Syllabus of Record

Program: CET Prague
Course Code / Title: PR/PPOL 310 AI and Cybersecurity Policy in Contemporary Europe
Contact Hours: 45
Recommended Credits: 3
Primary Discipline / Suggested Cross Listings: Public Policy / Information Technology, International Relations, Central European Studies
Language of Instruction: English
Prerequisites / Requirements: None

Description
Rapid advances in digital technologies and artificial intelligence have introduced a wide range of cybersecurity challenges and AI-related risks that increasingly affect critical infrastructure, supply chains, and democratic institutions. This course explores European cybersecurity and AI governance through the lens of law, politics, and technology, with a focus on the Central and Eastern European region. It examines how the EU responds to digital threats with frameworks such as NIS2, the Cyber Resilience Act, and the AI Act, while comparing these approaches with U.S. strategies on cybersecurity and artificial intelligence. Emphasis is placed on policy, governance, and the societal impact of emerging technologies, providing students with tools to critically assess regulatory choices in an insecure world.

Objectives
Through their participation in this course, students will:

- Gain an understanding of the European Union's cybersecurity and AI governance legal frameworks (e.g., NIS2, Cyber Resilience Act, AI Act) and their implications for CEE (Central and Eastern European) countries.
- Analyze the intersection of law, policy, and technology in shaping responses to cybersecurity and AI-related risks.
- Compare European approaches with those of the United States and other global actors, highlighting similarities, divergences, and lessons learned.
- Identify and critically assess how cybersecurity and AI governance frameworks affect different social groups unequally in CEE societies.
- Engage with diverse local voices in cybersecurity policy (e.g., practitioners, researchers, regulators, and civil society) to build an inclusive understanding of digital resilience.
- Develop the ability to evaluate real-world case studies of cyber incidents and AI governance challenges from a policy perspective.
- Strengthen practical policy analysis skills by connecting theoretical frameworks with contemporary cybersecurity practice (e.g., risk management, vulnerability disclosure, resilience building).

Requirements

Active participation is essential in this course. Students are expected to attend each class and field study course component, as outlined in the CET Attendance Policy. Students are expected to read all assigned materials before the relevant class session and come prepared to participate thoughtfully in class discussions. Reading assignments are generally 10-20 pages per class session. All assignments must be submitted via Canvas unless otherwise noted.

Graded assignments include:

- **Participation:** "Participation" does not mean a mere passive presence in classes. Participation means active participation in the course discussions based on assigned readings and student's own sources. Students should always be ready to answer any of the questions/tasks related to weekly assignments in the syllabus. All course components are considered, including field experiences.

- **Homework:** Throughout the semester the student submits two short response papers to selected readings and two reflection journal entries (approximately 750 words each).

- **Presentation:** Each student will prepare a 10-minute presentation for the class, with 5 minutes for questions afterwards. The presentation draws on case studies to illustrate concepts discussed in the assigned reading and in the course.

- **Final research paper:** The final paper comprises 8-10 pages on a topic determined in consultation with the instructor.

- **Final quiz:** The final quiz covers the understanding of key themes and assigned readings from the entire course. The quiz will consist of a combination of multiple-choice and short-answer questions.

Grading
The final grade is determined as follows:

Participation *(see rubric below)*	20%
Homework (4 at 5%)	20%
Presentation	15%
Final research paper	20%
Final quiz	25%

Class Participation Grading Rubric

	A – 90-100% Exemplary	B – 80-89% Proficient	C – 70-79% Developing	D – 60-69% Unacceptable	F – 0-59% Missing
Frequency of class participation	Actively contributes 2+ times per meeting	Actively contributes at least 1 time per meeting	Actively contributes at least half of the time during term	Actively contributes less than half of the time during term	Does not contribute
Quality of class participation*	Contribution is always thoughtful, accurate, and constructive, frequently interacting with peers	Contribution is mostly thoughtful, accurate, and constructive, usually interacting with peers	Contribution is somewhat thoughtful, accurate, and constructive, sometimes interacting with peers	Contribution is rarely thoughtful, accurate, and constructive, rarely interacting with peers	Does not contribute or interact with peers
Level of class preparation	Always fully prepared and on task	Mostly prepared and on task	Somewhat prepared and on task	Rarely prepared and on task	Consistently unprepared and not on task

Readings / Resources

2024 Report on the State of the Cybersecurity in the Union, https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations, March 2025. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?utm_source=chatgpt.com

Barbierato, E., and A. Gatti. "The Challenges of Machine Learning: A Critical Review." *Electronics* 13 (2024): article 416. https://doi.org/10.3390/electronics13020416

Bommasani, R., et al. *On the Opportunities and Risks of Foundation Models*. 2021. https://crfm.stanford.edu/report.html

Bommasani, R., et al. "Do Foundation Model Providers Comply with the Draft EU AI Act?" 2023. https://crfm.stanford.edu/2023/06/15/eu-ai-act.html

Bygrave, Lee A. “The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes.” *Computer Law & Security Review* 56 (2025): 106071. https://doi.org/10.1016/j.clsr.2024.106071

