Frequently Asked Questions

Master of Science in Cybersecurity

1. What is the programme schedule?

Name of Provider			National College of Ireland										
Programme Title (i.e. named award)			MSc in Cyber Security										
Award Title (QQI named award)			MSc in Cyber Security										
Stage Exit Award Title			Postgraduate Diploma in Science in Cyber Security										
Modes of Delivery (FT/PT/ACCS/BLENDED/OC etc.)			PT, Blended, Block, ACCS										
Award Class	Award NQF Level	Award EQF Level	Stage	Stage NQF Level	Stage EQF Level	Stage Credit (ECTS)			Date Effective			ISCED Subject Code	
Major	9		Award	9		90			September 2016			481	
Ref	Module Title		Semester	Module		ECTS	Total Student Effort				Allocation of Marks		
				Status (M/E)	NQF Level	Credit Number	Total Hours	Contact Hours	Directed e-Learning	Independent Learning	CA %	Project %	Exam %	Total %
	Security Fundamentals		1	M	9	10	250	24	24	202	100	0	0	100
	IT Law and Ethics		1	M	9	5	125	12	12	101	100	0	0	100
	Network Security and Penetration Testing		1	M	9	5	125	24	24	77	40	60	0	100
	Secure Programming for Web		2	M	9	10	250	36	24	190	60	40	0	100
	Cryptography		2	M	9	5	125	12	12	101	100	0	0	100
	Malware Analysis		2	M	9	5	125	12	12	101	60	40	0	100
	Research in Computing		3	M	9	5	125	12	12	101	20	80	0	100
	Secure Programming for Application Development		3	M	9	5	125	24	12	89	60	40	0	100
	Incident Response and Analytics		3	GE1	9	5	125	12	12	101	100	0	0	100
	Forensics and eDiscovery		3	GE1	9	5	125	12	12	101	100	0	0	100
	Cloud Security		3	GE2	9	10	250	24	24	202	60	40	0	100
	Research Methods		4	M	9	5	125	12	12	101	60	40	0	100
	Internship		4	M	9	25	600	10		490	0	100	0	100
	Special Regulations: Note 1: A student must pass Research in Computing and not repeat more than 10 ECTS credits to be eligible to register for the Internship Note 2: Learners must complete and pass Internship. Note 3: **Students must choose ONE Group Elective** **Group Elective 1 – Forensics** (Modules: Incident Response and Analytics, Forensics and eDiscovery) **Group Elective 2 – Cloud Security** (Modules: Cloud Security)												

2. Will it state in the diploma that this course is online?

The Diploma will state that the programmes is a Master of Science in Cybersecurity. It will not state it is Online on the diploma.

3. What is the fee?

Those working in a private or commercial semi state organisation can avail of the part funded fee (subject to approval). Fees are due in full prior to the course commencing each year. Fees can be found on the course page.

4. Can you pay in installments?

It is possible to pay in installments up until 5 days before the course is due to commence. All outstanding fees must be paid before the course starts.

5. Is there tax relief if so, can you claim back any tax?

You may apply for tax relief however it is the responsibility of each applicant to contact the tax office regarding this. We can provide a receipt for fees paid if needed.

Frequently Asked Questions

6. How many on-campus days are there per semester?

This is a 100% online programme and there are no on-campus days.

7. How you will it be taught

The school uses a variety of teaching methods, in accordance with the rules, policies and procedures of the College. All students should read these notes which explain what is required in lectures, tutorials, and other teaching sessions.

Students should be aware that there is a clear link between attendance at and engagement in learning sessions, and performance in modules.

Directed Activities:

Directed activities consist of video/reading and tutorial based practical exercises that take place on Moodle, the college's Learning Management System. This content is flexible in nature and each week learners will have the time between their last class and their next upcoming class to work through the materials. These materials will provide the prework for the live classes and it is vital that learners complete these in advance of their next class as these materials will not be covered in the live class, however the activities undertaken in the live class may rely on the prework being completed. Learner progress on the directed activities will be monitored by the course director in order to provide support to learners who may fall behind.

