COURSE UNIT DESCRIPTION

Course Unit Title	Code
CYBERSECURITY IN INTERNATIONAL RELATIONS	

Lecturer(s)	Department(s)
Coordinator: lect. dr. Lior Tabansky **Other(s):**	Institute of International Relations and Political Science, Vilnius university, Vokiečių str. 10, LT-01130, Vilnius, tel. +370 52514130, e-mail: tspimi@tspmi.vu.lt

Study cycle	Type of the course unit
First	Elective

Mode of delivery	Course unit delivery period	Language (s) of instruction
Face-to-face	6 (spring) semester	English

Requirements for students	
Pre-requisites: -	**Co-requisites (if any):** -

Number of credits allocated	Total student's workload	Contact hours	Self-study hours
5	135	32	103

Purpose of the course unit: programme competences to be developed		
Aim of this course is to provide a comprehensive conceptual knowledge in International Relations (IR) and cybersecurity, while combining it with a necessary technical understanding of the concrete workings of cyberspace and their security implications; also to develop practical knowledge of cybersecurity matters throughout history and up to nowadays, as well as ability to analyze and evaluate different complex cybersecurity issues through the lens of IR.		
Learning outcomes of the course unit	**Teaching and learning methods**	**Assessment methods**
Students will able to systemically explicate International Relations theoretical advances and debates on cybersecurity from a wide range of approaches.	Peer discussion, individual studies (critical analysis of assigned literature), presentation, problem-oriented lectures, technical explanations, analysis of empirical cases, practical exercises	High-quality and active participation in seminar discussion, presentation, final examination
Students will be able to explain the historical development of cyber incidents, cybersecurity policies and norms regulating them, as well as to identify and evaluate their impact on individuals and societies.		
Students will acquire an adequate understanding of the technical aspects of information security in order to grasp their political and security implications.		
Students will be able to critically analyze the phenomenon of cybersecurity drawing on existing scholarly research as well as to provide evidence-based policy recommendations on how to manage the social, political, legal and ethical consequences of the developments in this sphere.		
Students will be able to assess how realistic different cyberwarfare scenarios are from both technical and political perspectives.		
Students will be able to analyze the interconnection between the technical and geopolitical aspects of cybersecurity, to critically assess legal, social and ethical consequences of the developments in this sphere.		
Students will be able to formulate advise to the policy world in a down-to-earth and pragmatic way.		

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.		

Content: breakdown of the topics	**Contact hours**							**Self-study: hours and assignments**	
	Lectures	Consultations	Seminars	Practical sessions	Laboratory activities	Internship/work	**Contact hours**	**Self-study hours**	**Assignments**
1. Introduction: • Introducing the course programme; • Technical basics; • ICT history; • Cyber international relations.			2				**2**	**6**	**Each seminar is structured and divided into 3 general parts: a) peer discussion of the assigned readings; b) technical explanations necessary to situate and understand the topic; c) empirical illustrations and peer discussion, short practical exercises related to the week's topic.** Read and analyze: Lessig, Lawrence. 1999. Code: And Other Laws of Cyberspace. Basic Books; Choucri, Nazli, and David D. Clark. 2019. International Relations in the Cyber Age. MIT Press; (pages will be specified before class)
2. Traditional cyber strategic studies I: the politics of cyberwarfare	2		2				**4**	**8**	Read and analyze: Perkovich, George, and Ariel E. Levite, eds. 2017. Understanding Cyber Conflict: Fourteen Analogies. Washington, D.C: Georgetown University Press; Kello, Lucas. 2017. The Virtual Weapon and International Order. Yale University Press; (pages will be specified before class)
3. Traditional cyber strategic studies II: technical constraints in cyberwar			2				**2**	**8**	Read and analyze: Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar. Rand Corporation; (pages will be specified before class); Nye, Joseph S. 2017. 'Deterrence and Dissuasion in Cyberspace'. International Security 41(3): 44–71.
4. Cyberattacks: some case studies			2				**2**	**6**	Read and analyze: Farwell, James P., and Rafal Rohozinski. 2011. 'Stuxnet and the Future of Cyber War'. Survival 53(1): 23–40; Russell, Alison Lawlor. 2014. Cyber Blockades. Georgetown University Press; (pages will be specified before class).
5. Representing, constructing, and securitising cyber threats			2				**2**	**6**	Read and analyze: Hansen, Lene, and Helen Nissenbaum. 2009. 'Digital Disaster, Cyber Security, and the Copenhagen School'. International Studies Quarterly 53(4): 1155–75; Dunn Cavelty, Myriam. 2013. 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the

