Module Descriptor

Title	Cybercrime and Online Risks		
Session	2025/26	**Status**	active
Code		**SCQF Level**	9
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Education and Social Sciences**		
Module Co-ordinator	R Gundur		

Summary of Module

Cyberspace is an immense realm that facilitates communications and actions in a vast array of everyday applications. Cyberspace makes world-crossing connections easy and affords people opportunities to engage and interact in evolving ways. Unfortunately, the opportunities afforded by the internet can also be used for nefarious purposes.

This class is not technical; you do not need any advanced computer skills to succeed. It is designed to provide an overview of cybercrime and how it impacts on people and society more generally. It is designed to equip you with skills that allow you to identify and respond to problems quickly, an asset that will be important in the job market that awaits you.

Upon completion of this module, students will have knowledge regarding:

- some of the many crimes which use cyber technology, either fully or in part, to commission a criminal activity,
- the risks that individuals, companies, and governments face in cyberspace, and
- the difficulties in developing responses to these crimes domestically, regionally, and internationally.

The tasks in this module will teach students how to examine contemporary issues related to cybercrime and risks in cyberspace, analyse quickly evolving dynamics, and produce clear, industry-relevant outputs with that analysis.

Class outline (Subject to change based on contemporary cyber concerns)

1. Introduction: our digital world and how to write an integrated critical commentary
2. What is cybercrime and who does it?
3. Measuring cybercrime and identifying victims
4. Privacy and data breaches
5. Surveillance
6. Cyber-bullying, online harassment, and technology-facilitated coercive control
7. Social engineering
8. Attacking computer systems, ransomware, and critical infrastructure threats
9. The dark web
10. Online extremism, misinformation, and disinformation

11. Emerging threats 12. Regulating cyberspace and responding to cybercrime

Module Delivery Method	**On-Campus**[1] ☒	**Hybrid**[2] ☐	**Online**[3] ☐	**Work -Based Learning**[4] ☐
Campuses for Module Delivery	☐ Ayr ☐ Dumfries	☐ Lanarkshire ☐ London ☒ Paisley	☐ Online / Distance Learning ☐ Other (specify)	

Terms for Module Delivery	Term 1	☒	Term 2	☐	Term 3	☐
Long-thin Delivery over more than one Term	Term 1 – Term 2	☐	Term 2 – Term 3	☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Demonstrate a broad understanding of how internet-connected technologies are and can be used to facilitate the commission of crimes and antisocial behaviour.
L2	Critically assess the development of ICT and the risks they have in terms of facilitating crime and exposing individuals to crime in brief and long-form work-place-style communications.
L3	Identify and engage with publicly available and open-source information and appropriate academic sources regarding past and unfolding cyber and ICT incidents.
L4	Evaluate costs and potential costs of a recent cybercrime attack and ongoing cybercrime and deviant activities and develop mitigation strategies.
L5	Communicate and assess complex information in concise, clear, and professional way for generalist audiences using verbal and written communication strategies.

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	**SCQF 9** Students will demonstrate a knowledge of cybercrime, online deviance, and digital security and privacy that is informed by forefront developments and develop a critical understanding of principles,

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

	concepts, and terminology related to cybercrime, digital spaces, and online deviant behaviour.
Practice: Applied Knowledge and Understanding	**SCQF 9** Students will apply knowledge, skills and understanding in using a range of professional skills and techniques applied to professional-level contexts that include a degree of unpredictability and will practice routine methods of enquiry and research.
Generic Cognitive skills	**SCQF 9** Evaluating a range of sources, students will be able to make both snap and considered judgements regarding routine problems and issues in the context of cybercrime, cybersecurity, and cyberdeviance. Students will also undertake critical analysis of issues and synthesize information from a diverse range of sources
Communication, ICT and Numeracy Skills	**SCQF 9** Students will use a wide range of routine research and communication skills. They will also develop sector-associated skills in terms of searching for information, writing briefs and presenting complex situations to relevant stakeholders.
Autonomy, Accountability and Working with Others	**SCQF 9** Students will demonstrate professionalism, via producing their work on a regular basis, editing their own work, and providing constructive criticism of their peers' work.

Prerequisites	**Module Code**	**Module Title**
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching	
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.	
Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	12
Laboratory / Practical Demonstration / Workshop	24
Asynchronous Class Activity	12
Independent Study	152
n/a	
n/a	
TOTAL	200

Indicative Resources
The following materials form essential underpinning for the module content and ultimately for the learning outcomes: Baker, R. (2023). Deep Dive: Exploring the Real-World Value of Open Source Intelligence. John Wiley & Sons. Bazzell, M. (2022) Extreme Privacy: What It Takes to Disappear. 4th edn.: Independently Published. Lewis, S. J. (ed.) (2017) Queer Privacy: Essays From the Margins of Society: Mascherari Press. Powell, A. and Henry, N. (2017) Sexual violence in a digital age. London: Palgrave MacMillan. Yar, M. and Steinmetz, K. F. (2023) Cybercrime and Society. Fourth Edition edn. Los Angeles: SAGE. n.b., I will use the latest editions available at the time the class runs. These are the current latest editions of these texts. Students will also be required to read blogs and websites such as Wired and Krebs on Security. I will select appropriate blogs based on what is currently being maintained at the time the class runs.
(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements
In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time. **For the purposes of this module, academic engagement equates to the following:** Attending and participating in scheduled on-campus teaching sections, completing asynchronous online activities, and completing and submitting assessments on time.

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Aligned with the overall commitment to equality and diversity stated in the Programme Specifications, the module supports equality of opportunity for students from all backgrounds and with different learning needs. Using Moodle, learning materials will be presented electronically in formats that allow flexible access and manipulation of content. The module complies with University regulations and guidance on inclusive learning and teaching practice. Specialist assistive equipment, support provision and adjustment to assessment practice will be made in accordance with UWS policy and regulations.
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Social Sciences**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**

Module Eligible for Compensation	☒ **Yes** ☐ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	UG Criminology
Moderator	TBC
External Examiner	C. Rhodes
Accreditation Details	
Module Appears in CPD catalogue	☒ **Yes** ☐ **No**
Changes / Version Number	1

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Portfolio
Assessment 2
10 minute presentation
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Portfolio	☐	☒	☒	☒	☒	60	

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Presentation	☒	☒	☒	☒	☒	40	

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	hours

Change Control

What	When	Who
consultation over assessment descriptors	14 March 24	Nick Jenkins
Consulted over SCQF framework descriptors, assessment balance, and volume of assessment	15 March 24	Ian Gillan
Reviewed external feedback	26 Feb 2025	Ian Gillan