Learners who are more confident may also be allowed move ahead of the content, although this is at the discretion of the lecturer.

Live classes:

You should attend live classes (attendance is monitored) as these provide an opportunity to ask questions related to the Directed Activities undertaken that week, and to work through practical content supported by your lecturer. All lecturers will provide learning materials on Moodle, but these are intended to supplement, not Page 11 of 29 supplant, the live session itself, which will be wider-ranging and provide support for your own study. You should not expect to be able to note down everything that is said in live sessions and copying things down verbatim will distract you from the more important task of listening. The lectures are there to stimulate interest and further study. Student engagement such as questioning, screen sharing, or discussion are encouraged. They are not primarily sessions in which lecturers dictate information.

Online Attendance:

In the case that a class is delivered online, students are expected to attend and engage to the same degree that they would in a face-to-face class. Online classes will take place via Microsoft Teams and students are required to use the Desktop application and log in via their student account details in order to attend classes. Classes will be listed in the Teams Calendar.

During online classes it is important that students follow correct classroom etiquette and the following ground rules will apply:

•Students must mute their mics and turn off webcams when logging in

Frequently Asked Questions

•Students will preferably communicate with the lecturer via microphone, however a message in the chat system is also appropriate
•If a student has a question while the lecturer is speaking, they should indicate this via the chat, or via the hands up feature
•Most classes will be recorded, however the timing and release of these recordings is at the discretion of the lecturer

Continuous Assessments:
Attendance at continuous assessments is of vital importance (attendance is monitored) and all students are expected to prepare for these in advance. It is important that continuous assessments are completed as it will affect how you progress throughout the programme. Continuous Assessment Schedules will be released at the beginning of each semester.

8. Is there a requirement to complete an internship?

The internship runs over 15 weeks, in the last semester of the course. It requires working full-time for the first 12 weeks in an ICT related business environment. The last 3 weeks will be allocated for the preparation of the portfolio to be submitted Part-time students that are working in the IT sector can undertake the Internship within the company they work for by being involved in a Cyber Security related project.

9. Further information about the Internship

Students consolidate the knowledge and skills acquired in other modules by carrying out a project that combines both research and technical skills within a workplace

The learners will investigate, design, produce and evaluate **an ICT solution related to Cybersecurity**.

2 types:

a. Industry Internship: The work for the project will be carried out in an ICT related business environment

b. Academic Internship: The research project proposed in the RIC module will be developed

Students must submit a portfolio (as part of the module assessment) that consists of:

c. a research paper-style report -- “thesis”

d. an artefact/product/software

e. a configuration manual, and

f. a presentation (overview of the report + demo) -- “viva”

g. a monthly internship activity report (for Industry Internship)

Frequently Asked Questions

All students need to do an internship, this can be academic or industry. In some cases the role students hold within their current company may make them eligible to secure their own Industry Internship. This means that during 12 weeks you will work on a cybersecurity-project where you will develop a portfolio to submit for grading (a paper-style report, artefact/demo, internship report and configuration manual). The work developed can be a solution you proposes to a problem in your company, you just need to be aware that the results have to be made available to NCI academic examiners (although non-disclosure agreements can be put in place if required). During the Industry internship, you will be assigned an academic supervisor. In order for this internship to be approved, you would firstly need to submit some documentation such as the job-description.

10. Examples of Theses - http://norma.ncirl.ie/view/divisions/mscincybersecurity/

A

Alaba, Adedoyin (2021) *Detecting Spam Campaigns on Twitter Using Machine Learning Approach.* Masters thesis, Dublin, National College of Ireland.

Alves Fagundes, Jonatas (2021) *An approach for malware detection on IoT systems using machine learning.* Masters thesis, Dublin, National College of Ireland.

B

Babu Rao Pawar, Nagasunder Rao Pawar (2021) *Detection of Phishing URL using Machine Learning.* Masters thesis, Dublin, National College of Ireland.

