MODULE DESCRIPTION CARD – SYLLABUS

This module is a part of the Intensive International Education Programs in the field of Cybersecurity organised at Poznan University of Technology as part of the „IMPACT – Innowacyjne Międzynarodowe Programy w AI, Cyberbezpieczeństwie i Teleinformatyce" project implemented SPINAKER Program of the National Agency for Academic Exchange, financed by the European Social Development Fund 2021–2027 (ESDF).

Module name:	Number of hours:	Lecturer:
Cybersecurity in a Hyper-Connected World	10	Prof. Mariusz Głąbowski

Module Descriptions:

This module introduces students to cybersecurity challenges and defence principles in highly interconnected digital ecosystems shaped by IoT, 5G, cloud computing, and edge architectures. As digital infrastructures become globally distributed and interdependent, security threats increase in scale, speed, and complexity. The module examines technologies, attack vectors, security architectures, and governance models required to protect hyper-connected environments.

Topics include IoT and edge computing architectures, securing connected devices, network segmentation, Zero Trust Architecture (ZTA), cloud security fundamentals, federated identity and access management, supply chain security, privacy risks, and the SAGSIN model—an emerging conceptual model for designing secure architectures in hyper-connected systems.

Case studies from real-world incidents illustrate how vulnerabilities propagate across interconnected infrastructures and how appropriate mitigation strategies can be designed.

Purpose of the support under Module:

The module supports the goals of the IMPACT program by developing competencies in cybersecurity for next-generation digital infrastructures. The specific objectives include:

- Understanding the principles of hyper-connectivity, IoT, 5G, cloud, and edge systems.
- Identifying threats and attack vectors characteristic of interconnected environments.
- Applying security controls for IoT ecosystems and connected devices.
- Learning network security strategies, including segmentation and Zero Trust Architecture.
- Understanding cloud security fundamentals and shared responsibility models.
- Using federated identity and access management to secure distributed systems.
- Learning the SAGSIN model for resilient, secure architectures in hyper-connected systems.
- Recognising supply chain security risks, dependencies, and mitigation frameworks.
- Understanding privacy challenges created by pervasive sensing and data flows.
- Analysing real-world cyber incidents to extract security lessons for modern infrastructures.

Method of support under Module:

Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;
- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;
- a test to verify the acquisition of competences.

Module-related learning outcomes:

Knowledge:

Upon successful completion, the student:

1. Understands the concept of hyper-connectivity and the functioning of IoT, 5G, edge, and cloud technologies.
2. Knows the primary threats and attack vectors affecting interconnected digital ecosystems.
3. Understands the principles and challenges of securing IoT devices and low-power embedded systems.
4. Knows the fundamentals of network segmentation, micro-segmentation, and Zero Trust Architecture (ZTA).
5. Understands cloud security foundations, shared responsibility models, and common risks.
6. Has knowledge of federated identity and access management approaches in distributed systems.
7. Understands the SAGSIN model and its application in building secure, resilient architectures.
8. Recognises supply chain security challenges and the cascading impact of upstream compromises.
9. Understands privacy risks posed by pervasive data collection and ubiquitous connectivity.
10. Knows major real-world cybersecurity incidents and their relevance to hyper-connected system defence.

Skills:

The student:

1. Can identify vulnerabilities across IoT, cloud, and edge components and map potential attack vectors.
2. Can propose segmentation and Zero Trust strategies for securing interconnected systems.
3. Can evaluate cloud environments for basic security requirements and mitigation strategies.
4. Can apply federated identity models and access control principles to distributed infrastructures.

5. Can analyse supply chain dependencies and propose risk mitigation approaches.
6. Can evaluate privacy impacts of hyper-connected system deployments.
7. Can interpret real-world cyber incidents to derive lessons for system design and governance.

Social competences:

The student:

1. Understands the ethical, privacy-related, and societal implications of pervasive connectivity.
2. Recognises the need for secure-by-design thinking in complex, distributed digital environments.
3. Appreciates interdisciplinary collaboration required to secure next-generation infrastructures.
4. Is aware of global interdependencies and the importance of cyber resilience and trust frameworks.

Criteria for verifying learning outcomes

Learning outcomes of the course are verified via an assessment test.

Method of verification/validation of learning outcomes

The verification of the learning outcomes is based on answers to the questions in the test. The test is passed if the student answers correctly at least 50% of the questions.

Workload

25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework