

Course Syllabus

I. General Information

Course name	Cybersecurity law
Programme	European and International Legal Studies
Level of studies (BA, BSc, MA, MSc, long-cycle MA)	BA
Form of studies (full-time, part-time)	Full-time
Discipline	Law
Language of instruction	English

Course coordinator/person responsible	dr hab. Małgorzata Ganczar (prof. KUL) dr Agnieszka Parol
---------------------------------------	--

Type of class (<i>use only the types mentioned below</i>)	Number of teaching hours	Semester	ECTS Points
lecture	30		3
tutorial			
classes			
laboratory classes			
workshops			
seminar			
introductory seminar			
foreign language classes			
practical placement			
field work			
diploma laboratory			
translation classes			
study visit			

Course pre-requisites	
-----------------------	--

II. Course Objectives

- C1. Familiarization: with legal terminology in English in the field of law cybersecurity in Poland and in the world.
- C2: To provide knowledge and develop skills in the field of independent analysis of sources of law and documents used in the practice of law, i.e. legal acts, court decisions, other legal acts, documents in English in the field of cybersecurity law.
- C3: Provide general knowledge of legal phrases and terms used cybersecurity in English and methodological and workshop preparation for interpreting and written texts.
- C4: Developing the ability to translate legally: a legal act, a judgment, a document, a

scientific article in English.
 C5: Enriching the knowledge of legal English with professional phrases and formulations used in the practice of law through written translation exercises, development of the ability to interpret legal texts in English, the development of skills preparation of a pleading, opinion, position, etc. in English.

III. Course learning outcomes with reference to programme learning outcomes

Symbol	Description of the objective effect	Directional Effect Reference
KNOWLEDGE		
W_01	He/she knows and understands the mechanisms of international cooperation in the field of Cybersecurity	K_W02
W_02	He/she knows and understands the basic principles of creating and developing various forms of entrepreneurship at the national and EU level in the context challenging national and global cyber environment	K_W05
W_03	He/she knows the position of the individual in the international system and human rights protection sources in the context challenging national and global cyber environment	K_W06
W_04	He/she knows the principles of the digital market and the impact of digitization on contemporary society in the field of Cybersecurity	K_W10
ABILITIES		
U_01	He/she is able to analyse basic social, political and economic processes of international, regional and national scope in the field of Cybersecurity	K_U01
U_02	He/she is able to analyse EU sources, case law of national and international courts, access EU documents, knows the mechanisms of their interpretation and efficiently uses EU websites and legal information services also regarding the use of artificial intelligence in the field of Cybersecurity	K_U02
SOCIAL COMPETENCES		
K_01	He/she formulates critical opinions, being open to new ideas and ready to change opinions in light of available data and expert opinions	K_K04

IV. Course Content

This course provides an examination of the legal language aspects of cybersecurity law. The overall objective of the course is to provide an understanding of state behavior in a changing and

challenging national and global cyber environment. This course will draw upon readings, lectures, class discussions, group presentations, and crisis simulations to foster an understanding of cybersecurity policy and to help students develop an analytic framework for understanding current legal debates. Students have to be able to apply the different theories and their key concepts in a case study. Current affairs and student interests will also shape the topics to be discussed as case studies under the core

Syllabus below:

1. Data Security Laws and Enforcement Actions
2. Cybersecurity Litigation
3. Cybersecurity Requirements for Specific Industries
4. Cybersecurity and Corporate Governance
5. Anti-Hacking Laws
6. Polish Government Cyber Structure
7. Public–Private Cybersecurity Partnerships
8. Surveillance and Cyber
9. Cybersecurity and Cyber-warfare
10. Cybersecurity and Polish Government Contractors
11. Polish Privacy Laws
12. International Cybersecurity Law
13. Cyber and the Law of War
14. Cybersecurity Court Opinions
15. Summary of the course

