RIGA GRADUATE SCHOOL OF LAW

Course Outline

Course number	**RTL104**					
Course title	**Cybercrime and Cybersecurity**					
Credit points	3 ECTS (2 CP)					
Total hours	24					
Contact hours	24					
Independent studies	48					
Course level	Maters					
Prerequisites	None					
Category	Mandatory		Restricted elective		Free elective	

COURSE RESPONSIBLE

Name	***Academic degree***	***Academic position***
Dr Vasileios Karagiannopoulos	LLB, LLM, PhD, CFIP	Guest Professor

COURSE TEACHERS

Name	***Academic degree***	***Academic position***
Dr Vasileios Karagiannopoulos	LLB, LLM, PhD, CFIP	Guest professor

COURSE ABSTRACT

The course offers a combination of criminological and socio-legal analysis of cybercrime together with a wider understanding of important cybersecurity issues. Initially, the course will focus on cybercrime

and will provide an in depth understanding of the different types of cybercrime and online deviance from hacking and hacktivism to cyberstalking, online fraud and online piracy. During these sessions, we will discuss cybercriminal practices and techniques, relevant legal developments and practical challenges in terms of dealing with these crimes. Moreover, the course will look at the practical and ethical principles relating to digital forensic investigations that relate to the uncovering and prosecuting of cybercrimes and other crimes involving digital evidence.

Subsequently the course will focus on important cybersecurity issues such as organisational risk management and incident response mechanisms and will also offer an analysis of the phenomenon of cyberterrorism and cyberwarfare, which has generated heated discussions in terms of attribution of cyberattacks and also regarding the mitigation of the impact of such attacks. Finally, the course will close with a forward-looking overview of the future of digital crime, as it will be facilitated by the development of cryptocurrencies, 3D printing and the Internet of Things as these technological developments generate new opportunities for crime and pose serious regulatory challenges for governments and law enforcement.

GRADING CRITERIA

Criteria	***Weighting***
2000-word essay	100%

COURSE REQUIREMENTS

COURSE PLAN – MAIN SUBJECTS

No.	***Main subjects***	***Planned hours***
1	Cybercrime issues and relevant regulations	14
2	Cybercrime investigations	2
3	Advanced issues of online crime and cybersecurity	6
4	Essay writing skills	2

COURSE PLAN – SESSIONS

Session	*Session subjects and readings*	*Lecture/ Seminar*
1	Lecture 1: Introduction: 1. Module layout, aims and assessment 2. Defining cybercrime and the challenges it poses Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group. Chapters 1-2 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group Chapter 1 Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE. Chapter 1 Additional Readings: Yar, M. (2012). E-Crime 2.0: The Criminological Landscape of New Social Media. Information & Communications Technology Law, (Issue 3), 207 Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles. Social & Legal Studies, (Issue 2), 243	
2	Lecture 2: Hackers, crackers and hacktivists: The birth and development of hacking, its criminalization 1. The hacker movement 2. Criminalization of hacking and legal developments 3. Malware and relevant challenges Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group. Chapter 3-4 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group Chapters 3-4 Additional Readings: Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE. Chapter 3 Karagiannopoulos, V. (2018). Living with Hacktivism : From Conflict to Symbiosis. Palgrave Macmillan Jordan, T. (2008). Hacking : digital media and technological determinism. Polity	

Session	*Session subjects and readings*	*Lecture/ Seminar*
3	Lecture 3: Identity theft and Cyberfraud – Financial crime in cyberspace 1. Different types of fraud and identity theft online 2. Regulating fraud and identity theft through law and technology Recommended readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group Chapter 6 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group Chapter 6 Additional Readings: Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. Routledge. Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. Police Practice & Research: An International Journal, 19(6), 537–549. https://doi.org/10.1080/15614263.2018.1507890	
4	Lecture 4: Online child abuse images and paedophile rings 1. Offences relating to child sexual exploitation online 2. Policing crimes of child sexual exploitation online Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group Chapter 8 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group Chapter 10 Additional Readings: Nair, A. (2019). The regulation of internet pornography issues and challenges. Routledge Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE. Chapter 8	

Session	*Session subjects and readings*	*Lecture/ Seminar*
5	Lecture 5: The birth of the piracy movement, its development and its regulation 1. Piracy subcultures 2. The evolution of law to deal with online piracy 3. Law enforcement and industry responses Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group Chapter 5 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group pp.169-178 Additional Readings: Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE. Chapter 5	
6	Lecture 6: Communication offences online: Cyberbullying, harassment and online stalking 1. The birth and rise of social media and communication offences 2. Relevant legislation and interesting cases – what are the challenges? Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group Chapter 9 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group Chapter 8 and 11 Additional Readings: Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE. Chapter 9	

Session	*Session subjects and readings*	*Lecture/ Seminar*
7	Digital investigations: Practical and legal challenges 1. Core princinples of digital forensics 2. The legal challenges in digital forensics 3. Practical challenges with digital evidence Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group Chapter 12, 14 Sachowski, J. (2018). Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise, CRC Press - Chapter 1 from "principles of digital forensics" until the "process methodology" – Chapter 4, only the ACPO guidelines – Chapter 5 and 12 Additional Readings: Gogolin, G. (2012). Digital forensics explained. CRC Press - Chapter 2 and 7	
8	Cyberterrorism and Cyberwarfare 1. Defining cyberterrorism and cyberwarfare 2. The relevant legislation 3. Understanding the challenges regarding cyberwarfare Recommended Readings: Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics : an introduction. Routledge, Taylor & Francis Group Chapter 10 Gillespie, A. (2016). Cybercrime : key issues and debates. Routledge, Taylor & Francis Group Chapter 5 Additional Readings: Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE. Chapter 4 The WIRED Guide to Cyberwar: https://www.wired.com/story/cyberwar-guide/ Jensen, E. T. (2016). The Tallinn Manual 2.0: Highlights and Insights. Geo. J. Int'l L., 48, 735.	

Session	*Session subjects and readings*	*Lecture/ Seminar*
9	3D printing and crime 1. Understanding the nature and developments around 3D printing technologies 2. Exploring and analysing the various possibilities for using these technologies in criminal activity 3. Evaluating the practical challenges of regulating such activities Formlabs (2019, September 27) Planes, skulls & suitcases: solving the perfect crime through 3D printing. https://formlabs.com/uk/blog/solving-crime-through-3d-printing/ GlobalData Healthcare (2021, February 4) 3D printing of drugs can revolutionise personalised medicine and improve sustainability. https://www.medicaldevice-network.com/comment/3d-printing-drugs-personalised-medicine-sustainability/ Montalbano, E. (2020, August 19) The sounds a key make can produce 3D-printed replica, Threat Post. https://threatpost.com/the-sounds-a-key-make-can-produce-3d-printed-replica/158457/ Newman, L. H. (2020, August 4) A cheap 3D printer can trick smartphone fingerprint locks. Wired. https://www.wired.com/story/cheap-3d-printer-trick-smartphone-fingerprint-locks/ Schofield. C. (2020, November 25) Criminals can now 3D print your house keys from a Facebook photo. Yorkshire Evening Post. https://www.yorkshireeveningpost.co.uk/read-this/criminals-can-now-3d-print-your-house-keys-from-a-facebook-photo-3047169 Official Journal of the European Council. (1991, June 18) Council. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0477&from=EN Official Journal of the European Council. (2017, May 17) Directives. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0853&from=EN Official Journal of the European Council. (2012, March 14) Regulations. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:094:0001:0015:En:PDF Chase, R. J., & LaPorte, G. (2018). The next generation of crime tools and challenges: 3D printing. NIJ J, 279, 49-57. Clark, L. (2013, May 11) Disarming Corruptor distorts 3D printing files for sharing of banned items. Wired. https://arstechnica.com/information-technology/2013/11/disarming-corruptor-distorts-3d-printing-files-for-sharing-of-banned-items/ Daly, A., Mann, M., Squires, P., & Walters, R. (2021). 3D printing, policing and crime. Policing and Society, 31(1), 37-51. IACP Police Chief (2022) 3D printing new kinds of crime. Police Chief Magazine, https://www.policechiefmagazine.org/3d-printing-new-kinds-of-crime/ Yanisky-Ravid, S., & Kwan, K. S. (2016). 3D printing the road ahead: The digitization of products when public safety meets intellectual property rights - a new model. CARDozo L. REv., 38, 921.	

Session	*Session subjects and readings*	*Lecture/ Seminar*
10	Cryptocurrencies, crime and practical and regulatory challenges 1. Become familiar with cryptocurrencies such as Bitcoin and Ethereum and how they work 2. Discuss the potential ways they could be used for criminal activities 3. Analyse examples of regulatory efforts in relation to cryptocurrencies and their efficiency Basic readings: Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of economic Perspectives, 29(2), 213-38. Chohan, U. W. (2017). Assessing the differences in bitcoin & other cryptocurrency legality across national jurisdictions. Available at SSRN 3042248. Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. Research in International Business and Finance, 56, 101387. Huang, R. (2020, December 29) The 'Chinese mining centralization' of bitcoin and ethereum. https://www.forbes.com/sites/rogerhuang/2021/12/29/the-chinese-mining-centralization-of-bitcoin-and-ethereum/?sh=4a3d3cc22f66. Huston, J. (2020). The energy consumption of bitcoin mining and potential for regulation. Geo. Wash. J. Energy & Envtl. L., 11, 32. Redman, J. (2017, July 18) Following money through the bitcoin laundry is not so easy. https://news.bitcoin.com/following-money-bitcoin-laundry/ Stokel-Walker, C. (2021, November 2) How a Squid Game crypto scam got away with millions. https://www.wired.co.uk/article/squid-game-crypto-scam. Thomson Reuters Foundation. (2021, May 13) How Bitcoin mining impacts the environment. https://www.youtube.com/watch?v=NQTNy_5_gkY Trautman, L. J. (2018). Bitcoin, virtual currencies, and the struggle of law and regulation to keep peace. Marq. L. Rev., 102, 447. Wharton University of Pennsylvania. (2021, October 5) Will China's ban hurt cryptocurrencies? https://knowledge.wharton.upenn.edu/article/will-chinas-regulation-kill-cryptocurrencies/	

