**INFORMATION SECURITY GROUP**  
**Course Specification 2016-17**

<table>
<thead>
<tr>
<th>Code</th>
<th>IY5612</th>
<th>Course Value</th>
<th>20</th>
<th>Status:</th>
<th>Option</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Title:</th>
<th>Cyber Security</th>
<th>Availability:</th>
<th>Spring Term</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Prerequisites:</th>
<th>None</th>
<th>Recommended:</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Co-ordinator:</th>
<th>Stephen Wolthusen</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Course Staff:</th>
<th>Stephen Wolthusen</th>
</tr>
</thead>
</table>

**Aims:**

The objective of this module is to develop an understanding of advanced adversaries and threats to information systems, and particularly the interaction of information with physical systems at scales ranging from embedded and industrial control systems up to critical infrastructures at national and supra-national scales. The module also aims to impart an understanding of assurance mechanisms for both the development and operation of security-sensitive and other high-integrity systems.

**Learning Outcomes:**

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

- Have an understanding of network robustness and failures, together with key underlying theoretical concepts
- Understand critical (information) infrastructures, vulnerabilities, and their dependencies
- Appreciate the specific security problems of cyber-physical including SCADA systems and selected infrastructure
- Understand complex attacks, analytical models for such attacks, and assurance mechanisms

**Course Content:**

Introduction to cyber security and critical infrastructures, national cyber security strategies  
Complex attacks, the cyber kill chain and selected campaigns  
Networks and dependencies: From models of large scale networks to an understanding of network robustness and cascading failures  
Critical infrastructures and interdependencies, models and case studies for interdependencies  
Security of cyber-physical systems: Control systems and attacks on cyber-physical systems  
Control systems security: SCADA and distributed control systems, protocols and their security  
Attack modelling techniques: Static and dynamic risk and adversary models, concurrency and adversary behaviour  
System assurance, certification, and accreditation mechanisms

**Teaching & Learning Methods**

Lectures, exercise sheets (including formative feedback), tutorials

**Key Bibliography:**


**Formative Assessment and Feedback:**

Two of the exercise sheets will be marked and provided to students as formative feedback.

**Summative Assessment:**

Exam 100(%) This course is assessed solely by written examination consisting of a two-hour exam. (3 out of 5 questions)  
Coursework None.  
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.