O.P. Jindal Global University
A Private University Promoting Public Service
NAAC Accreditation - 'A' Grade

Course Title

INTRODUCTION TO CYBER CRIMINOLOGY

Course Instructor: Ms. Nivedita Salar

Jindal Institute of Behavioral Sciences (JIBS)

4 Credit Course

BE-E-0039

SPRING SEMESTER 2026

Faculty Contact: Nivedita Salar
Email: nivedita.salar@jgu.edu.in
Office Hours: *TBD*
Classroom: *TBD*
The information provided herein is by the Course Coordinator. The following information contains the official record of the details of the course.

PART I

Course Title: Introduction to Cyber Criminology		
Course Code	BE-E-0039	
Course Duration	15 weeks	
No. of Credit Units	4	
Level	UG	
Pre-Requisites	Nil	
Pre-Cursors	Nil	
Equivalent Courses	Nil	
Exclusive Courses	Nil	
Class Timing	*TBD*	

PART II

Course Description:

This 4-credit course will provide an introduction to Cyber Criminology. Cyber Criminology is *"the study of causation of crimes that occur in the cyberspace and its impact in the physical space"* (International Journal of Cyber Criminology, 2007 www.cybercrimejournal.com). As an academic discipline, cyber criminology encompasses a multidisciplinary field of inquiry - criminology, sociology, psychology, victimology, information technology and computer / internet sciences. "At its core, cyber criminology involves the examination of criminal behavior and victimization in cyber space from a criminological or behavioral theoretical perspective". Now, the discipline of cyber criminology is more than ten years old and it has successfully entered the portals of academia in the form of courses starting from minor courses (University of Alabama, Regis University, and Purdue University, USA offer a minor in Cyber Criminology) to Associates in Arts (A.A) Degree (at Arizona Western College, USA).

The course will introduce the participants to history of cyber-crime and cyber criminology, forms of cybercrime (Machine and Human Oriented), theories of cyber criminology and cyber laws. This will be a theoretical course and can be understood without deep technical knowledge of computers.

Course Aims:

- To study the history and evolution of cybercrime and the dynamics of cyber space.
- To understand the forms of cyber crime
- To examine Cyber Criminology as an academic sub-discipline of Criminology.
- To understand the theories of Cyber Criminology

Course Intended Learning Outcomes:

After completing this module, you will be able to understand:

- The dynamics of cyber space in which cyber-criminal interacts with its target.
- The vulnerability of internet user to cyber victimization aroused due to persistent reliance on internet in modern lifestyle.
- History and evolution of cyber-crime.
- Intervention of cyber-crime from individual and international level.
- Forms of cyber-crime, both machine and human oriented.
- The concept, history, evolution and definition of cyber criminology.
- Theories of Cyber Criminology.

Assessment Process:

The course will be majorly taught using class discussions, anecdotes, presentations, readings, and experiential exercises. The evaluations will include in-class activities, individual and group presentations, written assignments, quizzes, and projects. Please note that the assessments listed in the course manual are subject to change. Any changes will be communicated to the class well in advance.

Percentage breakdown of Grade:

Assessment	**Weightage**	**Content**	
Quiz 1	20 points	MCQ and short-answer quiz	**Internal Assessments: 70**
Quiz 2	20 points	MCQ and short-answer quiz	
Class Participation	10 points	Awarded based on class, decorum, & conduct through the length of the course	
Final Exam			**Final exam: 30**

30% End Semester Exam (Closed book and timed)

(*Please note that absenteeism on day of assessment will not be entertained and no assessments shall be rescheduled.)

Grading of Student Assessment

Letter Grade	Grade Value	Grade Points	Interpretation
O	**80 and above**	**8**	**Outstanding:** Exceptional knowledge of the subject matter, thorough understanding of issues; ability to synthesize ideas, rules and principles and extraordinary critical and analytical ability.
A+	**75-79**	**7.5**	**Excellent:** Sound knowledge of the subject matter, thorough understanding of issues; ability to synthesize ideas, rules and principles and critical and analytical ability.
A	**70-74**	**7**	**Very Good:** Sound knowledge of the subject matter, excellent organizational capacity, ability to synthesize ideas, rules and principles, critically analyze existing materials and originality in thinking and presentation
A-	**65-69**	**6**	**Good:** Good understanding of the subject matter, ability to identify issues and provide balanced solutions to problems and good critical and analytical skills.
B+	**60-64**	**5**	**Fair:** Average understanding of the subject matter, limited ability to identify issues and provide solutions to problems and reasonable critical and analytical skills.
B	**55-59**	**4**	**Acceptable:** Adequate knowledge of the subject matter to go to the next level of the study and reasonable critical and analytical skills.
B-	**50-54**	**3**	**Marginal:** Limited knowledge of the subject matter and irrelevant use of materials, and poor critical and analytical skills.
P1	**45-49**	**2**	**Pass 1:** Pass with Basic understanding of the subject matter.
P2	**40-44**	**1**	**Pass 2:** Pass with Rudimentary understanding of the subject matter.
F	**Below 40**	**0**	**Fail:** Poor comprehension of the subject matter; poor critical and analytical skills and marginal use of the relevant materials. Will require repeating the course.

Course Outline

Unit I: History of Cyber Crime and Cyber Criminology (Week 1)

a. Cyber Crime: History and Evolution
b. Cyber Criminology: Evolution, Contribution and Impact

Readings and Reference Material:

1. Diamond, A., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology, 9*, 24-34.
2. Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cyber crime scholarship. *Deviant Behavior, 35,* 20–40. doi:10.1080/01639625.2013.822209
3. Holt, T., & Bossler, A. M. (2016). *Cyber crime in Progress: Theory and Prevention of Technology-enabled Offenses*. Abingdon, Oxon: Routledge.
4. Jaishankar, K. (Ed.) (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal behavior*. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group. ISBN: 9781439829493.

Unit II: Forms of Cyber Crime – Machine Oriented (Week 2 – 3)

a. Hacking
b. Malicious Code - Computer Viruses, Worms, and Trojans
c. Cyber Piracy
d. Cyber Terrorism
e. Cyber Warfare

Reading and Reference Material:

1. Thomas, D. (2002). *Hacker culture*. University of Minnesota Press.
2. Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, 239, 288.
3. Wall, D., & Yar, M. (2010). Intellectual Property Crime and the Internet: cyber piracy and the stealing of Information Intangibles. In Y. Jewkes and M. Yar (eds.), *Handbook of Internet Crimes* (pp. 255-272). Willan Publishing: Devon.
4. Clarke, R., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to do about it*. New York: Harper Collins.
5. Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Project Air Force, RAND Corporation.

Unit III: Forms of Cyber Crime – Human Oriented (Week 4 -6)

a. Cyber Bullying
b. Cyber Stalking
c. Sexting
d. Revenge Porn
e. Online Sextortion
f. Child Pornography
g. Online Child Grooming
h. Identity related Cyber Crimes
i. Cyber Obscenity and Pornography
j. Internet Addiction Disorder (IAD)
k. Online Gambling

Readings:

1. Martellozzo Elena and Emma A. Jane. (2017). *Cybercrime and its Victims*. Abingdon, Oxon: Routledge.
2. Navarro, J. S. Clevenger, and C. D. Marcum. Eds. (2016). *The Intersection between Intimate Partner Abuse, Technology, and Cybercrime: Examining the Virtual Enemy*. Durham, North Carolina: Carolina Academic Press.
3. Schmallager, F., and Pittaro, M. Eds. (2008). *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall.
4. Wall, David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.
5. Yar, Majid. 2013. *Cybercrime and Society*. Second edition. Thousand Oaks, CA: SAGE.

Unit IV: Theories of Cyber Criminology (Week 7-9)

a. Space Transition Theory of Cyber Crimes
b. Routine Activities Theory and Cyber Crimes
c. Social Learning Theory and Cyber Crimes
d. De-Individuation Theory and Cyber Crimes
e. Moral Disengagement Theory and Cyber Crimes

Readings:

1. Agustina, José & Felson, Marcus. (2015). Routine Activities, Delinquency, and Youth Convergences. 10.1002/9781118512449.ch8. *The Handbook of Criminological Theory*, Publisher: Wiley.
2. Bandura, A. (1999). Moral Disengagement in the Perpetration of Inhumanities. *Personality and Social Psychology Review*, *3*(3), 193–209.
3. Chang, J. (Fall, 2008). The Role of Anonymity in De-individuated Behaviour: A Comparison of De-individuation Theory and the Social Identity Model of De-individuation Effects (SIDE). *The Pulse: Undergraduate Journal of Baylor University, 6*(1), 1-8.
4. Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cybercrime causation factors in Ghana. *African Journal of Computing & ICT, 2*(1), 37-48.
5. Holt, T. J., Burruss. G. W., & Bossler, A. (2012). Social learning and cyber-deviance: examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*(2), 31-61.
6. Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In F. Schmallager & M. Pittaro. (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.
7. Wada, F., Longe, & O. Danquah (2012). Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories. *Journal of Internet Banking and Commerce*, *17*(1), 1.
8. Yar, M. (2005). The novelty of 'cyber crime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407-427.

