The Hebrew University of Jerusalem

Syllabus

Cyber-Criminology - 61823

Last update 16-09-2019

HU Credits: 2

Degree/Cycle: 2nd degree (Master)

Responsible Department: Criminology

Academic year: 2020

Semester: 1st Semester

Teaching Languages: Hebrew

Campus: Mt. Scopus

Course/Module Coordinator: Michael Wolfowicz

Coordinator Email: michael.wolfowicz@mail.huji.ac.il

Coordinator Office Hours:

Teaching Staff:

Mr. Michael Wolfowicz

Course/Module description:

Like Criminology, Cyber criminology is a multidisciplinary discipline, and includes components from fields such as victimology, sociology and psychology. As we move into the digital age, the field is expanding, and its importance is increasing. In recent years, in many countries, including Israel, there has been a decline in traditional crime. However, some believe that crimes and criminals have migrated to the cyber domain, and that in reality, this decline can be misleading. Cyber crimes can be divided into crimes targeting the digital space itself, as well as crimes that use the digital space as a tool. Cyber related crimes include ordinary crimes that we are all familiar with: property, violence, sexual, drug crime, as well as issues such as terrorism, and national security.

Course/Module aims:

Learning outcomes - On successful completion of this module, students should be able to:

This course will provide students with a broad understanding and appreciation of cybercrime as a discipline, including the application of criminology in theoretical frameworks and methodologies for cybercrime research, an in-depth understanding of the multitude of current topics and trends.

Attendance requirements(%):

100

Teaching arrangement and method of instruction: Frontal

Course/Module Content:

1. Introduction to cyber criminology

In this lecture we will discuss the place of the cyber space in criminology. We will discuss the various types of crimes that occur online and the main issues.

2. Criminological theories in cyber space

We will discuss some key theories pertaining to cybercrime; Social learning theory, routine activity theory, social control theory, self-control theory.

3. Cyber-focused crime: financial crime, fraud, identity theft

We will discuss cyber-characterized crimes in the field of financial crimes, theft,

fraud and identity theft.
4. Cyber -enabled crimes: harassment, sexual crime, bullying
We will discuss crimes against people related to harassment, sexual crime, bullying, etc.

5. Victims in the cyber world
We will discuss how victimology research affects our understanding of cybercrime.

6. Online and social radicalization
We will discuss the role of the Internet as a factor in radicalization, including various theories for understanding how it works.

7. The Internet as an assistant to "Offline" crime:
We will discuss how the Internet is used to promote "offline" crimes through support groups that work for different ideologies or groups such as gangs, mass murderers (such as school attacks), and "lone wolves".

8. Transferring crime from the cyber world to the real world.
We will discuss various cyber-related crimes that begin on the Internet, or that are made possible online, but from which actual harm occurs offline.

9. Attacks, and burglaries
We will discuss various types of cyber crimes aimed at disrupting or harming other elements of the cyber world. We will discuss the different motives that indicate different types of attacks.

10. Policing and Enforcement: Part I
We will discuss how policing and enforcement is carried out against cyber-enabled crime.

11: Policing and Enforcement: Part 2
We will discuss how policing, enforcement, and protection is done against cyber-targeted crime.

12. Online tracking
We will discuss how the Internet is used by law enforcement agencies as a surveillance and crime prevention tool, and private institutional infringement.

13. Algorithms: Their impact on the Internet and us
We will discuss the role of algorithms as an environmental factor that influences how we use the Internet and its role in promoting deviant attitudes and behaviors from a social perspective.
Conclusions of the course

Required Reading:

1. Introduction to cyber criminology

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1(1), 1-6.

Diamond, B., & Bachmann, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology 1. International Journal of Cyber Criminology, 9(1), 24.

2. Criminological theories in cyber space

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. American Journal of Criminal Justice, 37(3), 378-395.

3. Cyber-focused crime: financial crime, fraud, identity theft

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), 267-296.

4. Cyber -enabled crimes: harassment, sexual crime, bullying

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here?. Aggression and violent behavior, 34, 193-200.

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, violence, & abuse, 19(2), 195-208.

5. Victims in the cyber world

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime science, 7(1), 5.

6. Online and social radicalization

Hawdon, J., Bernatzky, C., & Costello, M. (2018). Cyber-Routines, Political Attitudes, and Exposure to Violence-Advocating Online Extremism. Social Forces.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. Criminology & Public Policy, 16(1), 99-117.

7. The Internet as an assistant to "Offline" crime:

Irwin-Rogers, K., Densley, J., & Pinkney, C. (2018). Gang violence and social media. In The Routledge international handbook of human aggression (pp. 400-410). Routledge.

Oksanen, A., Hawdon, J., & Räsänen, P. (2014). Glamorizing rampage online: School shooting fan communities on YouTube. Technology in society, 39, 55-67.

8. Transferring crime from the cyber world to the real world.

Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. Archives of sexual behavior, 44(1), 45-66.

9. Attacks, and burglaries

Cox, C. (2015). Cyber capabilities and intent of terrorist forces. Information Security Journal: A Global Perspective, 24(1-3), 31-38.

Rege, A. (2014). A criminological perspective on power grid cyber attacks: Using routine activities theory to rational choice perspective to explore adversarial decision-making. Journal of Homeland Security and Emergency Management, 11(4), 463-487.

10. Policing and Enforcement: Part I
Holt, Thomas J., George W. Burruss, Adam Bossler. 2015. "Policing Cybercrime and Cyberterror." Criminal Justice and Criminology Faculty Publications
11: Policing and Enforcement: Part 2
Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. Policing: An International Journal of Police Strategies & Management, 27(3), 341-357.
Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology, 7(1), 1.
12. Online tracking
Marquis-Boire, M., Scott-Railton, J., Guarnieri, C., Kleemola, K., Technica, K. S. T., Gear, S., ... & Kennedys, D. (2012). Police Story: Hacking Team's Government Surveillance Malware.
13. Algorithms: Their impact on the Internet and us
Wood, M. A. (2017). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious. Theoretical Criminology, 21(2), 168-185.

Additional Reading Material:

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.
Rokven, J. J., Weijters, G., Beerthuizen, M. G., & van der Laan, A. M. (2018). Juvenile Delinquency in the Virtual World: Similarities and Differences between Cyber-Enabled, Cyber-Dependent and Offline Delinquents in the Netherlands. International Journal of Cyber Criminology.
Yar, M. (2012). E-Crime 2.0: the criminological landscape of new social media. Information & Communications Technology Law, 21(3), 207-219.
Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.
Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). 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.
Macdonald, S., & Whittaker, J. (2019). online Radicalization. Online Terrorist Propaganda, Recruitment, and Radicalization, 33.
Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. Sexual Abuse, 22(1), 3-24.

Regnér, L. (2014). The YouTube-Born Terrorist. Journal Exit-Deutschland. Zeitschrift für Deradikalisierung und demokratische Kultur, 2, 139-189.

Course/Module evaluation:

End of year written/oral examination 60 %
Presentation 0 %
Participation in Tutorials 10 %
Project work 30 %
Assignments 0 %
Reports 0 %
Research project 0 %
Quizzes 0 %
Other 0 %

Additional information: