WM9P1-15 Cyber Security Research Methods

24/25

Department
   WMG
Level
   Taught Postgraduate Level
Module leader
   Elzbieta Titis
Credit value
   15
Module duration
   4 weeks
Assessment
   100% coursework
Study location
   University of Warwick main campus, Coventry

Description

Introductory description

This module focuses on the development, growth, and enhancement of individual analytical and research skills for postgraduate cyber security students, subsequently covering issues of academic and ethical rigour and validity in cyber security research activities.

As such, it is purposefully designed to meet the complex learning and professional needs of postgraduate cyber security students to provide them with the skills and competencies needed to undertake an independent, original piece of research, and successfully complete a dissertation in cyber security. For this purpose, the delivery of the module is well-aligned with the student learning journey, ensuring students readiness for applying for ethical approval and working with their supervisors moving forward.

Specifically, the module comprises a set of carefully designed learning activities, materials, and resources focused on research skills relevant for cyber security, including a deep understanding of the application of methods for data collection, techniques for analysing data, and research ethics for protecting individuals involved and preserving the integrity of the science.

Module aims

1. To provide students with high levels of skills, knowledge, and competency in the area of cyber security research.
2. To provide students with the opportunity to contextualise and apply learning in the field of cyber security research to their wider studies by undertaking an independent piece of cyber security research using appropriate methodological and analytical techniques.
3. To provide students with in-depth knowledge of ethical and legal requirements and professional conduct within the field of cyber security in general and cyber security research more specifically.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The module covers the basic tenets of science with an emphasis on the scientific method and the importance of science to cyber security, and the prerequisites needed to conduct cyber security research.

Standalone, domain-specific topics, such as malware analysis, digital forensics, usable security, and software assurance, will be introduced in the context of research process and methods, in addition to wider security and ethical considerations, the latter including deception and privacy. This will be exercised by providing students with real-world research problems to consider ways forward to build and extend on the existing results using appropriate methods and approaches, while adhering to principles related to legal and ethical considerations in research (i.e., academic integrity), some of which are unique to cyber security (i.e., unauthorised access, capturing some PII when collecting cyber data, deception techniques, breaking a TOS or EULA for research, etc.). This will be followed by discussing practical details, such as test environments and open datasets and software.

The syllabus will include (but is not limited to):

- Epistemological, philosophical and axiological foundations of cyber security research.
- Construction of research strategy.
- Sampling and data collection.
- Validity and reliability.
- Analytical techniques.
- Legal and ethical standards.

Learning outcomes

By the end of the module, students should be able to:

- Develop a research proposal within the field of cyber security, aligning the problem, research objectives, research questions, and research design.
- Critically investigate and analyse sources of information appropriate to a given research problem.
- Identify and evaluate specific issues and challenges for doing research in the cyber security domain and propose suitable mitigations/controls to conduct research safely and effectively.

- Report findings with clarity and an appropriate degree of confidence, referring to both wider scholarship and own proposed investigations.
- Critically understand key aspects of research methods and ethics in cyber security for generating impactful knowledge, validating theories, adding critical rigour, and promoting moral and social values.

Indicative reading list

Cottrell, S., 2017. Dissertations and Project Reports: A step by step guide. Bloomsbury Publishing.
Oliver, P., 2012. Succeeding With Your Literature Review: A Handbook For Students: A Handbook for Students.
Yin, R.K. ,2018. Case Study Research and Applications: Design and Methods (6th ed.). Thousand Oaks, CA: Sage.

[View reading list on Talis Aspire](#)

Interdisciplinary

In addition to looking in-depth at cyber security research methods, the module covers general information about the scientific inquiry as it applies across many disciplines of science.

Subject specific skills

The module provides students with the opportunity to develop skills needed to successfully undertake their studies and independent research in cyber security. In recognising the variety in student backgrounds, students will be supported to develop a foundational to advanced level of skill capability depending on their needs.

Subject specific skills students will acquire on the module include:

- Scoping the literature appropriate to the field.
- Establishing research problems and questions.
- Exploring and selecting viable research methods.
- Planning research and caring out appropriate analyses.
- Evaluating specific security, privacy, and ethical issues and challenges.
- Applying for ethics approval.
- Undertaking multi-disciplinary research.

Transferable skills

Transferable skills students will acquire on the module include, but are not limited to:

- Evaluating wider ethical considerations.
- Researching literature.
- Communication, critical thinking, and problem solving.
- Time management.
- Teamwork.

Study

Study time

Type	Required
Lectures	6 sessions of 1 hour (4%)
Supervised practical classes	24 sessions of 1 hour (16%)
Online learning (independent)	5 sessions of 1 hour (3%)
Private study	55 hours (37%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time
Report on undertaking a research project	80%	48 hours

The report will consist of two parts. Students will review one of the two specific published research papers provided. For their chosen paper, they will critically evaluate the extent to which the learning outcomes for this module would have been satisfied by the research behind the paper (part 1). Students will then devise a new investigation as informed by the findings of the paper they reviewed previously (part 2).

	Weighting	Study time
Multiple choice test	20%	12 hours

The multiple choice test will assess theoretical knowledge about research methods and ethics in cyber security, which will be carried out in scheduled teaching time.

Feedback on assessment

Written feedback for each assignment.
Verbal feedback during tutorial sessions.
Summative feedback on assignments.

Availability

Courses

This module is Core for:

- Year 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)
- Year 1 of TWMS-H1SH Postgraduate Taught Cyber Security Management (Full-time)