MSc in Security and Resilience: Science and Technology

This document provides a definitive record of the main features of the programme and the learning outcomes that a typical student may reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities provided. This programme specification is primarily intended as a reference point for academic and support staff involved in delivering the programme and enabling student development and achievement, for its assessment by internal and external examiners, and in subsequent monitoring and review.

Programme Information						
Programme Title		Security and Resilience: Science and Technology				
Award(s)		MSc	PG Dip	PG Cert		
Programme Code(s)		F3SR (1YFT) F3SR24 (2YPT)	F3SD12 (1YFT) F3SD24 (2YPT)	F3C12 (1YFT) F3C24 (2YPT)		
Awarding Institution		Imperial College London				
Teaching Institution		Imperial College London				
Faculty		Faculty of Natural Sciences				
Department		Department of Physics				
Associateship						
Main Location of Study		South Kensington Campus				
Mode and Period of Study		MSc: 1 calendar year full-time (12 months) MSc: 2 calendar years part-time (24 months) PGDip: 1 calendar year full-time (12 months) PGDip: 2 calendar years part-time (24 months) PGCert: 1 calendar year full-time (12 months) PGCert: 2 calendar years part-time (24 months)				
Cohort Entry Points		Annually in October				
Relevant QAA Benchmark Statement(s) and/or other external reference points						
Total Credits	PG Cert	ECTS:	30	CATS:	60	
	PG Dip		60		120	
	MSc		90		180	
FHEQ Level		Level 7 - Master's				
EHEA Level		2nd cycle				

Specification Details	
Student cohorts covered by specification	2021-22 entry
Person Responsible for the specification	Dr W.G Proud and Prof W. Lee
Date of introduction of programme	October 2019
Date of programme specification/revision	October 2021

Programme Overview

Security and Resilience are of increasing importance on a world basis. The system of geopolitical détente of the Cold War has effectively vanished. While some areas of the world are experiencing growth and/or unprecedented peace e.g. China and Western Europe, there are many areas which are not experiencing such a desirable period. The change in the electronic and information technologies from 1981* to the present day are truly phenomenal. The growth in speed, interconnectivity and access to information is unprecedented. Globalisation and liberalisation of markets and movement of people has further changed the societal landscape.

This MSc, PGDip and PGCert programmes are designed and developed in line with the research and research activities of the Institute of Security Science and Technology (ISST): a cross-faculty institute involving engineers and natural scientists.

Resilience can be defined as the ability of a society and its organisations to accommodate 'stress' through an understanding of risk. Societal stress can arise due to changes in natural environment, political unrest, physical threat, financial crisis and information leakage. In general security is used to mitigate and remove threat to vital societal structures, both physical and psychological. This course will through the use of vignettes cover acts of human intervention, large-scale accidents, systemic effects and discuss this in terms of prevention and mitigation post-event.

Areas such as financial security, transportation, cyber threats as well as more 'traditional' physical environment/threat are addressed. Additionally, the research methodologies both qualitative and quantitative are discussed with significant reference studying human cognition and behaviour. This aspect is often missing from many STEM courses, in the Physical Sciences and Engineering. However, many resilience and security aspects depend strongly on an understanding of human-machine and human-human interactions. The vital role of behavioural science in security endeavours is a core element of this course.

The Key Concepts: Security in Context module brings the technical, engineering and science aspects together. It outlines, through a series of vignettes and interaction with practising security professionals, the relevance and applications of the concepts in the core modules and places the elective components in context. The needs and effects of political decisions and regulatory process is brought out in this module.

This course is significantly different to other security courses on offer at competitor institutions. Many security courses tend to focus on policy aspects, often exclusively qualitative, without referencing a quantitative STEM framework. Conversely, risk analysis tends to towards a numeric solution. This course will deliberately position itself at the interface between these viewpoints and also addresses issues of implementation and physical limitations. Themes of science and technology, human activity and application to society are established first, as the course pushes into areas of policy.

This course is primarily aimed at taking STEM educated graduates and providing them with the fundamental conceptual tools and technologies to address the wide-range of these issues. Graduates from this course could seek employment in any one of the appropriate areas of government, academia and industry. Furthermore, the course will equip students to consider the pursuit of entrepreneurial STEM concepts and develop their own exploitable ideas.

In addition, candidates without a STEM background but with significant relevant experience would be considered for entry to this course. The part-time option is available to students and organisations who need to balance between employment and study.

*The introduction of the Sinclair ZX81 computer, the first widely available programmable home computer, under £100.

Learning Outcomes

The MSc will provide STEM graduates and active professionals with the technical and entrepreneurial training necessary for successful careers in the growing resilience and security industry.

