COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
CYBERSECURITY LAW AND CYBERCRIME	

Lecturer(s)	Department(s)
Coordinator: adjunct prof. dr. J. Kulesza **Other(s)**: -	Department of International Law, Faculty of Law and Administration, University of Lodz, Poland; e-mail: joanna_kulesza@wpia.uni.lodz.pl

Study cycle	Type of the course unit (module)
Second	Optional

Mode of delivery	Period when the course unit (module) is delivered	Language(s) of instruction
Face-to face	1 (autumn) semester	English

Requirements for students	
Pre-requisites: None	**Co-requisites (if any):** None

Number of credits allocated	Total student's workload	Contact hours	Self-study hours
5	133	32	101

Purpose of the course unit (module): programme competences to be developed		
The purpose of this course is to enhance students' knowledge about the principles and complex legal processes developed by governments, the private sector, and civil society on the domestic and international level to secure the Internet; to develop the ability to systemically interpret and assess statutory law related to cyberspace and its application in the jurisprudence of courts and by other jurisdictional institutions; and to critically evaluate legal and ethical challenges regarding large-scale cybersecurity threats and cyberattacks or other risks on personal, nation-state or global level due to new cyber technologies.		
Learning outcomes of the course unit (module)	**Teaching and learning methods**	**Assessment methods**
Students will be able to demonstrate conceptual uderstanding of the policies and stakeholders involved in the internet governance debate and will be able to compare the key policy aspects of cybersecurity questions related to relevant laws and policies.	An interactive method of teaching during lectures and seminars (the analysis of problematic issues, presentations on assigned topics, group discussions); individual studies (individual search of information, critical literature studies and the analysis of theoretical and practical problems)	Participation in class activies (assigned topics, discussions), individual paper (project)
Students will be able to apply the concepts of cybercrime, cybersecurity, cyberwarfare and cyberpower, and evaluate how they relate to internet policy while analyzing relevant recent caselaw set against national and regional reactions to cyberthreats.	An interactive method of teaching during lectures and seminars (the analysis of problematic issues, drafting of e-submissions and e-presentations, presentations on assigned topics, group discussions); individual studies (individual search of information, critical literature studies and the analysis of theoretical and practical problems)	Participation in class activies (assigned topics, practical exercises, discussions), individual paper (project)
Students will be able to systematically analyse the interaction of international, European and national legal regulation with regard to the exploitation and enforcement of cyberspace law and assess the compliance of	An interactive method of teaching during lectures and seminars (the analysis of problematic issues, drafting of e-submissions and e-presentations presentations on assigned topics, group discussions); individual studies (individual search of information, critical	Participation in class activies (assigned topics, practical exercises, discussions),

national legislation with the European and international legal acts.	literature studies and the analysis of theoretical and practical problems)	individual paper (project)
Students will be able to independently analyse complex cybersecurity issues and challenges in combating crime online and will be able to critically assess legal, social and ethical consequences of the developments in this sphere.	An interactive method of teaching during lectures and seminars (the analysis of problematic issues, presentations on assigned topics, group discussions); individual studies (individual search of information, critical literature studies and the analysis of theoretical and practical problems)	Participation in class activies (assigned topics, discussions), individual paper (project)
Students will be able to identify threats to collective and individual online security with the distinction between cybercrime and cybersecurity and model innovative strategies for legal regulation, *inter alia* to provide proposals on the necessary changes of legislation as well as on adoption of new legislation.	An interactive method of teaching during lectures and seminars (the analysis of problematic issues, drafting of e-submissions and e-presentations, presentations on assigned topics, group discussions); individual studies (individual search of information, critical literature studies and the analysis of theoretical and practical problems)	Participation in class activies (assigned topics, practical exercises, discussions), individual paper (project)
Students will be able to critically evaluate own accomplishments and to enhance acquired knowledge and abilities independently, *inter alia*, by using of legal information data bases and other sources, selecting relevant theoretical and practical material, and substantiating their own conclusions on the achievements of jurisprudence and by using relevant research method.	An interactive method of teaching during lectures and seminars (the analysis of problematic issues, exercises related to usage of ICT systems, presentations on assigned topics, group discussions); individual studies (individual search of information, critical literature studies and the analysis of theoretical and practical problems)	Participation in class activies (assigned topics, practical exercises, discussions), individual paper (project)
Students will professionally communicate orally and in written, unambiguously and reasonably convey owns well-grounded ideas, arguments and conclusions based on theoretical and practical knowledge and will be able to trigger or to contribute to the discussion with specialists and non-specialists providing their own insights in an international context.	An interactive method of teaching during seminars (the analysis of problematic issues, drafting of e-submissions and e-presentations, exercises related to usage of ICT systems presentations on assigned topics, group discussions); individual studies (individual search of information, critical literature studies and the analysis of theoretical and practical problems)	Participation in class activies (assigned topics, practical exercises, discussions), individual paper (project)

Content: breakdown of the topics	**Contact hours**							**Self-study work: time and assignments**	
	Lectures	Consultations	Seminars	Practical sessions	Laboratory activities	Internship/work placement	**Contact hours**	**Self-study hours**	**Assignments**
1. Introduction of Subject • Cyberspace Law in the global context • How is cyberspace law different? • State Jurisdiction in Cyberspace • International Law and Internet Governance	4						**4**	**10**	Analysis of relevant study materials, preparation of presentations on assigned topics.
2. Global Internet Governance • Internet Governance in the Global Context • Cybersecurity Research Concepts	4						**4**	**10**	Analysis of relevant study materials, preparation of presentations on assigned topics.