Critical Infrastructure Association of the Slovak Republic. *Cybersecurity in Slovakia: How to Protect Against Growing Threats?* 30 March 2025. https://www.akisr.sk/cybersecurity-in-slovakia-how-to-protect-against-growing-threats

Dickmann, R. “Vulnerability Management as Compliance Requirement in Product Security Regulation—A Game Changer for Producers’ Liability and Consequential Improvement of the Level of Security in the Internet of Things?” *International Cybersecurity Law Review* 4 (2023): 21–37. https://doi.org/10.1365/s43439-022-00064-9

Dunn Cavelty, M., & Wenger, A. (Eds.). (2022). Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation (1st ed.). Routledge. https://doi.org/10.4324/9781003110224

Enakome Oka, M., and M. Hromada. “The Role of Auditors in Critical Infrastructure Protection: Case in Czech Republic.” *Transportation Research Procedia* 74 (2023): 1239–1245. ISSN 2352-1465. https://doi.org/10.1016/j.trpro.2023.11.267

European Union Agency for Cybersecurity (ENISA). *Cybersecurity of AI and Standardisation (Report)*. March 2023, https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport

European Union Agency for Cybersecurity (ENISA). *Securing Machine Learning Algorithms* (Report). December 2021, https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms

European Union Agency for Cybersecurity (ENISA). *Standardisation in support of the Cybersecurity Certification*. February 2020, https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i

European Union Agency for Cybersecurity (ENISA). Artificial Intelligence and Cybersecurity Research, June 2023 https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research

European Union Agency for Cybersecurity (ENISA). How to set up CSIRT and SOC. December 2020 https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

The EU’s Cybersecurity Strategy for the Digital Decade. 14 December 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

FIRST: Computer Security Incident Response Team (CSIRT) Services Framework https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

Gardenier, A. M. "From Criminal to Crucial Participation: The Case of Dutch Volunteer Hackers." *Social Inclusion* 13, no. 1 (2025). https://www.researchgate.net/publication/388526175_Modernizing_Hungary's_Cybersecurity_Framework_Addressing_Evolving_Threats_and_Enhancing_National_Resilience

Goanta, Catalina, et al. "The Great Data Standoff: Researchers vs. Platforms Under the Digital Services Act." *arXiv preprint* arXiv:2505.01122, 2025.

Grotto, A. J., and J. Dempsey. "Vulnerability Disclosure and Management for AI/ML Systems: A Working Paper with Policy Recommendations." Working paper, November 15, 2021. Available at SSRN: https://ssrn.com/abstract=3964084

Kelemen, R., et al. "Modernizing Hungary's Cybersecurity Framework: Addressing Evolving Threats and Enhancing National Resilience." *Rechtskultur*, December 2024. https://doi.org/10.36213/01-20

Kilian, R., et al. "European AI Standards – Technical Standardization and Implementation Challenges under the EU AI Act." February 26, 2025. http://dx.doi.org/10.2139/ssrn.5155591

Koltn N., et al. "Responsible Reporting for Frontier AI Development." 2024. https://arxiv.org/abs/2404.02675

Kuhl, Katherine. *Pegasus in Hungary: Analyzing Hungary's Use of Pegasus on Journalists with Lessig's Four Modalities of Regulation* (Senior thesis, Fordham University, International Studies, 2024) Fordham Research Commons https://research.library.fordham.edu/cgi/viewcontent.cgi?article=1138&context=international_senior

Krishnan, Naveen. "AI Agents: Evolution, Architecture, and Real-World Applications." *arXiv preprint* arXiv:2503.12687, 2025.

Liszkowska, D. "'Cybersecurity and Threats to Electoral Processes in Central European States on the Example of Poland and Germany'." *Przegląd Zachodni*, no. 4 (2024): 55–68. https://doi.org/10.60972/PZ.2024.4.55

Ludvigsen, Kaspar Rosager. "Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law." *arXiv preprint* arXiv:2503.07250, 2025.

Metcalf, J., and R. Singh. "Scaling Up Mischief: Red-Teaming AI and Distributing Governance." *Harvard Data Science Review*, Special Issue 5 (2024). https://doi.org/10.1162/99608f92.ff6335af

Petrová, K., J. Spatenka, and L. Vaclavik. "Assessment of Cybersecurity of Organizations: An Empirical Study of Czech and Slovak Organizations." *Journal of Eastern European and Central Asian Research (JEECAR)* 11, no. 3 (2024): 668–682. https://doi.org/10.15549/jeecar.v11i3.1666

Radoniewicz, F. Cybercrime in Selected European Countries (2022). In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) Cybersecurity in Poland. Springer, Cham. https://doi.org/10.1007/978-3-030-78551-2_25

Rampášek, M., M. Mesarčík, and J. Andraško. "Evolving Cybersecurity of AI-Featured Digital Products and Services: Rise of Standardisation and Certification?" *Computer Law & Security Review* 56 (2025): 106093. https://doi.org/10.1016/j.clsr.2024.106093

Ristevska, Tea. *Enhancing Cybersecurity Cooperation in Central and Eastern Europe.* Pulaski Policy Paper, No. 11 (Warsaw: Pulaski, 23 October 2024). https://pulaski.pl/wp-content/uploads/2024/10/Pulaski_Policy_Paper_No_11_2024.pdf

Terlecka-Maciejewska, M. "Cybersecurity in Polish Security System." *Scientific Papers of Silesian University of Technology. Organization and Management Series*, no. 198, article 31 (2024?). https://managementpapers.polsl.pl/wp-content/uploads/2024/07/198-Terlecka-Maciejewska.pdf

Villani, S. "The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System." *European Journal of Risk Regulation* 16, no. 2 (2025): 485-497. https://doi.org/10.1017/err.2025.24

Zou, Andy, et al. "Security Challenges in AI Agent Deployment: Insights from a Large Scale Public Competition." *arXiv preprint* arXiv:2507.20526, 2025.