									Cyber-Security Discourse’. International Studies Review 15(1): 105–22.
6. Space, time, ignorance: critical & poststructuralist approaches			2				**2**	**6**	Read and analyze: Balzacq, Thierry, and Myriam Dunn Cavelty. 2016. ‘A Theory of Actor-Network for Cyber-Security’. European Journal of International Security 1(2): 176–98; Aradau, Claudia, and Tobias Blanke. 2015. ‘The (Big) Data-Security Assemblage: Knowledge and Critique’. Big Data & Society 2(2): 205395171560906.
7. Student presentations			4				**4**	**10**	Preparation for the presentation. Topic has to be agreed upon in advance (e.g., specific cyber security policy analysis, policy recommendations, analysis of a cybersecurity incident with suggestions of how to prevent it in the future, etc.)
8. Private actors and governance			2				**2**	**6**	Read and analyze: McCarthy, Daniel R. 2018. ‘Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order’. Politics and Governance 6(2): 5; Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. 2017. ‘Public–Private Partnerships on Cyber Security: A Practice of Loyalty’. International Affairs 93(6): 1435–52.
9. Critical infrastructure and cybersecurity in the everyday			2				**2**	**6**	Read and analyze: Aradau, Claudia. 2010. ‘Security That Matters: Critical Infrastructure and Objects of Protection’. Security Dialogue 41(5): 491–514; Dunn & Christensen 2020, Securing 'the Homeland': Critical Infrastructure, Risk and (In)Security.
10. Internet filtering and censorship			2				**2**	**6**	Read and analyze: Deibert, Ronald J. 2003. ‘Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace’. Millennium: Journal of International Studies 32(3): 501–30; Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2008. Access Denied: The Practice and Policy of Global Internet Filtering. The MIT Press; (pages will be specified before class)
11. Privacy and data breaches			2				**2**	**6**	Read and analyze: Schwartz, Paul M., and Daniel J. Solove. 2011. ‘The PII Problem: Privacy and a New Concept of Personally Identifiable Information’. *New York University Law Review* 86: 1814. Bigo, Didier, Engin Isin, and Evelyn Ruppert. 2019. *Data Politics: Worlds, Subjects, Rights*. Routledge. Finnemore, Martha, and Duncan B. Hollis. 2016. ‘Constructing Norms for Global Cybersecurity’. *American Journal of International Law* 110(3): 425–79.
12. Information warfare and social media			2				**2**	**6**	Read and analyze:

									Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. 2018. ‘State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation’. International Affairs 94(5): 975–94; Giles, Keir. 2016. The Next Phase of Russian Information Warfare. NATO StratCom Centre of Excellence.
13. Cybercrime, the blockchain and the “dark web”			2				**2**	**6**	Read and analyze: Amoore, Louise, and Marieke De Goede. 2005. ‘Governance, Risk and Dataveillance in the War on Terror’. Crime, Law and Social Change 43(2): 149–73; Filippi, Primavera, and Benjamin Loveluck. 2016. ‘The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure’. Internet Policy Review.
14. Quantum technologies			2				**2**	**5**	Read and analyze: Wendt, Alexander. 2015. Quantum Mind and Social Science. Cambridge University Press; Der Derian, James. 2009. Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network. Routledge; (pages will be specified before class).
Final exam								**12**	Preparation for the final exam.
Total	**2**		**30**				**32**	**103**	