• European Union/Council of Europe / International Communication Union (ITU)									
3. The Cyberthreat Landscape within the world of internet governance – focus session • Cybersecurity and cybercrime • Threats, vulnerabilities, and consequences • The state of security today • Cyber-incidents case studies (Estonia attacks, Stuxnet, WannaCry; NotPetya)	4						**4**	**15**	Analysis of relevant study materials, preparation of presentations on assigned topics, practical exercises.
4. Critical Infrastructure Protection, Cybercrime and Cybersecurity • Regional Approaches to CI protection (EU and NIS Directive, US and beyond) • Multistakeholderism and Cybersecurity • UN, ITU, NATO, ICANN and IGF	4						**4**	**10**	Analysis of relevant study materials, preparation of presentations on assigned topics.
5. Preventing cyberattacks in international law • International Law's Role in Securing Cyberspace • Sources and Nature of International Law • Treaties/Customary International Law • War in Cyberspace	4						**4**	**10**	Analysis of relevant study materials, preparation of presentations on assigned topics, practical exercises.
6. Cybercrime • Specifing Cybercrimes • Council of Europe Convention on Cybercrime • The Octopus Conference • Online Mobs • Case studies	2						**2**	**10**	Analysis of relevant study materials, preparation of presentations on assigned topics, practical exercises.
7. Prevention, Attribution and Liability in Cyberspace • State Jurisdiction and International Cooperation • Prevention, Cyberdefence, Active Cyberdefence, Cyberweapons • Cyberwar Considerations	2						**2**	**10**	Analysis of relevant study materials, preparation of presentations on assigned topics.
8. Individuals and Security • Freedom of Information and Surveillance • US FISAA and encryption • Fake News and Online Propaganda • Hate Speech Online • ISP Liability and AI			4				**4**	**11**	Analysis of relevant study materials, preparation of presentations on assigned topics, practical exercises.
9. Emerging Trends for Cybersecurity • Hacking and Cyberpower • Privacy and Surveillance			4				**4**	**15**	Individual paper summarizing takeaways from the course.
Total	**24**		**8**				**32**	**101**	

Assessment strategy	Weight, percentage	Assessment period	Assessment criteria
Participation in class activities	40	During semester	Students will be expected to demonstrate both the knowledge gained during the course as well as their abilities to apply it in a given situation. Assessment of participation in class activities consists of: - presentation of assigned topics (capability to critically assess the issues, to identify the most significant features, tendencies and developments related to the particular topic, to provide orally clear arguments in support of their points made in a logical, coherent and structured manner); - practical exercises (comprehensive analysis of practical situations while drafting of e-submissions and e-presentations for dispute resolution, and performing exercises related to usage of ICT systems); - participation in discussions (capability to provide correct answers to questions, formulate problems and suggest (search for) solutions, offer thoughtful critical remarks, contribute to other participants' ideas, etc.).
Individual paper (project) + presentation	60	At the end of course	Individual paper (project) "*Current challenges to global cybersecurity and how to effectively prevent them"* assessment consists of: 1. 30 percent for: 1.1. content (comprehensive problem analysis, creativity, proper source application, critical analytical thinking, conclusion/recommendation formulation); 1.2. structure and style (clear structural parts, proper language style, exact wording, source references, appropriate and ethical citation use); 2. 30 percent for: 2.1. presentation (concentrated, efficient and convincing work presentation, adhesive language, the use of informative visual aids); 2.2. efficient and active participation in discussion (providing correct answers to questions, formulating problems and suggesting (searching for) solutions, offering thoughtful critical remarks, etc.).

Author	Year of publication	Title	Issue of a periodical or volume of a publication	Publishing place and house or web link
Compulsory reading				
1. Ed. Michael N. Schmitt	2017	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations		OUP
2. Council of Europe	2001	Convention on Cybercrime		https://www.coe.int/en/web/cybercrime/the-budapest-convention
3. John S. Davis II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase	2018	Stateless Attribution Toward International Accountability in Cyberspace		https://www.rand.org/pubs/research_reports/RR2081.html
4. Graham Greenleaf	2019	2017-2018 Further Update to Graham Greenleaf's Asian Data Privacy Laws – Trade and Human Rights Perspectives	UNSW Law Research Paper No. 19-4	
5. Scott Shackelford	2019	The Future of Frontiers		https://ssrn.com/abstract=3318521
6. Johan David Michels and Ian Walden	2018	How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical	Queen Mary School of Law Legal Studies Research	

		Infrastructure Under the NIS Directive	Paper No. 291/2018	
Optional reading				
1. Amos N. Guiora	2017	Cybersecurity: Geopolitics, Law and Policy		Routledge
2. Michael N. Schmitt	2013	Tallinn Manual		OUP
3. Alexander Klimburg	2017	The Darkening Web: The War for Cyberspace		Penguin Press
4. Adam Segal	2016	The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate ...		Hachette Book Group
5. European Commission	2016	The Directive on security of network and information systems (NIS Directive)		https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC