Cyber Security and Law (MA)

Syllabus

2025/2026 Spring

Subject's code: HOE7150

Subjects capacity: 6 ECTS credits

Language: English

Subject's aims/objectives: To get an overview about the legal basis of cyber security in different levels and acquire a broader perspective for the assessment the role of regulatory frameworks in the process of cybersecurity management.

Topics covered:

1. Introduction to cybersecurity and basics
2. Cyber history and normative frameworks
3. Cybersecurity strategies
4. Cybersecurity and the EU
5. Cybercrime
6. Politically motivated cyber operations
7. International case studies
8. International law and cyber activities

Learning outcomes:

By the end of the course the student:

- Describes the evolution and basic concepts of cyber security
- Assesses the role of law among other dimensions of cybersecurity management
- Is able to identify the levels and sources of legal norms applicable to cyber security
- Analyses legal aspects of cyber security incidents internationally

Subject matter and study process: This course is designed for students without technical background. Its purpose is to provide a general understanding of the nature of cyber security challenges and it will examine a wide spectrum of legal areas and existing instruments relevant to the field. This course will mainly focus on European and international regulation of cyber security and it will place the substantive legal framework into a comprehensive perspective, by elaborating on some technological, military, policy, economic aspects as well. Topics discussed cover concepts, definitions related to cybersecurity, EU regulatory framework related to cybersecurity in the information society, cybercrime, international law and cyber operations.

Lectures start with presenting current media reports. Any student can be called upon and expected to outline a current news piece in the field of cybersecurity and law. The aim is to get familiar with and learn to read cybersecurity-related news, discuss unknown words, concepts, clarify technical and other questions, so informed questions are encouraged. By the

end of the course students should be able to independently identify legal issues in media pieces reporting about cybersecurity. Also it is important to get acquainted with terms that are commonly used and be aware of media hypes.

Following the news-sessions, course material will be delivered in interactive lecture format, where the previously indicated discussion points will be raised and students will be required to share their views. Students will be called-upon randomly to answer questions, offer positions and participate in discussions. Materials, including course slides, will be made available in Moodle in due course.

All dates, topics and material are subject to changes and constantly developing. Indicated reading is mandatory in cases of normative material posted or hyperlinked in Moodle. Other sources are recommended unless marked otherwise. Lecturer may clarify during the lectures the exact scope of mandatory reading, add new sources.

Evaluation method: Differentiated grading and non-graded evaluation

Final grade composition: Active participation (see below) is a prerequisite. Exam gives 100% of the final grade.

Coverage of SDG and ERS: Not covered

Students: This is a compulsory course for students studying on HAJM programme

Special needs: Persons with disabilities can participate in this course. Please inform the professor(s) in the beginning of the course of any special instruction, or assessments of this course that may be necessary to enable you to fully participate in this course.

Registration: Students who would like to take the course should declare the course in the ÕIS (Student Information System) by deadlines set in the academic calendar.

Prerequisite knowledge: Preferably knowledge of EU Institutional Law, Criminal Law, Public International Law

Prerequisite resources: MS Office programmes. For free student download see the instructions https://confluence.ttu.ee/it-info/it-arvuti-ja-oppetoeoekoht/arkvara/microsoft-office-kodukasutus

Lecturers: Agnes Kasper, PhD

E-mail: agnes.kasper@taltech.ee

Office hours: by appointment

Preferred means of contact: message via Moodle or by email, responses within 5 workdays

Schedule for the classes: Tuesdays 17.45-21.00, weeks: odd (03 Feb, 17 Feb, 03 March, 17 March, 31 March, 14 Apr, 28 Apr, 12 May)

Seminars (case studies) : 16.00-17.30 (before the lecture) 17 March, 31 March, 28 April, 12 May.

Venue: SOC-308 and SOC-213. The course is planned as primarily in-person participation format. However, the lecturer may enable online participation via videolink (eg. BBB in Moodle). Further details are provided before each lecture.

E-support: Course materials, assignments and submission venues are accessed via the e-learning environment Moodle under the course title HOE7150 Cyber Security and Law (2026 spring).

Course link: https://moodle.taltech.ee/course/view.php?id=37162

Enrolment method: self-enrolment, inactive users are automatically removed after 90 days

Enrollment key: APT1

Study literature: Study literature is continuously developing and is based on current legislative frameworks and new initiatives. Students are expected to read all legal instruments referred during the lectures and in the course page. Key literature and recommended literature will be indicated and distributed in Moodle. Select key literature:

