SS3503: CRIME, DEVIANCE AND ANTI-SOCIAL BEHAVIOUR IN CYBERSPACE

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Crime, Deviance and Anti-social Behaviour in Cyberspace

Subject Code
SS - Social and Behavioural Sciences
Course Number
3503

Academic Unit
Social and Behavioural Sciences (SS)

College/School
College of Liberal Arts and Social Sciences (CH)

Course Duration
One Semester

Credit Units
3

Level
B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course aims to help students understand cybercrime, including cyber-deviance, crypto-related crimes, money laundering, and digital crime. It explores how new crimes are bred and old crimes and deviant behaviours are facilitated by the Internet. It also examines how cybercrime challenges existing laws and criminal procedures, and delves into issues related to the prevention of crime and deviance in cyberspace, and specifically addresses topics such as crypto-related offenses, money laundering techniques in the digital realm, and other forms of digital crime.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Understand the nature and classification of cybercrime and cyber-deviance;	20		x	
2	Implement sociological and criminological theories to explain cybercrime and cyber-deviance;	20		x	
3	Evaluate the effectiveness of existing counter-measures against cybercrime; and	30	x	x	x
4	Demonstrate the ability to use innovative ways to analyse cybercrime or cyber-deviance and to develop possible preventative measure	30	x	x	x

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	Mini lectures on related topics conducted by the course lecturer are offered to students. One or two guest speakers will be invited as necessary to share their expertise.	1, 2, 3, 4	

2	Group exercises and discussion	Students are encouraged to describe the nature of and explain the underlying factors associated with criminological issues such as cyber-deviance,cybercrime, terrorism, cybercrime prevention and investigation issues.	1, 2, 3, 4	
3	Fieldvisit/ community activity	Students will meet practitioners during their field visits to government departments, private sector organisations or NGOs. They are required to consolidate their observations and write a reflection paper following the visit(s).	1, 3	
4	Group presentation	Students will be divided into groups for presentation purposes. In their presentations, students need to demonstrate critical thinking and creative solutions towards a self-chosen cybercrime or cyber-deviance related issue.	1, 3, 4	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	AT1: Participation	1, 2, 3, 4	15	
2	AT2: Group presentation andproject work	1, 2, 3, 4	35	
3	AT3: Individual papers Reflection papersShort essay	1, 2, 3, 4	50	

Continuous Assessment (%)

100

Examination (%)

0

Assessment Rubrics (AR)

Assessment Task

1. Participation

Criterion

Capability to understand and ability to explain the nature and characteristics of cybercrime andcyber-deviance, and to implement sociological and criminological theories toexplain cybercrime and cyber-deviance

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Not even reaching marginal levels

Assessment Task

2. Group Presentation and Project Work

Criterion

Ability to communicate critical ideas and arguments in evaluating the effectiveness of current legal responses, and to use innovative ways to analyse cybercrime orcyber-deviance with possible preventive measure development, in grouppresentation and relevant project work

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Not even reaching marginal levels

Assessment Task

3. Individual Papers, Reflection Papers, and Short Essay

Criterion

Ability to explain in detail in presenting critical ideas and arguments in evaluating the effectiveness of current legal responses, and to use innovative ways to analyse cybercrime orcyber-deviance with possiblepreventive measure development, in writing

Excellent (A+, A, A-)

High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

Understanding crime and deviance in the digital age
The Emergence of cyberspace and cybercrime
Defining cybercrime and cyber-deviance
Types of cybercrime and cyber-deviance
Legal responses to cybercrime
Preventing cybercrime
Preventing cyber-deviance
crypto-related offenses
money laundering
digital crime
crypto-related offenses, money laundering techniques in the digital realm, and other forms of digital crime

Reading List

Compulsory Readings

	Title
1	Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: Crime and justice in digital society. Routledge.
2	Nagunwa, T. (2014). Behind identity theft and fraud in cyberspace: the current landscape of phishing vectors. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 3(1), 72-83.
3	Jewkes, Y., & Yar, M. (Eds.). (2013). Handbook of Internet crime. Routledge.

Additional Readings

	Title
1	Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. Crime Science, 11, 1-35.
2	Holt, T. J., & Bossler, A. M. (2014). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 35(1), 20-40.
3	Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. Police Practice and Research, 19(6), 519-536.
4	Butler, S. (2019). Criminal use of cryptocurrencies: a great new threat or is cash still king?. Journal of Cyber Policy, 4(3), 326-345.
5	Yar, M. (2013). The global "cybercrime" problem: Definitions, scope, and responses. International Review of Sociology, 23(2), 217-233.

6	Smith, N. R. (2019). International order in the coming cryptocurrency age: The potential to disrupt American primacy and privilege?. Rising Powers Quarterly, 3(1), 77-97.
7	Choi, K. S., & Lee, C. S. (2018). The present and future of cybercrime, cyberterrorism, and cybersecurity. International Journal of Cybersecurity Intelligence & Cybercrime, 1(1), 1-4.
8	Maras, M. H. (2014). The nature, causes, and consequences of cybercrime in college and university communities. Journal of Contemporary Criminal Justice, 30(3), 231-250.