Unit V: Psychology and Cyber Crime (Week 10-11)

a. The Cognitive Revolution: Looking for answers of why good people steal intellectual property
b. The Strategic Role of Thought

Readings:

1. Oliver R. Goodenough, Gregory Decker, J.D. (2010). Why Do Good People Steal Intellectual Property? *Law, Mind and Brain* . Ashgate Press.

Unit Vl: Cyber Laws (Week 12-13)

c. Cyber Offences under the Information Technology Act
d. Cyber Offences under the Indian Criminal Laws

Readings:

2. Duggal, P. (2005). Cyber-Crime in India: The Legal Approach. In Broadhurst R. & Grabosky P. (Eds.), *Cyber-Crime: The Challenge in Asia* (pp. 183-196). Hong Kong University Press. Retrieved from http://www.jstor.org/stable/j.ctt2jc6s1.17
3. Halder, D. (2015). A retrospective analysis of S.66a: Could S.66a of the information technology act be reconsidered for regulating 'bad talk' in the internet? *Indian Student Law Review (ISLR), 3*, 91–118.
4. Pahurkar, P. (2010). Offences and Penalties under the IT Act, 2000. Retrieved from http://www.legalservicesindia.com/article/article/offences-&-penalties-under-the-it-act-2000-439-1.html.
5. The Information Technology Act, 2000 as amended in 2008.
6. The Indian Penal Code (1860).

Professional Conduct in Classroom

You are expected to arrive on time in the classroom and follow the classroom decorum. It is expected that you are punctual in class and be seated immediately within the first two minutes so that the class can start on time. **Students arriving after a ten-minute window from the designated start time will be refused entry/attendance**. You are expected to participate in the classroom discussions, activities and presentation. Participation is essential in this class. You are also expected to be respectful when the instructor is teaching. Furthermore, you are welcomed to share your thoughts in the class but you are expected to do that respectfully and be welcoming of other perspectives in the class even if you disagree with the same.

Notes on Plagiarism

Plagiarism is not acceptable! Please refrain from copying and pasting paragraphs and sentences from your reading materials. This include copying someone's words, structure, grammar, ideas, thoughts, and phrases and passing them as your own. Too many quotes are not acceptable!

What is acceptable? Using one quote which is not more than 40 words with proper citation. Use citation! It's a must! Present the content you read from your reading materials in your own words! Think and critically analyse the content! The source should be always acknowledged in your written material and presentation. All papers in this class will be checked electronically for plagiarism.

Attendance Policy

Students are expected to attend all classes (100% attendance). A student who fails to attend a class is expected to inform the Course Instructor, in writing, the reason for their absence. A minimum of 75% attendance is mandatory, failing which, student is not permitted to take the final/end term exam.

Safe Space Pledge

Some parts of this course may discuss a range of issues that might result in distress for some students. Discussions and images in the course might also provoke strong emotional responses. To make sure that all students collectively benefit from the course, and do not feel troubled due to either the contents of the course, or the conduct of the discussions, it is incumbent upon all within the classroom to pledge to maintain respect towards our peers. This does not mean that you need to feel restrained about what you feel and what you want to say. Conversely, this is about creating a safe space where everyone can speak and learn without inhibition and fear. This responsibility lies not only on students, but also the instructor.

Disability Support and Accommodation Requirements

JGU endeavors to make all its courses accessible to students. All students with a known disability needing academic accommodations are required to register with the Disability Support Committee dsc@jgu.edu.in. The Committee has so far identified the following conditions that could possibly hinder student's overall well-being. These include: physical and mobility related difficulties; visual impairment; hearing impairment; medical conditions; specific learning difficulties e.g. dyslexia; mental health.

The Disability Support Committee maintains strict confidentiality in its discussions. The students should preferably register with the Committee in the first week of the semester as disability accommodation requires early planning. DSC will approve and coordinate all the disability related services such as appointment of academic mentors, specialized interventions and course related requirements such as accessible classrooms for lectures, tutorials and examinations.

All faculty members are required to refer students with any of the above-mentioned conditions to the Disability Support Committee for addressing disability-related accommodation requirements.

Mental Health Support

To book an appointment with Sukoon Health: **+91 8826996393**

Sukoon 24/7 Helpline: **+91 8396907132**