Bararia, Aarsh Rajesh (2021) *Image Steganography on Cryptographic text using Neural Networks.* Masters thesis, Dublin, National College of Ireland.

Bingi, Santosh Raj (2021) *Improving the classification rate for detecting Malicious URL using Ensemble Learning Methods.* Masters thesis, Dublin, National College of Ireland.

C

Chaudhary, Chirag (2021) *Novel Approach to Detect SQL Injection Attacks.* Masters thesis, Dublin, National College of Ireland.

Cherniy, Dmitry (2021) *Securing Embedded Metadata with Symmetric and Asymmetric Encryption.* Masters thesis, Dublin, National College of Ireland.

Cheung, Cho Fai Bartholomew (2021) *Improving the privacy of Facebook users through browser plugin.* Masters thesis, Dublin, National College of Ireland.

Cogan, Jordan (2021) *Using feature selection to improve intrusion detection.* Masters thesis, Dublin, National College of Ireland.

Collins, David (2021) *Pen Testing Framework for IoT Devices.* Masters thesis, Dublin, National College of Ireland.

Cooney, Keith (2021) *Operational Technology Intrusion Detection Application for Power Grid Security Operations Centres.* Masters thesis, Dublin, National College of Ireland.

F

Fritzen, Marcia Patricia (2021) *Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions.* Masters thesis, Dublin, National College of Ireland.

G

Goh, Kar Chun (2021) *Toward Automated Penetration Testing Intelligently with Reinforcement Learning.* Masters thesis, Dublin, National College of Ireland.

H

Hussain, Nassir (2021) *Gaps and Improvements in Secure Development – In Practice.* Masters thesis, Dublin, National College of Ireland.

I

Ijaiya, Junaid (2021) *Augmenting The Compliance of ISO 27001 Operations Security by Automating the Manual Change Request Process in a Fin-Tech Environment.* Masters thesis, Dublin, National College of Ireland.

Ingale, Anushka (2021) *Identity Verification with Integrated Protected Graphical and Text Password.* Masters thesis, Dublin, National College of Ireland.

Irivbogbe, Idehen Jimmy (2021) *Securing Internet of things (IoT) using SDN - enabled Deep learning Architecture.* Masters thesis, Dublin, National College of Ireland.

J

Jaiswar, Ramesh (2021) *DDoS Attack prediction and classification at Application Layer for Web protocol using Kmeans – SVM Machine Learning Algorithm.* Masters thesis, Dublin, National College of Ireland.

Jaiyeola, Ayobami (2021) *Robust Intrusion Detection Model for Internet of Things.* Masters thesis, Dublin, National College of Ireland.