At the conclusion of the MSc the students will be able to:

- Define and analyse security in terms of factors such as; behavioural science, social, environmental, infrastructure, communication and information.
- Use the appropriate statistical and data analysis tools;
- Examine and implement Security system engineering as applied to complex situation and the development of new products/processes. Implement appropriate technology
- Entrepreneurship, innovation and business techniques for taking new products to market including the practical, legal and technical constraints;
- Implement techniques to evaluate and undertake practical research in developing strategies to deal with complex security and resilience issues.
- To evaluate a range of technical and policy solutions to select optimal combinations. Balance quantitative and qualitative considerations for decision making
- Plan and undertake a major independent research project.
- Ensure research designs meet the ethical standards required of human subject studies where necessary.
- Communicate the results of the research, development or strategy, orally and in writing to a wide audience;
- Manage teams and demonstrate leadership in both technical and business domains.

At the conclusion of the PGDip the students will be able to:

- Define and analyse security in terms of factors such as; behavioural science, social, environmental, infrastructure, communication and information.
- Use the appropriate statistical and data analysis tools;
- Examine Security system engineering as applied to complex situations
- Implement techniques to evaluate and undertake practical research in developing strategies to deal with complex security and resilience issues.
- To evaluate a range of technical and policy solutions to select optimal combinations. Balance quantitative and qualitative considerations for decision making
- Plan and undertake a supervised research project.
- Ensure research designs meet the ethical standards required of human subject studies where necessary.

- Communicate the results of the research, development or strategy, orally and in writing to a wide audience;
- Demonstrate leadership in technical domains.

At the conclusion of the PGCert the students will be able to:

- Define and analyse security in terms of factors such as; behavioural science, social, environmental, infrastructure, communication and information.
- Understand the appropriate statistical and data analysis tools;
- Examine Security system engineering as applied to complex situations
- Undertake practical research to deal with complex security and resilience issues.
- Understand a range of technical and policy solutions to select optimal combinations. Balance quantitative and qualitative considerations for decision making
- Ensure research designs meet the ethical standards required of human subject studies where necessary.
- Communicate the results of the research, development or strategy, orally and in writing to a wide audience;
- Demonstrate understanding in technical domains.

The learning outcomes for individual modules are discussed in detail in the module outlines.

The Imperial Graduate Attributes are a set of core competencies which we expect students to achieve through completion of any Imperial College degree programme. The Graduate Attributes are available at: www.imperial.ac.uk/students/academic-support/graduate-attributes

Entry Requirements	
Academic Requirement	The minimum requirement is normally a First Class UK Bachelor's Degree with Honours in a relevant engineering, mathematical or physical sciences discipline (or a comparable qualification recognised by the College)
Non-academic Requirements	N/A
English Language Requirement	Standard requirement IELTS score of 6.5 overall (minimum 6.0 in all elements)

The programme's competency standards documents can be found at: www.imperial.ac.uk/natural-sciences/departments/physics/students/current-students/taught-postgraduates/

Learning & Teaching Strategy	
Scheduled Learning & Teaching Methods	A variety of teaching methods will be used in the course, tailored to the learning outcomes desired and reflecting the different learning styles of the students, with. • Lectures; • Laboratory work; • Computational exercises;

	• Workshops and case studies; • Individual project work.
E-learning & Blended Learning Methods	• Lecture material; • Online discussions; • Links to other relevant learning material.
Project and Placement Learning Methods	The students will complete: • Several short group projects during the course (guided by experienced professionals in the field and supported by academic staff). • A four-month independent project under academic supervision.
Assessment Strategy	
Assessment Methods	A variety of assessment methods will be used in the course, reflecting the variety of skills taught and the different learning styles of the students. Written examinations, oral examinations, problems sheets, practical work and team-work are all used to ensuring a wide range of competencies are assessed and that students get rapid feedback on their learning. Where assessment are shared with other courses the Management Board will ensure that the module assessment reflects the needs of all the courses.
Academic Feedback Policy	
The students will receive feedback from the problem classes, short projects and group exercises. The feedback policy will follow the guidelines of the Department of Physics, where feedback should be provided to the student within ten working days of the work being submitted. Feedback for major pieces of coursework should be provided within four weeks, though marks may not be available until after the Board of Examiners meeting.	
Re-sit Policy	
Students will be permitted to retake written examination on one occasion only. Students will not be permitted to retake practical classes and projects. The College's Policy on Re-sits is available at: http://www.imperial.ac.uk/student-records-and-data/for-current-students/undergraduate-and-taught-postgraduate/exams-assessments-and-regulations/	

Mitigating Circumstances Policy
The College's Policy on Mitigating Circumstances is available at: http://www.imperial.ac.uk/student-records-and-data/for-current-students/undergraduate-and-taught-postgraduate/exams-assessments-and-regulations/

Programme Structure

Full-time	Pre-session	Term One	Term Two	Term Three	Term Four
Core Modules	0	4	4	1	0
Elective Modules	0	1	1	0	0
Projects	0	1	1		0

Assessment Dates & Deadlines

Written Examinations	May/June
Coursework Assessments	Continuous
Project Deadlines	September
Practical Assessments	Continuous

Assessment Structure

Marking Scheme

The marking scheme will follow the appropriate marking scheme in the current 'Regulations for the Examination of Master's level degrees' and for PGCert and for PGDip as appropriate (and these will take precedence over the description given in this specification).

