GHENT UNIVERSITY

Course Specifications

Valid as from the academic year 2019-2020

Selected Issues: Cybercrime, Technology and Surveillance (B001531)

Due to Covid 19, the education and evaluation methods may vary from the information displayed in the schedules and course details. Any changes will be communicated on Ufora.

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

Credits 4.0 **Study time** 120 h **Contact hrs** 45.0 h

Course offerings in academic year 2023-2024

A (semester 2) English Gent

Lecturers in academic year 2023-2024

Offered in the following programmes in 2023-2024	crdts	offering

Teaching languages

English

Keywords

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

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 pornography, copyright infringements), 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 and French.

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 substantiated opinion on the various criminological and legal dimensions and aspects of cybercrime, technology and surveillance.
3 Independently consult, analyse and critically and scientifically assess (historical) sources, (scientific) literature and (empirical) research data concerning cybercrime, technology and surveillance and reactions thereto.
4 Write a clear report on the results of (own) scientific research and/or personal views.
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

Guided self-study, integration seminar, self-reliant study activities

Learning materials and price

A reader with relevant literature, legislation and policy documents will be made available on the electronic learning platform.

References

- Gillespie, Alisdair (2016), Cybercrime: Key issues and debates, Routledge
- Holt, Thomas and Bossler, Adam (2016), Cybercrime in Progress: Theory and prevention of technology-enabled offenses, Routledge
- Kitchin, R. (2014), The data revolution: Big data, open data, data infrastructures and their consequences, Sage Publications
- Lloyd, Ian (2017), Information Technology Law, Oxford University Press
- Murray, Andrew (2016), Information Technology Law: The Law and Society, Oxford University Press
- Rowland, Diane, Kohl, Uta and Charlesworth, Andrew (2016), Information Technology Law, Routledge
- Siegel, E. (2013), Predictive analysis: The power to predict who will click, buy, lie or die, John Wiley & Sons

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.

Evaluation methods

end-of-term evaluation and continuous assessment

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

Oral examination, assignment

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

Oral examination

Examination methods in case of permanent evaluation

Assignment

Possibilities of retake in case of permanent evaluation

not applicable

Extra information on the examination methods

- Periodic evaluation: oral exam with short-answer questions and open questions, based on the materials and discussions during the lectures. Open questions envisage testing students' 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: paper, oral presentation of the paper (e.g. by means of a short video clip) and a group discussion.
  For the 2nd chance students can submit their paper in August and present it at an agreed time. Students who have already submitted a paper in the 1st examination period have to rework their paper.

Calculation of the examination mark

Periodic evaluation: 50%
Permanent evaluation: 50%

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.