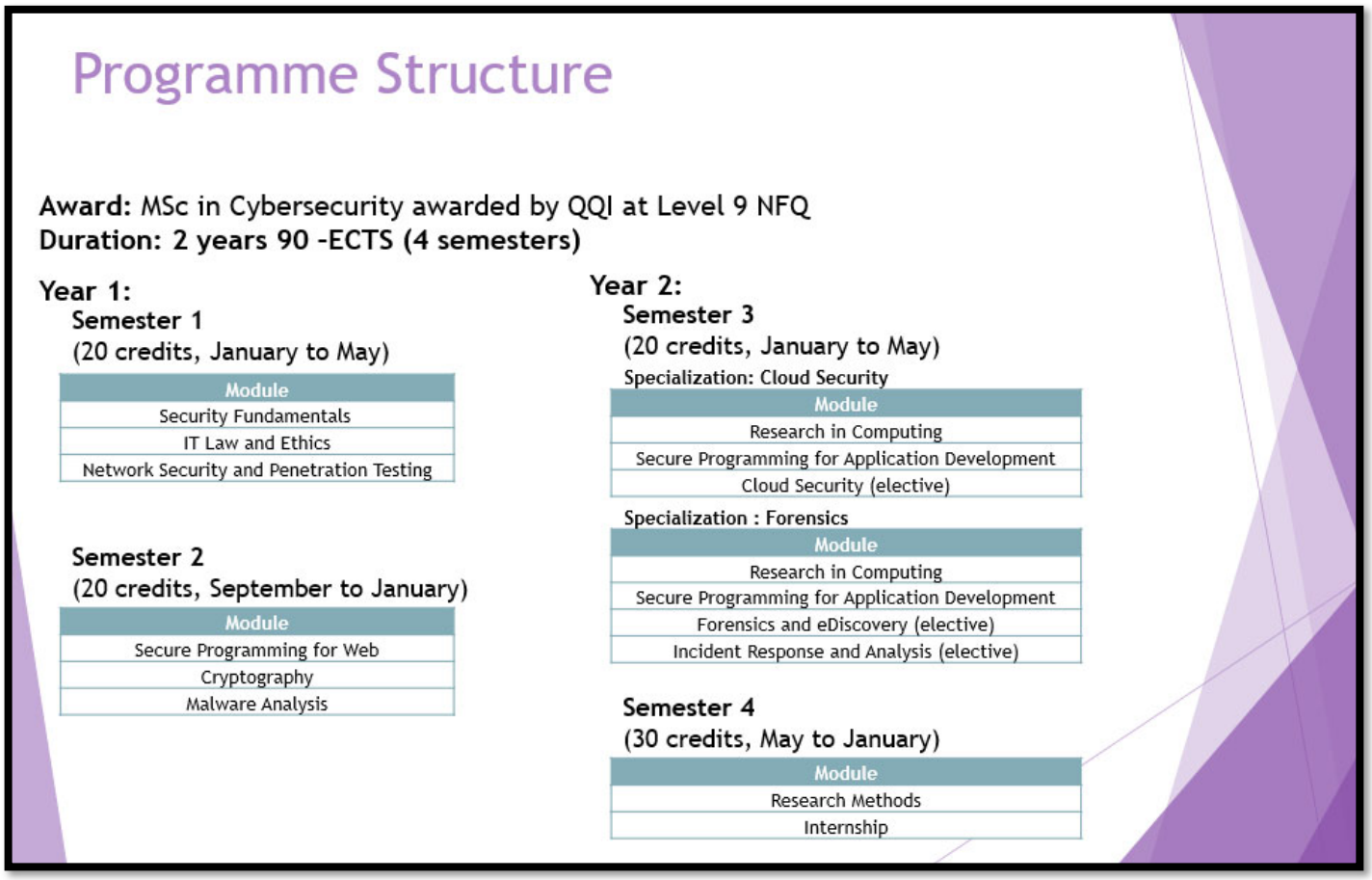
Jetti, Lakshmi Bhargav (2021) *User Authentication Based on the Keystroke Dynamics using Multi-Layer Perceptron.* Masters thesis, Dublin, National College of Ireland.

Frequently Asked Questions

11. How much effort is required?

All modules in NCI are specified in terms of the European Credit Transfer and Accumulation System (ECTS*).

- **The ECTS is based on the estimated student workload** required to achieve the objectives and learning outcomes of a module or programme of study.
- **Student workload** in terms of ECTS consists of the time required to complete all learning activities for that module **including** factors such as the number of **contact hours**, the number and length of written or verbally presented assessment exercises, class preparation and private study time, laboratory classes, examinations, professional training placements, and so forth.
- **These are notional hours of total student effort - in practice, there will be variation in subjects and students in terms of how much time and effort they need to learn something.**
- **Typically, 1 ECTS = 20 - 25 hours of total student effort**.
- In the part-time mode, students would have to complete 20 credits per semester (30 in the last one, split according to the schedule shared with you previously).
- Example Sem 1: 20 ECTS per sem x 25 hrs = 500 hrs per sem / 16 weeks = 31.3 hrs per week (academic week with 5 contact hrs + 5 direct learning + 21.3 hrs independent learning)



Frequently Asked Questions

*ECTS is the recommended academic credit system for higher education in Ireland and across the European Higher Education Area