- Handbook on Cyber Security (Volume V, 2nd edition, 2019), https://esdc.europa.eu/documentation/handbook-on-cyber-security/
- Ramses A. Wessel, European law and cyberspace. In: Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Elgar Publishing, 2021, eISBN: 9781789904253, DOI: https://doi.org/10.4337/9781789904253
- "The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms" by Nikola Pijović. (See in CYCON 2021 Proceedings, Chapter 12, pp. 215-231)
- Osula, Anna-Maria; Kasper, Agnes; Kajander, Aleksi (2022). EU common position on international law and cyberspace. Masaryk University Journal of Law and Technology, 16 (1), 89−123. DOI: 10.5817/MUJL2022-1-4.
- Tallinn Manual 2.0, Cambridge, 2017
- Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States (2025) available at https://ccdcoe.org/library/publications/handbook-on-developing-a-national-position-on-international-law-and-cyber-activities-a-practical-guide-for-states/
- CyberLaw Toolkit available at https://cyberlaw.ccdcoe.org/wiki/Main_Page

Course requirements and assessment:

1. ***Prerequisites: Active participation – NON-GRADED (pass/fail)***

- Daily media reports. Students are required to present and discuss 2-3 current, cybersecurity-related news from the media at each lecture.
- Presentation/report. Each student is required to make a presentation based on assigned questions and/or material. Presentation should be 15-20 minutes long and make use of a presentation software. Depending on the number of students presentation can be given as a group assignment. Further instructions will be posted in Moodle in February, when all course registrations are done.

2. ***Exam - GRADED, 100%***

Students complete a comprehensive multiple choice/short answer quiz in Moodle. Open book. Individual work. Eligibility for assessment: satisfactory and timely completion of prerequisites (media reports and presentation).

Final grade is calculated in the following manner

A(5)-100%-91%

B(4)- 90%- 81%

C(3)- 80%-71%

D(2)- 70%- 61%

E(1)- 60%- 51%

F(0)- 50% -0%

Evaluation criteria

1. **ACTIVE PARTICIPATION – Non-graded, prerequisite (P/F)**

Minimum requirements to pass:

- ***6 media reports are submitted, AND***
- ***Satisfactory presentation.***

Submission of daily media reports. Minimum 6 media reports must be submitted. Media reports are evaluated on a non-graded basis. Students are called upon randomly to present and discuss their news reports. The student's reports are deemed Satisfactory if the topic is presented clearly and understandably, discussion and explanations are understandable, important information differentiates from less important, individual effort is clearly visible. If a student present at the lecture is not called upon to present or discuss a media report at the lecture, it is still deemed that (s)he has submitted a Satisfactory media report. Media reports for missed classes can be submitted in Moodle.

Presentation: Presentations are evaluated on a non-graded basis. Presentations are deemed Satisfactory if the assigned topic/material is presented clearly and understandably, discussion and explanations are understandable, important information differentiates from less important, individual effort is clearly visible. Presentation is a *prerequisite* for the completion of the course.

COURSE SCHEDULE

The plan, topics and schedule are subject to change without prior notice

Date and topic	***Keywords and discussion points***	***Useful reading & normative material***	***Assignments for next lecture***
03 Feb 2026 Topic 1. Course intro and cyber history Topic 2. Introduction and normative frameworks	Keywords: Admin matters, history, basic concepts, norms in cyberspace, current and emerging frameworks Discussion points: **„Do legal norms matter in cyberspace? Why?“** **“Is there such a thing as cyberlaw?”**	1. Syllabus, course requirements, schedule, etc. (available in Moodle) 2. IT for lawyers (available in Moodle) 3. Geers – Strategic Cyber Security, Chapter 2.2 A technical primer (available in Moodle) 4. Barlow – Declaration of Independence of Cyberspace https://www.eff.org/cyberspace-independence 5. Tsagourias – The Legal Status of Cyberspace https://www.elgaronline.com/view/9781782547389.00010.xml	1. Prepare Cybersecurity news for next lecture 2. Read: Easterbrook – Cyberspace and the Law of the Horse https://chicagounbound.uchicago.edu/journal_articles/1148/ 2. Read 1 national cybersecurity strategy for next lecture. See Cyber Strategies in CCDCOE database https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies 3. Read NIS2 Directive- and your own country’s national legislation implementing the NIS/NIS2 Directive
17 Feb 2026 Topic 3. Cybersecurity Strategies Topic 4. Cybersecurity & the EU	Keywords: National cybersecurity strategies, cyber resilience, cyber-specific regulation	1. Guide to Developing a National Cybersecurity Strategy, pages 27-53 (also see https://ncsguide.org/)	1. Cybersecurity news for next lecture 2. Presentation deliverable assigned to groups/individuals 3. Read Council Regulation (EU)

