and business models of cybercrime, including the underground black market, the Russian Business Network model, the command chain, the 0-day lifecycle, dark-web marketplaces (Silk Road and Italian storefronts), and money-laundering mechanisms such as the hawala system, illustrating a criminal market whose estimated value now rivals or exceeds the global drug trade.

Part Two introduces the conceptual stack of modern AI data science, machine learning, deep learning, and generative AI, and critically probes where and whether these techniques actually help in security, arguing through a real penetration-test case study that much attack activity leaves no data to learn from.

Part Three demonstrates the security fragility of AI systems themselves, showing how the guardrails of a conversational model can be circumvented through adversarial prompting, framed as a cautionary awareness exercise on the dual-use risks of generative AI.

Learning Objectives

By the end of the session, participants will be able to:

- Describe how cybercrime evolved from recreational hacking into an organized, profit-driven ecosystem, and characterize its principal actors and business models.
- Explain the economic scale of the underground market and the structural factors — invisibility, perceived untouchability, low effort/high yield, geographic reach, and global cooperation — that make cybercrime attractive.
- Distinguish the surface web from the deep and dark web, and identify the categories of goods and services traded illicitly, along with laundering techniques such as hawala.
- Differentiate data science, machine learning, deep learning, generative AI, and “AI” proper, and articulate what each can and cannot realistically contribute to cybersecurity.
- Critically assess the limits of data-driven defense, recognizing that many attacks generate little or no exploitable data.
- Understand that AI systems are software artifacts and therefore attackable and appreciate the dual-use and ethical risks of generative models, including prompt-based safety bypasses.
- Recognize the ethical, privacy, governance, and human-dignity principles that should guide the design and deployment of AI.



Prof. Claudio Cilli

CGEIT, CRISC, CISA, CISM

Prof. Claudio Cilli is a recognized world leading authority in the areas of National Security and Intelligence, company protection, information systems security and compliance, with over 30 years of experience. He currently advises governments and int'l companies in the cyber-security and critical infrastructures protection areas.

University professor and researcher. Lesson arguments include: computer science, software compilers, lexical and semantic analyzers, information systems analysis and development. Member of the scientific and advisory boards. Teacher in the post-graduate master's in computer security and IT Governance.

Consultant to the U.S. Government and companies who supply the Department of Defense. Consultant at the United Nations. With many big firms, he is responsible of IS Audit and security projects, which include civil and military sectors, software quality and code security, security of the information systems and installations. Designed and implemented systems based on mainframes and distributed architecture, including Disaster Recovery and both data and physical security, information and site protection.