Content

Topic 1 – Cybersecurity and AI in a Changing Security Environment

- From Cold War to Cyber War, Historical evolution of European (in)security and digital threats.
- How AI reshapes threat landscapes (deepfakes, autonomous attacks, AI-enhanced defense)
- Impact on critical infrastructure, supply chains, and democratic institutions

Topic 2 – European Cybersecurity Governance and Policy Landscape

- The EU's Cybersecurity Strategy for the Digital Decade
- Multi-layered EU frameworks (NIS2, Cybersecurity Act, Cyber Solidarity Act)

- National strategies and implementation challenges in CEE
- Institutional actors: European Commission, ENISA, CSIRTs

Topic 3 – Cybersecurity Policy and Governance in CEE under NIS2
- How NIS2 reshapes national cybersecurity strategies and institutions
- Local approaches across Slovakia, Czechia, Poland, and Hungary
- Policy trade-offs between centralization, national sovereignty, and EU harmonization
- Capacity and resource challenges in CEE for meeting EU cybersecurity ambitions

Topic 4 – Critical Infrastructure and Operational Technology (OT) Security
- Distinctions between IT and OT risks (energy grids, healthcare systems, transport)
- Securing industrial control systems and manufacturing environments
- Case examples of OT vulnerabilities (e.g., Colonial Pipeline, FrostyGoop)
- Policy and governance approaches for OT in CEE

Topic 5 – Cyber Resilience Act and Cybersecurity of Digital Products
- Security-by-design and lifecycle obligations, conformity, CE marking
- How CRA impacts software vendors, SMEs, and global supply chains
- Links to the EU's broader digital product safety framework (e.g., Radio Equipment Directive, AI Act, Product Liability Directive).
- Contrast with US approaches to product security

Topic 6 – AI Act and AI-Driven Cybersecurity
- AI Act's risk-based categories and security implications
- AI in defense and AI in offense: dual-use dilemmas
- AI agents and Agentic AI
- Trustworthy AI: explainability, bias, and governance

Topic 7 – Cybersecurity Governance and Organizational Responsibility
- Corporate accountability, board-level oversight, and liability
- Case studies: *SolarWinds* (supply chain breach), *Uber* (breach disclosure failure)
- CISO and compliance functions in EU regulatory context (NIS2, DORA)

Topic 8 – Security Research, Ethical hacking and Vulnerability Disclosure
- Coordinated Vulnerability Disclosure (CVD), Bug bounty programs, Ethical hacking, NVD, CVE, EUVD
- Testing security of AI
- Tensions between criminal law and protection of good-faith researchers
- Practical experiences from CEE ethical hackers and CSIRTs

Topic 9 – US–EU Comparative Perspectives on Cybersecurity and AI
- US model: market-driven, voluntary frameworks (e.g., NIST), executive orders
- EU model: regulatory harmonization and rights-based governance

- Certification, EU Cybersecurity Act, EU harmonized standards, standardisation of AI
- AI governance divergences and prospects for transatlantic cooperation

Topic 10 – Cybercrime, EU law and International Treaties

- Budapest Convention on Cybercrime and its relevance to CEE, UN Cybercrime Convention, EU E-evidence package
- E-evidence, orders, service providers
- Ransomware
- Balancing state security, digital rights, and cross-border cooperation

Topic 11 – Digital Rights in Cyberspace

- Cybersecurity's unequal social impacts in CEE (access, data retention, surveillance)
- Algorithmic bias and discrimination in AI systems (predictive policing, automated decision-making, facial recognition)
- Disinformation and platform governance (TikTok/ByteDance case, Meta's role in elections, Russian/Chinese influence campaigns in CEE, Pegasus surveillance)
- Civil society and NGO voices in regional cybersecurity debates

Topic 12 -- Roles, Skills and Workforce

- ENISA's European Cybersecurity Skills Framework (ECSF) and workforce challenges, roles and skills, cybersecurity workforce shortage and skills gap, NICE Workforce Framework for Cybersecurity
- Cybersecurity managers, Auditors, CSIRT, ISAC, SOC
- Building resilience through education, training, and inclusive policies
- Women in CyberSecurity, Women4Cyber, ŽenyVKyber
- Workforce in AI, AI literacy

Field study and experiential learning components may include:

- Pentest Lab/Security Operations Center, or CSIRT unit

Syllabus of Record is subject to minor changes in Term-specific Syllabus at faculty's discretion.