To summarise the current regulations:

Pass
To pass a student must achieve a mark of at least 50% in the aggregate mark for the Core element, AND a mark of at least 50% in the aggregate mark for the Elective element, AND achieve a mark of at least 50% in the 'Research Project' element.

Merit
To be considered for a Merit a student must achieve an aggregate mark of 60% or greater across the programme, AND a mark of at least 60% in two of the three elements, AND a mark of 50% in the remaining element.

Distinction
To be considered for a Distinction a student must achieve an aggregate mark of 70% or greater across the programme, AND a mark of at least 70% in two of the three elements, AND a mark of 60% in the remaining element.

Module Weightings			
Module	% Module Weighting (PG Cert)	% Module Weighting (PG Dip)	% Module Weighting (MSc)
Security in Context	20%	12.5%	8%
Behavioural Research Methods	16%	8.5%	6%
Behavioural Science and Security	16%	8.5%	6%
Network and Web Security	16%	8.5%	5.5%
CBRNE: the Physical Threat Space	16%	8.5%	5.5%
Sensors: Electronic and Natural	16%	8.5%	5.5%
Infrastructure and Transport Security	N/A	8.5%	5.5%
Research Skills Training		1 x Elective module 10%	2 x Elective modules 13%
Mathematical Methods			
Introduction to Shock Physics			
Shock Physics in Context			
SRST Self study project			
SRST PGDip Individual Research Review		27.5%	N/A
SRST MSc Individual Research Project		N/A	45%

Module List												
Code	Title	Core/ Elective	Year	L&T Hours	Ind. Study Hours	Place-ment Hours	Total Hours	% Writt en Exam	% Course-work	% Practical	FHEQ Level	ECTS
PHYS97112	Behavioural Research Methods	Core		35	90	0	125	90	10	0	7	5
PHYS97113	Behavioural Science and Security	Core		35	90	0	125	80	20	0	7	5
CO331	Network and Web Security	Core		28	97	0	125	85	15	0	6	5
PHYS97111	CBRNE: the Physical Threat Space	Core		35	90	0	125	80	20	0	7	5
PHYS97120	Sensors: Electronic and Natural	Core		35	90	0	125	80	20	0	7	5
PHYS97117	Infrastructure and Transport Security	Core		30	95	0	125	80	20	0	7	5
PHYS97119	Security in Context	Core		45	140	0	185	0	100	0	7	7.5
PHYS97116	SRST PGDip Individual Research Review	Core		12	400	0	412	0	80	20	7	16.5
PHYS97089	Research Skills Training	Elective		40	110	0	150	0	20	80	7	6
PHYS97046	Mathematical Methods for Physicists	Elective		30	120	0	150	80	20	0	7	6
PHYS97121	Introduction to Shock Physics	Elective		30	120	0	150	100	0	0	7	6
PHYS97122	Shock Physics in Context	Elective		30	120	0	150	100	0	0	7	6
PHYS97129	SRST Self-Study project	Elective		5	120	0	125	0	80	20	7	5

Module List												
Code	Title	Core/ Elective	Year	L&T Hours	Ind. Study Hours	Place-ment Hours	Total Hours	% Writt en Exam	% Course-work	% Practical	FHEQ Level	ECTS
PHYS97128	Hacking 4 Security	Elective		20	130	0	150	0	40	60	7	6
PHYS97115	SRST MScIndividual Research Project	Core		30	1007.5		1037.5	0	80	20	7	41.5

Please note that additional modules from a range of specialist modules within the College may be taken at the discretion of the Programme Director.

Supporting Information
The Programme Handbook is available at: TBC
The Module Handbook is available at: TBC
The College's entry requirements for postgraduate programmes can be found at: www.imperial.ac.uk/study/pg/apply/requirements
The College's Quality & Enhancement Framework is available at: www.imperial.ac.uk/registry/proceduresandregulations/qualityassurance
The College's Academic and Examination Regulations can be found at: www.imperial.ac.uk/about/governance/academic-governance/regulations
Imperial College is an independent corporation whose legal status derives from a Royal Charter granted under Letters Patent in 1907. In 2007 a Supplemental Charter and Statutes was granted by HM Queen Elizabeth II. This Supplemental Charter, which came into force on the date of the College's Centenary, 8th July 2007, established the College as a University with the name and style of "The Imperial College of Science, Technology and Medicine". www.imperial.ac.uk/admin-services/secretariat/college-governance/charters/
Imperial College London is regulated by the Higher Education Funding Council for England (HEFCE) www.hefce.ac.uk/reg/register/