V. Didactic methods used and forms of assessment of learning outcomes

Symbol	Didactic methods (choose from the list)	Forms of assessment (choose from the list)	Documentation type (choose from the list)
KNOWLEDGE			
W_01	Textual analysis; Brainstorming or discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Work with text; Case study; Conventional lecture; Conversational lecture; Problem lecture	Paper; Written test; Observation; Oral test; Presentation; Preparation / implementation of the project	Protocol / paper; printout/ paper file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card
W_02	Textual analysis; Brainstorming or discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Work with text; Case study; Conventional lecture; Conversational lecture; Problem lecture	Paper; Written test; Observation; Oral test; Presentation; Preparation / implementation of the project	Protocol / paper; printout/ paper file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card
W_03	Textual analysis; Brainstorming or	Paper; Written test; Observation; Oral test;	Protocol / paper; printout/ paper

	discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Work with text; Case study; Conventional lecture; Conversational lecture; Problem lecture	Presentation; Preparation / implementation of the project	file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card
W_04	Textual analysis; Brainstorming or discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Work with text; Case study; Conventional lecture; Conversational lecture; Problem lecture	Paper; Written test; Observation; Oral test; Presentation; Preparation / implementation of the project	Protocol / paper; printout/ paper file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card
SKILLS			
U_01	Textual analysis; Brainstorming/ discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Work with text; Case study; Conventional lecture; Conversational lecture; Problem lecture	Paper; Written test; Observation; Oral test; Presentation; Preparation / implementation of the project	Protocol / paper; printout/ paper file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card
U_02	Textual analysis; Brainstorming/ discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Work with text; Case study; Conventional lecture; Conversational lecture; Problem lecture	Paper; Written test; Observation; Oral test; Presentation; Preparation / implementation of the project	Protocol / paper; printout/ paper file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card
SOCIAL COMPETENCIES			
K_01	Brainstorming/ discussion group; Discussion; PBL (ProblemBased Learning); SWOT method; Case study; Conversational lecture; Problem lecture	Paper; Written test; Observation; Oral test; Presentation; Preparation / implementation of the project	Protocol / paper; printout/ paper file; Evaluated test; Evaluated written paper; Rating card / Observation report; Rating card

VI. Grading criteria, weighting factors.....

In the field of seminars in English, obtaining a credit requires obtaining min. 51% of correct answers from the final single-choice test consisting of 21 questions. Possibility of exemption from the colloquium in the case of preparing an optional paper – 50% and activity in classes – 50%. Correction of the oral test – 3 questions. In the case of Appendix No. 5 to the curriculum documentation for distance learning, related to the state of the pandemic, obtaining credit requires receiving min. 51% correct answers from the final single-choice test placed on the remote platform consisting of 21 questions. Correction of the oral test – 3 questions. Distribution of grades: unsatisfactory- 0-10 points; satisfactory – 11 points; satisfactory plus – 12; good – 13 points; good plus – 14-16 points; very good – 17-21 points Possibility of exemption from the colloquium in the case of preparing an optional paper – 50% and activity in classes – 50%.

VII. Student workload

Form of activity	Number of hours
Number of contact hours (with the teacher)	30
Number of hours of individual student work	45

VIII. Literature

Basic literature
Gheciu, A., Wohlforth, W. C., The Oxford Handbook of International Security, Oxford University Press, Oxford 2018;
Françoise G., Global Privacy and Security Law, Wolters Kluwer Law & Business: Austin 2007;
Footer M., Schmidt J.R., White N.D., Davies-Bright L., Security and international law, Hart Publishing 2016
Additional literature
Sullivan G., Transnational Legal Assemblages and Global Security Law: Topologies and Temporalities of the List, Transnational Legal Theory, (2014)5:1, 81-127, DOI: 10.5235/20414005.5.1.81;
Sullivan G., The law of the list: UN counterterrorism sanctions and the politics of global security law, Cambridge University Press: New York 2020;
Goold B.J., Lazarus L., Security and Human Rights, Hart Publishing: Bloomsbury 2019.