University of Gdańsk

Subject card

Subject name and code	Seminar III - ROJSZCZAK Marcin, PG_00198671						
Field of study	Criminology						
Date of commencement of studies	October 2026		Academic year of realisation of subject	2027/2028			
Education level	Master's studies		Subject group	Optional subject group			
Mode of study	full-time studies		Mode of delivery	at the university			
Year of study	2		Language of instruction	Polish			
Semester of study	4		ECTS credits	4.0			
Learning profile	academic		Assessment form	credit			
Conducting unit	Department of Legal Informatics -> Faculty of Law and Administration -> Rector						
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. Marcin Rojszczak					
	Teachers						
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	0.0	0.0	0.0	0.0	30.0	30
	E-learning hours included: 0.0						
Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan		Participation in consultation hours	Self-study	SUM	
	Number of study hours	30		0.0	70.0	100	
Subject objectives	The aim of the seminar is to prepare the student to independently develop a master's thesis in the field of new technology law, with particular emphasis on the legal and criminological aspects of cybersecurity, cybercrime, and the regulation of new and emerging technologies. The seminar is intended to develop the student's ability to identify and formulate research problems, critically analyse legal sources, case law and academic literature, select appropriate research methods, and construct and present academic arguments. In the course of the seminar, the student, in cooperation with the supervisor, defines and refines the subject of the research, formulates the research problem and research questions, collects and analyses source materials, prepares the structure of the thesis, and subsequently develops and improves its successive parts. The scope of the tasks is adapted to the stage of preparation of the master's thesis.						

Learning outcomes

Course outcome	Subject outcome	Method of verification
[KRYMMU2_U02] Is able to independently acquire knowledge and develop professional competences using various sources (in native and foreign languages) and modern technologies.	The student is able to independently identify, select, critically assess and use Polish and foreign academic, legal and technical sources, and to use modern tools supporting research and the preparation of the master's thesis.	[SU8] observation of student's independent or team work
[KRYMMU2_U05] Is able to independently propose solutions to problems, carry out decision-making processes in this area, organise and coordinate team work, and act in an entrepreneurial manner.	The student is able to independently solve problems arising in the preparation of the master's thesis, make well-founded decisions concerning research methods, structure and direction, and organise the process of completing the thesis.	[SU5] implementation of a problem task
[KRYMMU2_U01] Is able to apply theoretical knowledge of criminology and related disciplines to analyse, synthesise and interpret complex and non-routine problems, as well as to formulate solutions in changing and unpredictable conditions.	The student is able to apply knowledge of criminology, legal sciences and related disciplines to analyse, interpret and assess complex research problems concerning cybersecurity, cybercrime and new technologies, and to formulate well-founded conclusions.	[SU2] presentation/project/paper/ report
[KRYMMU2_K01] Is aware of the level of their knowledge and skills, critically evaluates them, understands the need for lifelong learning, and recognizes the importance of knowledge in solving cognitive and practical problems; when unable to solve a problem independently, seeks the opinions of experts.	The student is able to critically assess their own knowledge and research findings, identify the need to broaden their knowledge, and make use of substantive discussion and consultation in the process of preparing the master's thesis.	[SK1] oral statement/conversation/ discussion
[KRYMMU2_K03] Is convinced of the necessity of ethical and professional conduct, acts in accordance with ethical principles, identifies and formulates moral problems and ethical dilemmas related to their own and others' work, and seeks optimal solutions.	The student applies the principles of research ethics and academic integrity in the preparation of the master's thesis and is able to identify ethical issues related to conducting research, using sources and employing artificial intelligence tools.	[SK1] oral statement/conversation/ discussion

Subject contents

The seminar focuses on the legal and criminological aspects of the development of digital technologies, in particular cybersecurity, cybercrime, the protection of fundamental rights in the digital environment, and the regulation of new and emerging technologies.

The course covers, in particular: principles for selecting a research problem; formulation of the research objective, research questions, and thesis statements; research methods appropriate to legal studies and criminology; searching for, selecting, and critically analysing academic literature, legal acts, case law, and other source materials; use of national, EU, and international legal and academic information databases; developing the structure of the thesis; principles of academic argumentation; preparation and discussion of successive parts of the master's thesis; principles of citation and source documentation; verification, editing, and improvement of the prepared text; and principles of academic integrity, including the ethical use of artificial intelligence tools in accordance with applicable rules.

