GHENT UNIVERSITY

Course Specifications

Valid as from the academic year 2024-2025

Selected Issues: Cybercrime, Technology and Surveillance (B001717)

Course size *(nominal values; actual values may depend on programme)*

Credits 6.0 **Study time 180 h**

Course offerings and teaching methods in academic year 2026-2027

A (semester 2)	English	Gent	lecture
			independent work

Lecturers in academic year 2026-2027

Verdoodt, Valerie	RE21	lecturer-in-charge
Hardyns, Wim	RE23	co-lecturer

Offered in the following programmes in 2026-2027	**crdts**	**offering**
Master of Science in Teaching in Social Sciences(main subject Laws)	6	A

Teaching languages

English

Keywords

Cybercrime, technology, Information- and Communication Technologies (ICT), surveillance, big data, criminal law, fundamental rights, data protection, artificlal intelligence

Position of the course

The aim of the course is to gain a multi-perspective understanding of and insight into cybercrime phenomena, online risk behaviour, the use of technology and data analytics for law enforcement and intelligence purposes, and public and private sector surveillance strategies. The course focuses on the prevalence and etiology of cybercrime phenomena, historic, recent and actual developments at international and European level and societal, (criminal) policy and legislative approaches to cybercrime, the use of technology and surveillance.

Contents

- Phenomena: description and analysis of cybercrime phenomena, their prevalence and victim and offender characteristics, including hacking, ransomware, phishing, identity theft, online fraud & extortion, cyberharassment & -bullying, content-related offences (e.g. hate speech, child sexual abuse material), attacks on Critical (Information) Infrastructure, and cyberwarfare
- Technology dimension: use of technology and (big) data analytics for law enforcement and intelligence purposes, including predictive policing approaches, use of drones, (body)cameras and biometrics, smart infrastructures, the internet of things (IoT), and deployment of surveillance technology
- Legal dimension: national, European, international and comparative legislative approaches to cybercrime, technology & surveillance, including substantive law, procedural law, jurisdiction, liability, cybersecurity aspects, data protection and fundamental rights aspects
- European and international policy: EU (Council, European Commission, European Parliament, Fundamental Rights Agency, Europol, EC3, ENISA, Eurojust, Frontex), Council of Europe, OSCE, OECD and UN
- Multi-actor dimension: law enforcement authorities, intelligence services, CSIRTs, international & supranational organisations, companies (corporate social responsibility, self-regulation, cybersecurity and data breach obligations), data protection authorities, victim support services and digital literacy actors.

Initial competences

The student has successfully finished the courses of Substantive and Procedural Criminal Law, has knowledge of European and international institutional and policy developments, sufficiently masters scientific research methods or has obtained the above required competences in another way. The student is able to independently read and analyse articles in English.

Final competences

1 Identify, understand and interpret the relevant criminological and legal principles, instruments and case-law with regard to cybercrime, technology and surveillance.
2 Develop, articulate and orally present a critical and argumented opinion on the various criminological and legal dimensions and aspects of cybercrime, technology and surveillance.
3 Collecting, critically analyzing and scientifically evaluating(historical) sources, (scientific) literature and (empirical) research data concerning cybercrime, technology and surveillance and reactions thereto.
4 Write a clear report in team context on the results of scientific research and own critical opinion.
5 Develop a life-long learning attitude with regard to issues related to cybercrime and surveillance, by identifying, interpreting and reflecting on actual developments.

Conditions for credit contract

Access to this course unit via a credit contract is unrestricted: the student takes into consideration the conditions mentioned in 'Starting Competences'

Conditions for exam contract

This course unit cannot be taken via an exam contract

Teaching methods

Lecture, Independent work

Study material

Type: Slides

Name: Cybercrime, Technology and Surveillance
Indicative price: Free or paid by faculty
Optional: no
Language : English
Available on Ufora : Yes
Online Available : Yes
Available in the Library : No
Available through Student Association : No

Type: Reader

Name: Cybercrime, Technology and Surveillance
Indicative price: Free or paid by faculty
Optional: no
Language : English
Available on Ufora : Yes
Online Available : Yes
Available in the Library : No
Available through Student Association : No

References

See course material.

Course content-related study coaching

The lecturers will provide information and guidance regarding the format and teaching methods of the course. The lecturers are available for questions and feedback.

Assessment moments

end-of-term and continuous assessment

Examination methods in case of periodic assessment during the first examination period

Oral assessment

Examination methods in case of periodic assessment during the second examination period

Oral assessment

Examination methods in case of permanent assessment

Peer and/or self assessment, Assignment

Possibilities of retake in case of permanent assessment

examination during the second examination period is possible

Extra information on the examination methods

Periodic evaluation (60%): The exam is oral by default; if the number of students (across the various programmes in which the course is offered) surpasses 90, the lecturers retain the right to organise the exam for all students as a written exam, or to allow students the option to take the exam as a written exam (opt-in). The exam consists of short-answer questions and open questions, based on the materials and discussions during the lectures. Open questions envisage testing students' knowledge, understanding and analytical and interpretational skills regarding the causes, mechanisms, dynamics, complexity and interrelations of the phenomena concerned and societal, (criminal) policy, legislative and human-rights based approaches thereto.

Permanent evaluation (40%): group assignment on a question related to cybercrime, technology and surveillance. Guidelines on the use of generative AI tools provided by the lecturers must be respected. The evaluation consists of:

- Assignment (30%): the group work is assessed by the lecturers.Based on peer-feedback concerning the collaboration within the group, the group grade may be adjusted on an individual basis.
- Peer evaluation (10%): assessment of another group's assignment.

Second examination period: an individual assignment replaces the group assignment.

Students can only pass the course if both periodic and permanent evaluations are taken. If the student does not participate in the permanent evaluation in the first examination period, the exam can still be taken. The score for the exam is then carried over to the second chance period. If the student participates in the permanent evaluation and does not participate in the exam during the first examination period, the score for the permanent evaluation can be transferred to the second chance period or a revised paper can be submitted during the second chance period.

Calculation of the examination mark

- Periodic evaluation: 60%
- Permanent evaluation: 40%

The student is obliged to participate in all evaluations (both non-periodic and periodic); otherwise, he/she will be declared "failed" for the course. This means that if the final score is ten or more (out of twenty), this score will be reduced to the highest non-passing grade.