	Discussion point for lecture: „**What are the main points in your country's cybersecurity strategy?** **What is the role of law/regulation in the strategy?**“ **Is there a need for further security requirements beyond the NIS2? Why? What are the key differences and improvements between NIS1 and NIS2?**	2. EU Cybersecurity Strategy 2020 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 3. Handbook on Cyber Security, 2019 https://esdc.europa.eu/documentation/handbook-on-cyber-security/ 4. Ramses A. Wessel, European law and cyberspace. In: Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Elgar Publishing, 2021, eISBN: 9781789904253, DOI: https://doi.org/10.4337/9781789904253 NIS Tool https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool NIS2 Directive 2022/2555 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2555	2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
03 March 2026 Topic 5 and 6. Cybersecurity & the EU	Keywords: cyber resilience, cyber-specific regulation, cyber diplomacy, intermediary liability, sectoral cybersecurity regulations	1. EU Cybersecurity Act Regulation (EU) 2019/881 2. Draft Council Conclusions on a Framework for a Joint EU Diplomatic	1. Cybersecurity news for next lecture 2. Read the following CJEU judgements:

	What is the importance of standards and certification schemes in cybersecurity? **What does the term 'cyber diplomacy' mean? How does the cyber sanctions regime relate to attribution?** **In which cases can intermediaries be held liable for cyberattacks conducted by third parties using the intermediary's infrastructures?** **Which sector's legislation imposes the highest security requirements for its subjects? Why?**	Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") of 7 June 2017, nr 9916/17 3. Cyber sanctions, see https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/ 4. Digital Services Act Regulation (EU) 2022/2065 5. European Electronic Communications Code Directive (EU) 2018/1972 6. e-Privacy Directive 2002/58/EC 7. eIDAS Regulation (EU) No 910/2014 8. Payment Services Directive 2 Directive (EU) 2015/2366	Digital Rights Ireland (Joined Cases -293/12 and C-594/12) and Tele2 Sverige (C-203/15)
17 March 2026 Topic 7. Cybersecurity & the EU Topic 8. Cybercrime	Keywords: new initiatives for cyber resilience; data retention; tension between cyber investigations, criminal justice and human rights, intro to cybercrime, Botnet Directive, Budapest Convention **What is the relation between software vulnerabilities, updates and cybersecurity? Who**	1. DORA 2. Cyber Resilience Act 3. AI Regulation 4. E-Privacy Regulation 5. Cybercrime Convention / Budapest Convention https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185	1. Cybersecurity news for next lecture 2. Read Cybercrime Convention, https://www.coe.int/en/web/cybercrime/the-budapest-convention 3. Read DNS changer case (in Moodle)

	is liable for insecure products? Is there an obligation to patch known vulnerabilities? **What is the difference between data retention and quick freeze of data?** **Which one, in your opinion is more invasive in terms of violation of privacy?** **Is the Budapest Convention implemented in your country? To what extent?**	6. Botnet Directive https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32013L0040 7. Report on Botnet Directive implementation https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505307728824&uri=COM:2017:474:FIN	
31 March 2026 Topic 9 & 10. Cybercrime	Keywords: Substantive law in Budapest Convention, case studies - core cybercrimes & computer-related crimes Discussion points: **Complex cybercrime cases**	1. Lecture material – case studies 2. See in Moodle	1. Cybersecurity news for next lecture – find a news report about a core cybercrime and a computer-related crime
14 April 2026 Topic 11 & 12 International norms & cyber activities	Keywords: international cyber incidents, cyberespionage, Stuxnet, Wannacry, ID Card, UN GGE, UN OEWG, international norms Discussion points: **What are the most known cyber**	1. Significant cyber incidents - https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents 2. UN site on Developments in the field of information and telecommunications in the context of	1. Cybersecurity news for next lecture 2. Read: GGE Report A/76/135, https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

	incidents in your country? **What legal regimes may be applicable to the discussed cyber incidents?** **What is your country's position in/on the OEWG on Information Security?** **What norms of responsible state behaviour were proposed by the GGEs?** **Do voluntary norms matter in cyberspace? Do we need a new cybersecurity convention? Why?** **What are the two main approaches to international regulation of cyber operations?**	international security - https://www.un.org/disarmament/topics/informationsecurity/ 3. UN site for documents and statements related to the OEWG https://meetings.unoda.org/meeting/57871/statements 4. Schmitt and Vihul, The Nature of International Cyber Norms, IN: Osula and Rõigas (eds.) International Cyber Norms: Legal, Policy and Industry Perspectives - https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch2.pdf 5. "The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms" by Nikola Pijović. (See in CYCON 2021 Proceedings, Chapter 12, pp. 215-231)	
28 April 2026 Topic 13 & 14 International law and cyber activities	Keywords: peacetime regimes, below the use of force threshold, jus ad bellum, jus in bello Discussion points: **How does the principle/rule of**	1. Tallinn Manual 2.0 (available in Moodle) 2. See in Moodle	1. Prepare presentation

	sovereignty applies to cyber operations? **When does a cyberattack amount to use of force? Any examples?** **What is the meaning of 'direct participation in hostilities' in cyber conflict?**		
12 May 2026	Presentations/reports		Exam opens in Moodle
2 May 2026	Exam submission deadline		See in Moodle