Assessment strategy	**Weight, percentage**	**Assessment period**	**Assessment criteria**
Participation in seminars	40	During the semester	Students will be expected to demonstrate both the knowledge related to issues in cybersecurity gained during the course, as well as their abilities to apply it in a given situation. Assessment of participation in seminars consists of: - practical exercises (e.g., impromptu debate, group analysis of news pieces related to cybersecurity, formulating policy recommendations, etc.) (20% of grade); - participation in discussions (capability to refer to academic literature, provide correct answers to questions related to course literature, identify specific problems related to cybersecurity, suggest and search for solutions, offer thoughtful critical remarks, contribute to other participants' ideas, etc.) (20% grade).
Student presentation	30	During the semester	Both the presentational skills and the academic quality of the presentation will be assessed. In addition, students will have to give each other feedback, peer feedback quality will also be assessed. The assessment will be based on: - content (comprehensive problem analysis, original personal insights, proper source application, critical analytical thinking, clear arguments conclusion/recommendation formulation) (15% of grade); - delivery (concentrated, efficient and convincing work presentation, adhesive scientific language, the use of informative visual measures) (5% of grade); - participation in discussion (providing correct answers to questions, offering thoughtful critical remarks, contributing to other participants' ideas, etc.) (5% of grade); - peer-review (essential and relevant comments, capability to critically assess the issues, to formulate problems and suggest (search for) solutions, to identify the most significant features) (5% of grade).

Final examination	30	At the end of the course	Written examination, students will have to choose and answer 3 open ended questions out of 5. Using notes is not allowed. 3 points are given for an outstanding performance: the student lives up to the course's goal description in an independent and convincing manner with no or few and minor shortcomings. 2 points are given for a good performance: the student is confidently able to live up to the goal description, albeit with several shortcomings. 1 point is given for an adequate performance: the minimum acceptable performance in which the student is only able to live up to the goal description in an insecure and incomplete manner.

Author	Year of publication	Title	Issue of periodical or volume of publication	Publishing place and house or web link
Compulsory reading				
Lessig, Lawrence	1999	Code: And Other Laws of Cyberspace		Basic Books
Perkovich, George & Ariel E. Levite (Eds.)	2017	Understanding Cyber Conflict: Fourteen Analogies		Washington, D.C: Georgetown University Press
Kello, Lucas	2017	The Virtual Weapon and International Order		Yale University Press
Choucri, Nazli, & David D. Clark	2019	International Relations in the Cyber Age		MIT Press
Russell, Alison Lawlor	2014	Cyber Blockades		Georgetown University Press
Farwell, James P., and Rafal Rohozinski	2011	'Stuxnet and the Future of Cyber War	Survival 53(1), pp. 23–40	
Rid, Thomas, and Ben Buchanan	2015	'Attributing Cyber Attacks'	Journal of Strategic Studies 38(1–2), pp. 4–37	
Nye, Joseph S.	2017	'Deterrence and Dissuasion in Cyberspace'	International Security 41(3), pp. 44–71	
Hansen, Lene, and Helen Nissenbaum	2009	'Digital Disaster, Cyber Security, and the Copenhagen School'	International Studies Quarterly 53(4), pp. 1155–75	
Dunn Cavelty, Myriam	2013	'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse'	International Studies Review 15(1), pp. 105–22.	
Wendt, Alexande	2015	Quantum Mind and Social Science		Cambridge University Press
Der Derian, James	2009	Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network		Routledge
Recommended reading				
Libicki, Martin C	2009	Cyberdeterrence and Cyberwar		Rand Corporation
Gartzke, Erik, and Jon R. Lindsay	2015	'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace'	Security Studies 24(2), pp. 316–48	
Eriksson, Johan	2001	'Cyberplagues, IT, and Security: Threat Politics in the Information Age'	Journal of Contingencies and Crisis Management 9(4), pp. 200–210	
Dunn Cavelty, Myriam	2007	Cyber-Security and Threat Politics: US Efforts to Secure the Information Age		Routledge
Project Q	2019	Recordings of the Q5 Symposium		University of Sydney
Stevens, Tim	2016	Cyber Security and the Politics of Time		Cambridge University Press