Module code	**SEL703**			**Level**	7
Module title	**Cybersecurity**				
Status	Elective				
Teaching Period	Autumn/Spring				
Courses on which the module is taught	All Postgraduate Courses				
Prerequisite modules	No				
Notional learning hours	100	**Credit value**	10	**ECTS Credits**	5
Field trips?	Subject to Industry Conference and Events				
Additional costs	None				
Content notes	Awareness of emotional impact of experienced security threats				

1. Module description

This module will take you to explore the area of cybersecurity and address 'cyber skills' gaps in how security can (be made to) make sense. This is an interdisciplinary and naturally applied field that examines the behaviours, policies and practices around security systems in the context of online environments. This module is built on the foundations of cyberpsychology, digital anthropology and security studies. You may cover topics such as the managing of trust, security technologies, cybercrime, cultures of risk, the psychology of scamming, gaming behaviours, vulnerability and bias in security, cryptosecurity and decentralisation, data hacking, data handling and legal frameworks, online safety and how these reflect in practice. You will explore complex cyber security problems and address the mindsets, legislations and societal challenges around the technologies of value (what is worth securing). This module will provide you with the opportunity to address cyber security challenges providing theoretical and practical cases as well as a broad of perspectives and techniques for evaluating security solutions.

2. Learning Outcomes

Upon successful completion of this module, you will be able to:

Decision Making (RLO4):

Formulate informed decisions on cybersecurity in complex situations using critical and reflexive thinking.

Discipline Skills (RLO8):

Combine and employ advanced discipline-specific knowledge, techniques and tools for practical purposes in the field of cybersecurity.

Human and Environmental Impact (RLO10):

Critically reflect on and evaluate the impact of cybersecurity practices, including your own, on individuals, society, and on the environment**.**

3. Learning and teaching methods, and reasonable adjustments

You will engage in workshops and event that will explore professional and current cases on cybersecurity themes, which will be used for your final assessment. The workshops may take various forms such as masterclasses, guest speakers, forums, field trips, or exhibitions.

Additionally, each week, you will participate seminars that are carefully crafted to enhance your understanding and learning. These seminars will encompass a range of activities, including student-led discussions and presentations, analysis of case studies and dedicated reflection times on the topics being discussed. You will be encouraged to work individually and in groups during these sessions, potentially leading to public presentations of the outputs of those exercises.

Learning hours			**100**
Directed learning			**36**
Workshops/ classes/ seminars/ lead events	Supervision	Studio time	Other
36	0	0	0
Guided/Self-guided learning			64

4. Assessments and weighting, reasonable adjustment, and feedback methods

Assessment component 1: Portfolio, 100% [Portfolio pieces equivalent with 3,500-word critical reflexive report]

You need to prepare a digital portfolio consisting of a minimum of 8 pieces that represent a portfolio of practice of your work during the course. You need to examine your body of work and produce a reflexive report of 3,500 words that critically reflects on any chosen two cases from within the portfolio and the work as a whole.

The portfolio pieces can take various forms (for example and not restricted to, data visualisation, text, images, digital outputs). These pieces will be created weekly within the course as part of you course participation.

Reasonable adjustments for the assessment will be confirmed with students that have a support plan in place.

Mapping of assessment tasks:

Assessment components	**LO4**	**LO8**	**LO10**
Portfolio	x	x	x

The above assessment component is summative. Students will have the opportunity for formative assessment and feedback before each summative assessment.

5. Indicative resources

Norman, K. L. (2017). *Cyberpsychology* (2nd ed.). Cambridge University Press.

Bossomaier, T et al., (2018). *Human Dimensions of Cybersecurity*. Auerbach Publications Hubbard, D. et al., (2016) *How to Measure Anything in Cybersecurity Risk*. Wiley.

Carey, M and Jin, J., (2019) *Tribes of Hackers*. Wiley.

Gene, K., (2019) *The Unicorn Project*. IT Revolution Press

Rochi, W., (2022) *Cybersecurity and Privacy Law Handbook.* Packt Publishing

Hart, D., (2022). *The Cybersecurity Mindset: A Virtual and Transformational Thinking Mode*. Koehler Books

Craft, Z., (2023) *Cybersecurity Essentials for Business Leadership.* Wiley.

Finner, G et al., (2022) *Project Zero Trust: A Story About a Strategy for Aligning Security and the Business*. AudioB

Crespo--Pérez, G. (2021). *Factors that Influence the Cybersecurity Behavior: A Cross-Cultural Study*. ProQuest Dissertations Publishing.

Veale, M. & Brown, I. (2020). *Cybersecurity*. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1533

Vanunu, O et al., (2023) *Cyber and Hacking in the Worlds of Blockchain and Crypto*. Kindle Store

Werback, K., (2018) *The Blockchain and the New Architecture of Trust.* The MIT Press.

Other resources

Global Cyber Security Capacity Centre https://gcscc.ox.ac.uk/

Journals

Journal of Information Assurance & Cybsersecurity - is a peer reviewed international journal presenting scholarly works on information security to the benefit of the industrial and academic community, as well as to the cognizant government agencies. The Journal serves as a forum for authors who wish to present their original scientific findings — theories, methodologies, and applications — to the global information security community.

Journal of Information Security is an international journal dedicated to the latest advancements in information security. The goal of this journal is to provide a platform for scientists and academicians all over the world to promote, share, and discuss various new issues and developments in different areas of information security.

Journal of Cybersecurity Education, Research & Practice (JCERP) is a peer-reviewed scholarly online journal dedicated to promoting scholarship among faculty teaching and researching Cybersecurity topics.

Journal of Cybersecurity publishes accessible articles describing original research in the inherently interdisciplinary world of computer, systems, and information security

Journal of Cyber Security and Information Systems by the Cyber Security & Information Systems Information Analysis Center

Computers & Security the international source of innovation for the information security and IT Audit Professional

International Journal of Cyber-Security and Digital Forensics (IJCSDF) is a Peer Reviewed, Refereed, Indexed and Leading Journal in Cyber Security and Digital Forensics

International Journal of Information Security is an English language periodical on research in information security which offers prompt publication of important technical work, whether theoretical, applicable, or related to implementation.

Cybersecurity. Springer Open https://cybersecurity.springeropen.com/about

Computers in Human Behavior is a scholarly journal examining the intersection of technology and human actions, emotions, and social interactions across various disciplines.