12. Who is the course aimed at?

Ideal for **ICT professionals or graduates with an honours degree in computer science or in a cognate area (STEM*)** that wish to develop a career as a cybersecurity professional

Candidates who do not hold a computing degree and are **currently working in the IT sector may be considered**, based on relevant academic qualifications or extensive work experience

The part-time element is to help busy professionals to study and work at the same time As a graduate of this course, you will be able to:

- Conduct independent research and analysis in the cybersecurity domain including secure application design, development and testing within a given context, e.g.; web, cloud computing, and forensic investigation.
- Demonstrate practical skills and expert knowledge of technologies and tools that support cryptanalysis, application and service vulnerability detection and patching, security incidents detection and log file analysis.
- Critically evaluate the design and implementation and evaluation of a research idea.
- Analyse and evaluate the legal, ethical and economic ramifications of developing secure applications and services.
- Communicate effectively to a range of audiences in both written and verbal media and undertake self-learning in order to acquire new knowledge.

13. What are the academic Requirements?

Candidates must have:

- A level 8 Honours Degree in **computing or a cognate* area** with a 2.2 award or higher.
- Candidates are expected to have **programming ability**.
- An assessment and/or interview may be conducted to **ascertain suitability if** necessary for **candidates** who **do not meet the normal academic requirements**.
- The college operates a Recognition of Prior Experiential Learning (**RPEL**) scheme meaning applicants who do not meet the normal academic requirements may be considered based on relevant work and other experience. This may be assessed using a portfolio of learning, demonstration of work produced, and an interview. The programming ability of the applicant will also be assessed.
- Non-English speaking applicants must **demonstrate fluency in the English language** as demonstrated by IELTS academic score of at least 6.0 or equivalent

14. Is there a specific requirement to have skills programming/development?

Yes, the Entry requirement for this programme requires previous programme experience. As a general guide we ask that applicants have covered off 4 programming modules in their previous qualifications at level 8 for the MSc in Cybersecurity. Usually, you would have a

Frequently Asked Questions

number of programming languages covered as well and not just limited to one. All applicants are however assessed individually and other experience such as work experience is taken into consideration.

15. What are the credits

Level 9 NFQ 90 ECTS

16. What is RPEL?

RPEL stands for Recognition of Prior Experiential Learning which is a scheme run by NCI that can allow you to gain admission to a programme or to gain exemptions from some parts of a programme based on you providing evidence of relevant learning you achieved through your experiences in a workplace or community setting.

a. Who can apply for RPEL?

Credit for Prior Experiential Learning is intended for mature students who may or may not have had structured formal education but who have learned from their involvement in employment, community activities, home duties, sport etc.

b. What kind of experience is taken into account?

Credit for learning gained in employment: A person, as a result of experience gained in employment, might have achieved learning which can be equated to learning outcomes listed for subjects on an approved course.

Learning gained from voluntary/community activities: Individuals may have been carrying out duties in associations, sporting organisations or charities which might entitle them to exemptions from the learning outcomes on courses in politics, communications etc.`

Learning gained from experience working in the home: Individuals who have had substantial experience of managing a household and rearing children may have gained learning in the area of budgeting, time management, interpersonal skills etc. This might merit exemptions from learning outcomes in business studies.

Learning gained from previous courses/training: If you have undertaken a class that is relevant to the course you are applying for, regardless of the level, it will be taken into consideration for your application.

Frequently Asked Questions

17. Do you have a list of job titles the graduates have secured employment within different cybersecurity roles?

Application and Security Consultant
Apprentice Network Engineer
Associate Cyber Security
Cloud Software Engineer Cyber Security
Cloud Support Associate
Cyber Risk Analyst
Cyber Security Analyst
Cyber Security and Forensics Consultant
Cyber Security Engineer
Cyber Security Risk Analyst
Data Analyst
Discovery Technician
Graduate Cyber Security Consultant
Immersive Engineer
Information Security Analyst
Information Security Engineer
IT Security Operation Analyst
IT Specialist
Network Security Analyst
PHP Developer
QA Automation Engineer
Risk Analyst
Security Analyst Intern
Security Governance
Security Operations Centre Analyst
Security Operations Specialist
Senior Cyber Engineer
Senior Cyber security Analyst
Senior Information Security Analyst
Site Reliability Engineer
SOC Analyst
Software Developer
Software Quality Analyst
Technical Support Engineer
Technology Security Analyst
Virtualisation Engineer
VP Global Sales Marketing

