## Aims:

This course aims to complement other information security courses by focusing on cyber crime. Specialist criminal groups, as well as terrorist organisations, have been quick to exploit the opportunities embedded in the ways digital technologies and new media are used by individuals and organisations. In order to explore a wide range of topics and case studies related to this rapidly developing area, the course adopts a wide definition of the term ‘cyber threat’.

This course will:

- Introduce the students to the history and development of cyber crime
- Bring together knowledge from criminology, sociology, media studies and information security to study the cyber threat landscape from different perspectives.
- Offer students an opportunity to engage with a range of common cyber threats, such as identity theft, financial fraud, and terrorist activities.
- Explore the effects of cyber crime through the experiences of victims and law enforcement.
- Examine media representations and public perceptions of cyber-crime and cyber-terrorism.
- Explore emergent trends and developments in cyber crime and cyber terrorism.
- Analyse government counter-measures and counter-narratives.
- Consider the underlying motivations and reasons behind certain cyber crimes and how to handle a digital crime scene.

## Learning Outcomes:

On successful completion of the course students should be able to:

- Identify and evaluate trends in cyber crime and cyber terrorism
- Demonstrate an understanding of the history of cyber crime
- Relate cyber security methodologies to criminal methods
- Critically engage with and evaluate government, legal and mediated initiatives to counter cyber crime
- Apply the criminal and civil law to cyber criminality
- Understand the mechanisms hackers use to social engineer their victims
- Assess public understanding and media framing of cyber crime
- Draw on a wide range of examples and case studies to analyse questions related to the wider cyber threat landscape.

## Course Content:

- Introduction to cyber threats: Types of cyber crime and trends
- Legal Measures & principles of law
- History of cyber crime 1: traditional crimes
- Social engineering & Denial of Service
- Cyber terrorism & cyberwar
- Media frames, narratives, counter-narratives, and public debates
- Case Studies: Investigations into hacking, cases and misuse
- History of cyber crime 2: the dark net
- Content crime: stalking, pornography, harassment & malicious communications
- Digital Evidence
- The Future: The expansion of the Internet, pornography and other unsuitable material

## Teaching & Learning Methods:

11 weekly 3-hour lectures with use cases and additional media materials. Handouts, slides and reading lists will be provided via Moodle. Electronic copies of other resources, such as links to electronic journal articles held by the library and web references, will also be available through Moodle.

## Key Bibliography:


<table>
<thead>
<tr>
<th>Formative Assessment and Feedback:</th>
<th>Two assignments are given during which cyber crime scenarios are discussed from an examination perspective.</th>
</tr>
</thead>
</table>
| Summative Assessment:            | **Exam:** This course is assessed solely (100%) by written examination consisting of a two-hour exam (3 out of 5 questions).  
**Coursework:** Coursework does not contribute to the final assessment of this course (0%)  
**Deadlines:** The written examination will be held in the Summer Term. |

---

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department’s policy of continuous improvement and development. Every effort will be made to notify you of any such changes.