UNIVERSITY "UKSHIN HOTI" PRIZREN
International Summer School (ISS) 2026 Edition
Faculty of Law

SYLLABUS

Academic unit / faculty:	**Faculty of Law**			ISS edition:	**2026**
Course title:	**Cyberspace – Political and Social Aspects**				
Course status:	**Obligatory**	Code:		ECTS credits:	**4**
Teaching days/weeks:	**7 days / 1 weeks**	Teaching hours:		Lectures:	Exercises:
				7	**1**
Office hours:	**Daily (Monday-Friday, 1 Week)**				
Course professor 1. / Supervisor:	**Dr Tal PAVEL**		E-mail:	**Tal@cybureau.org**	
			Tel.:	**+40 725 694 194**	

COURSE CONTENT:

The course examines the political and social impacts of cyberspace.
Initially, it covers fundamental concepts of cyberspace before exploring the roles of different actors - including nation-states, cybercriminals, hacktivists, and terrorists - and the threats they present.
It highlights challenges faced by the state, organisations, and individuals, focusing on threats such as Social Engineering and the Dark Web, along with mitigation strategies.

Course objectives:	**Course learning outcomes:**
• Understanding the importance of cybersecurity. • The ability to obtain, select, analyse information, as well as to interpret it to comprehensively solve problems, challenges and incidents in the field of cyber security. • The ability to develop information security policies and management systems of the organisation.	Upon completing the course, students will be able to: • Analyse cyber security incidents, understand their political and social implications. • Identify and explain the roles of various actors in the political landscape of cybersecurity, including nation-states, non-state actors, and international organisations.

• The ability to flexibly use the acquired knowledge on cybersecurity in practice.	• Evaluate real-world instances of significant cybersecurity incidents and their political and social repercussions. • Understand and evaluate the methods and motivations behind cyber-attacks and develop strategies to mitigate social engineering attacks.

TEACHING METHODS:

- Lectures with active participation by the students,
- Explanation, discussion,
- Questions, cases.

CONDITIONS FOR COURSE IMPLEMENTATION:

Classroom equipped with computer, projector and other IT devices.

STUDENT EVALUATION METHODS AND GRADING SCALE:

The course is subject to continuous evaluation. At regular intervals we also ask students to participate in a more comprehensive evaluation. Student evaluation is done by exam, and the final grade consists of the following components:

- Regular and active attendance: 10%,
- **Midterm exam: 20%,**
- Course project: 10%,
- Final exam: 60%,

GRADING SCALE	
Evaluation in %	**Final grade**
91 – 100	10 (ECTS – A)
81 – 90	9 (ECTS - B)
71 – 80	8 (ECTS - C)
61 – 70	7 (ETCS - D)
51 – 60	6 (ETCS - E)
0 – 50	5* (ETCS – FX)

LANGUAGE OF EXAMINATION:

The examination tests are provided in English, and students submit their responses in English.

STUDENT DUTIES AND OBLIGATIONS:

Lectures	**Exercises and other study activities**
▪ Regular and active lecture attendance ▪ Active participation in discussions ▪ Respect of the University Code of Ethics etc.	▪ Regular attendance of exercises and study activities ▪ Respect of the University Code of Ethics etc.

STUDENT WORKLOAD:

Activity	**Hours**	**Days**	**Total hours**
Lectures	3	7	21

Exam assessment	2	3	6
Total student workload:			**101**
Note: 1 ECTS credit = 25 hours, for example if the course has 4 ECTS credits a student must have workload of at least 100 hours during the International Summer School (ISS).			

DAY	LECTURES		EXERCISES	
	Topic	**Hours**	**Topic**	**Hours**
1.	**Introduction to the Internet and Cyberspace** • Definitions • Internet, Web, Cyberspace • History • Features	3	**Exercise topic 1.** Discussion and distribution of the course project topics.	1
2.	**Introduction to Information Security** • Definitions • Data, Information, Security • Characteristics	3	**Exercise topic 2.** Assignments, quizzes and case studies related to the topic of the first day lecture.	1
3.	**Information Security Threats** • Definitions • Threat, Threat Agent • Threats categories	3	**Exercise topic 3.** Assignments, quizzes and case studies related to the topic of the second day lecture.	1
4.	**Social Engineering** • Definitions • History • TTPs • Prevention	3	**Exercise topic 4.** Assignments, quizzes and case studies related to the topic of the third day lecture.	1
5.	**Advanced Persistent Threat - APTs**	3	**Exercise topic 5.**	1

	• Definitions • APT vs Cybercrime • Russia, China, North Korea, Iran		Assignments, quizzes and case studies related to the topic of the fourth day lecture.	
6.	**Hacktivism – Anonymous and Wikileaks** • Definitions • Features • Ideology • Activities • Legacy	3	**Exercise topic 5.** Assignments, quizzes and case studies related to the topic of the fifth day lecture.	1
7.	**The Dark Web** • Definitions • Tools • Legitimacy • Content	3	**Exercise topic 7.** Assignments, quizzes and case studies related to the topic of the sixth day lecture.	1

LITERATURE:

- Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H. F., & Secret, A. (2023). The world-wide web. In *Linking the World's Information: Essays on Tim Berners-Lee's Invention of the World Wide Web* (pp. 51-65). https://dl.acm.org/doi/abs/10.1145/3591366.3591373
- Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710. https://hal.science/hal-03509116/
- Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69. https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf
- Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*. https://www.authorea.com/doi/full/10.22541/au.166385207.73483369/v1
- Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE access*, *10*, 39325-39343. https://ieeexplore.ieee.org/abstract/document/9743471
- Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *Ieee Access*, *9*, 11895-11910. https://ieeexplore.ieee.org/abstract/document/9323026
- Gawel, H. (2024). Hacktivism. *Internet Policy Review*, *13*(2), 1-12. https://policyreview.info/glossary/hacktivism
- Alexopoulou, S., & Pavli, A. (2021). 'Beneath This Mask There Is More Than Flesh, Beneath This Mask There Is an Idea': Anonymous as the (Super) Heroes of the Internet?. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *34*(1), 237-264. https://link.springer.com/article/10.1007/s11196-019-09615-6
- Hooper, S. J. (2023). Explaining Wikileaks and Julian Assange as structural threats to the liberal ideological hegemony of American foreign policy. *International Politics*, *60*(3), 616-634. https://link.springer.com/article/10.1057/s41311-022-00421-9
- Geenens, P. (2020). How worried should you be about nation-state attacks?. Network Security, 2020(3), 17-19.

- Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures. *Journal of ambient intelligence and humanized computing*, *14*(7), 9355-9381. https://www.proquest.com/openview/40bb014a782f41c0d3d7c655579786d0/1?pq-origsite=gscholar&cbl=2043913
- Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: A systematic approach. *Ieee Access*, *8*, 171796-171819.
- Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, *46*(3), 502-533. https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117
- Saleem, J., Islam, R., & Islam, M. Z. (2024). Darknet traffic analysis: A systematic literature review. *IEEE Access*, *12*, 42423-42452. https://ieeexplore.ieee.org/abstract/document/10460558

REMARKS FOR STUDENTS:

- Student should be aware of and respect the institution and Code of ethics.
- Student should respect the schedule of lectures, exercises and other study activities.
- Student should possess and show student ISS ID card during exam.
- Student course project/presentation/homework must comply with professor instructions.
- During the exam is strictly forbidden to use of mobile phone devices.