Session	*Session subjects and readings*	*Lecture/ Seminar*
11	Cybersecurity in the business sector: Risk management and incident response: 1. Understand the various risks businesses face and the drivers for implementing cybersecurity 2. Analyse the challenges regarding the implementation of preventative and reactive measures against cyberthreats 3. Explore best practices in terms of enhancing cybersecurity in the business sector also considering the implications of the pandemic Basic Readings: Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080 Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4), 234-246. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59. Cyber Security Breaches Survey. (2021). *Cyber Security Breaches Survey 2021*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 Furnell, S., & Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, *2009*(11), 7-11. Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8. Additional Readings: National Cyber Security Centre (NCSC). (2019). *Cyber security response and recovery*. https://www.ncsc.gov.uk/files/NCSC_A5%20Response%20and%20Recovery%20Guide_v3_OCT20.pdf National Cyber Security Centre (NCSC). (2020). Home working: preparing your organisation. https://www.ncsc.gov.uk/guidance/home-working	
12	Final Lecture: Revision and essay writing advice	

COURSE LEARNING OUTCOMES

This course has the following main learning outcomes:

Knowledge:

1. Students will learn about the history of cybercrime and the development of different techniques and practices criminals have developed for a variety of criminal activity online, from hacking to fraud and child pornography online
2. Students will learn about pertinent criminological theories and how they relate to cyberspace

3. Students will learn the various legislative and regulatory developments that have been put in place in order to deal with the different types of cybercrimes

4. Students will learn the basic principles of digital investigations and will also understand how organisations assess cyber-risk and respond to compromises

5. Students will learn about new and important developments that can have a global impact in terms of cybersecurity, such as the Internet of Things, the dark web and cyberwarfare.

Skills:

The students will develop:

1. High level academic skills in analysing cybercriminal behaviours and thinking about cybersecurity challenges.
2. Team working in class as well as personal study and self-conceptualisation skills.
3. Students will also enhance their academic writing skills and will learn to think in a multidisciplinary way when explaining current socio-political problems involving technology and deviance

Competencies:

1. **Criminological, regulatory and policing-related thinking:** recognize the human, interpersonal and technical sides of a problem; access, analyse and apply knowledge and skills from various disciplines; think critically and strategically in terms of identifying a problem and the relevant responses, but also the difficulties at investigating and resolving such cases, understanding the challenges of dealing with unexpected and original behaviours, apply knowledge and skills from past experiences to new situations; assess situations and identify problems;
2. **Information management:** think critically and gather, sort, store and use information to turn data into knowledge; research and interpret relevant information from a range of sources; review, retain and apply ideas; evaluate the validity and bias of information; use gathered data to draw conclusions or to create new sources of information that can be shared with others; document your sources of information; document your sources of information.
3. **Communication:** develop listening and note-taking skills, participate in classroom environment, collaborate on academic tasks, legal research and persuasive academic writing.

By completing the study course and successfully passing examination, the student will be able to:

Learning outcomes	***Evaluation criteria***		
	(40-69%)	***(70-89%)***	***(90-100%)***
Knowledge	The student has demonstrated basic levels of knowledge.	The student has demonstrated knowledge that complies with the expectations	The student has demonstrated in-depth knowledge

Skills	The student has demonstrated a basic level of the above skills	The student has demonstrated good skills.	The student has demonstrated excellent skills.
Competences	The student has demonstrated a basic ability to apply the knowledge	the student can apply the knowledge at a reasonably good level.	student is able to apply the knowledge independently and correctly.

Please analyse the contribution of defined grading criteria to learning outcomes. Number of grading criteria and learning outcomes should correspond to previously defined one.

Grading criteria	***Learning outcomes***					
	1.	**2.**	**3.**	**4.**	**5.**	**6.**
Essay	x	x	x	x	x	

COURSE LITERATURE

Compulsory literature

No.	***Author, year, title, publisher***
	Please see above Basic readinds

Additional literature and sources

No.	***Author, year, title, publisher***
	Please see above recommended readings