Seminar discussions also address current regulatory issues concerning, among others, national and EU cybersecurity law, cybercrime, the security of digital products and services, the protection of critical infrastructure, the regulation of artificial intelligence, automated content moderation, hate speech, electronic surveillance, privacy and data protection, encryption, and the development of emerging technologies, including quantum technologies.

Prerequisites and co-requisites

Basic knowledge of criminology, the fundamentals of law, and the functioning of the legal system. Ability to independently search for and analyse academic literature and source materials.

A command of English sufficient to use academic literature, European Union legal acts, and materials published by international institutions is recommended.

Specialist technical knowledge in computer science or cybersecurity is not required; the scope of the technical knowledge necessary will depend on the chosen topic of the master's thesis.

<table>
<tr><td>Assessment methods and criteria</td><td colspan="2"><table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td>Timely completion of successive stages of the master's thesis, in accordance with arrangements made with the supervisor and appropriate to the current stage of progress.</td><td>51.0%</td><td>100.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Recommended reading</td><td>Basic literature</td><td>1. C. Banasiński (ed), Cyberbezpieczeństwo. Zarys wykładu, wyd. 2, Wolters Kluwer, Warszawa 2023.
2. P. Opitek, D.R. Jaworski, Cyberprzestępczość w prawie karnym i kryminalistyce. Kompendium wiedzy, Difin, Warszawa 2025.
3. M.G. Porcedda, Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, Hart Publishing, 2023.
4. A. Murray, Information Technology Law: The Law and Society, 5th ed., Oxford University Press, 2023.
5. V. Franssen, S. Tosza (eds), The Cambridge Handbook of Digital Evidence in Criminal Investigations, Cambridge University Press, 2025.</td></tr>
<tr><td>Supplementary literature</td><td>1. D.R. Jaworski (red.), Cyberprzestępczość i nowe technologie. Współczesne wyzwania nauk prawnych, Difin, Warszawa 2024.
2. M. Siwicki, Cyberprzestępczość, C.H. Beck, Warszawa 2013.
3. J. Stelmach, B. Brożek, Metody prawnicze. Logika, analiza, argumentacja, hermeneutyka, wyd. 2, Wolters Kluwer, Kraków 2006.
4. M. Rojszczak, Bulk Surveillance, Democracy and Human Rights Law in Europe: A Comparative Perspective, Routledge, 2024.
5. M. Rojszczak, Beyond Hate Speech: Clearly Unlawful Content in EU Digital Law, Routledge, 2026.
6. P. Hacker, A. Engel, S. Hammer, B. Mittelstadt (eds), The Oxford Handbook of the Foundations and Regulation of Generative AI, Oxford University Press, 2026.</td></tr>
<tr><td>eResources addresses</td><td></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td colspan="2">Examples of research areas / thesis topics:
1. The European cybersecurity regulatory model after NIS2: a coherent system or fragmentation of regulatory obligations?
2. Manufacturers' responsibility for the cybersecurity of products with digital elements under the Cyber Resilience Act.
3. Implementation of the NIS2 Directive in Poland: the evolution of the national cybersecurity system and new obligations of essential and important entities.
4. Ransomware as a contemporary form of cybercrime: challenges of criminal liability, enforcement, and prevention.
5. Electronic evidence in combating cybercrime: the European e-Evidence framework and individual rights.
6. End-to-end encryption and the fight against serious crime: the limits of legal obligations imposed on digital service providers.
7. Automated detection and removal of hate speech in online services: between combating illegal content and protecting freedom of expression.
8. Artificial intelligence in law enforcement: limits on the use of predictive and analytical systems in light of the AI Act and fundamental rights.
9. Cybersecurity of artificial intelligence systems as a new regulatory challenge: the relationship between the AI Act, NIS2, and the Cyber Resilience Act.
10. The development of quantum computing and the legal protection of communications confidentiality: is cybersecurity law prepared for the post-quantum era?
11. Phishing, smishing, and social engineering fraud as forms of cybercrime: challenges of legal classification, detection, and prevention.
12. Malware, botnets, and unauthorised access to information systems: criminal liability and challenges in prosecuting perpetrators of cyberattacks.</td></tr>
<tr><td>Work placement</td><td colspan="2">Not applicable</td></tr>
</table>

Document generated electronically. Does not require a seal or signature.