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

Effective Term

Semester A 2023/24

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

SS2030 Introduction to Criminology

Equivalent Courses

Nil

Exclusive Courses

Nil

Part II Course Details

Abstract

This course aims to help students understand cybercrime and cyber-deviance. It discusses how new crimes are bred and old crime and deviance are facilitated by Internet. It also considers how cybercrime challenges existing laws and criminal procedures, and discusses issues related to the prevention of crime and deviance in cyberspace.

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.

Teaching and Learning Activities (TLAs)

	TLAs	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

Reading List

Compulsory Readings

	Title
1	Chang, Y. C. (2012). Cybercrime in the Greater China Region: Regulatory responses and crimeprevention across the Taiwan Strait. Cheltenham: Edward Elgar.
2	Jewkes, Y., & Yar, Majid (Eds.). (2010). Handbook of internet crime. Oregon: Willan.
3	Wall, D. S. (2007). Cybercrime. Cambridge: Polity Press.

Additional Readings

	Title
1	Artick, K. (2006). Cybercrime: The Council of Europe Convention. Washington, DC: TheLibrary of Congress.
2	Bakken, B. (2004). Moral panics, crime rates and harsh punishments in China.Australianand New Zealand Journal of Criminology, 37 (supplement): 67-89.
3	Brenner, S.(2003). Toward a criminal law for cyberspace: Distributed security. BepressLegal Series. Working Paper 15.
4	Brenner, S. (2006). Cybercrime jurisdiction. Crime, Law and Social Change, 46: 189-206.
5	Chang, Y. C. (2011). Cyber-conflict between Taiwan and China. Strategic Insight, 10(1):26-35.
6	Choo, K. K. R. (2008). Organised crime groups in cyberspace: A typology. Trends inOrganized Crime, 11, 270-295.
7	Cohen, S. (1987). Folk devils and moral panics. Oxford: Basil Blackwell.
8	Gorden, S., & Ford, R. (2006) On the definition and classification of cybercrime. Journal inComputer Virology, 2(1): 13-20.
9	Goldsmith, J. T., & Wu, Tim (2006). Who controls the internet? Illusion of a borderless world.New York: Oxford University Press.
10	Grabosky, P. (2007). The internet, technology, and organized crime. Asian Journal ofCriminology, 2, 145-161.
11	Howitt, D. (1998). Crime, the media and the law. Chichester: John Wiley & Sons.
12	McCusker, R. (2007). Transnational organised cyber crime: Distinguishing threat from reality.Crime, Law and Social Change, 46(4-5): 256-273.
13	Sandywell, B. (2006). Monsters in cyberspace cyberphobia and cultural panic in theinformation age. Information, Communication and Society, 9(1): 39-61.
14	Wall, D. (2008). Cybercrime and the culture of fear. Information, Communication and Society,11(6): 861-884.
15	Wilson, C. (2008). Botnet, cybercrime, and cyberterrorism: Vulnerabilities and policy issuesfor congress.Washington, DC: The Federation of American Scientists.
16	Yar, Majid (2005). The novelty of ‘cybercrime’: An assessment in light of routine activitytheory. European Journal of Criminology, 2(4): 407-427.

17	Young, K. S. (2004). Internet addiction: A new clinical phenomenon and its consequences.American Behavioral Scientist, 48(4): 402-415.
18	皮勇（2008）《網路安全法原論》。北京：中國人民公安大學出版社。