Frequently Asked Questions

18. Can you list the topics covered in the programme?

Content Area	Comments	Covered in Module
Essential		
Network security	Splunk; SMTP; DNS; OSI Model; TCP/IP	Network Security and Penetration Testing
Malware and intrusion detection	Reverse engineering, network traffic	Malware Analysis
Application & User Security	Browsers; Phising; Password Cracking; Ethical Hacking, Pentration testing	Secure Programming for Web, Network Security and Penetration Testing
Cyber crime detection and investigation	Right level	Incident Response and Analytics, Forensics and eDiscovery,
Cyber Security Incident Response		Incident Response and Analytics
Disaster Recovery/Business Continuity		Incident Response and Analytics
Web/App Penetration Testing	Tools & Technologies - practical - CTFs	Network Security and Penetration Testing
Operating Systems	Common schemes	Network Security and Penetration Testing,
Secure Coding/Programming	Include OWASP top 10	Secure Programming for Web, Secure Programming for Application Development
Important		
Risk management	Right level	Incident Response and Analytics
Advanced Threat Detection	Including inside threat detection	Malware Analysis
Digital forensics		Forensics and eDiscovery
Cyber Assurance/Compliance		Security Fundamentals, IT Law and Ethics, Incident Response and Analytics, Forensics and eDiscovery, Cloud Security
Information security management		Security Fundamentals
Security auditing and certification	NIST, PCI, HIPA	Incident Response and Analytics, Forensics and eDiscovery
Identity Theft	Key way into IT system	IT Law and Ethics
Cryptography	Too detailed for intro level - not too heavy on maths	Cryptography
Mobile Security		Security Fundamentals, Forensics and eDiscovery, Cloud Security
Malware/Packet Analysis		Malware Analysis
Advanced algorithms and data structures		Secure Programming for Application Development
Threat Modelling		Security Fundamentals, Secure Programming for Web, Cloud Security Network Security and Penetration Testing

Frequently Asked Questions

Scripting & Data Processing	to include Bash and Python Scripting and regular expressions	Secure Programming for Web, Network Security and Penetration Testing
Cloud and Multi-tenant Cloud Security		Cloud Security, Security Fundamentals, Forensics and eDiscovery
Technical Report Writing	Technical reports eg for customers	Internship, Network Security and Penetration Testing, Forensics and eDiscovery, Cloud Security
Optional		
Security Hygiene	Best practices	IT Law and Ethics
Automated Toolkit Use		Security Fundamentals, Network Security and Penetration Testing, Secure Programming for Web, Cryptography, Malware Analysis, Secure Programming for Application Development, Incident Response and Analytics, Forensics and eDiscovery, Cloud Security
Data Visualisation/Presentation/Graphic Design		Research Methods, Internship
Data Loss Prevention		Security Fundamentals, Cloud Security
Physical Security		Security Fundamentals
Legal/Regulatory Requirements	Privacy	IT Law and Ethics
Software Patterns	Design & software patterns	Secure Programming for Web
Distributed System Security		Incident Response and Analytics
Security Intelligence	Translating data analaysis into information for decision making	Secure Programming for Web, Secure Programming for Application Development
Social Engineering	greatest threat to any organisation	Security Fundamentals, Network Security and Penetration Testing, Cloud Security
Communications	translating technology/reducing jargon/maturating colleagues to take security seriously	Secure Programming for Web, Secure Programming for Application Development
Biometrics		Security Fundamentals
Opensource v Commercial Tools		Forensics and eDiscovery
Risk in the Internet of Things		Security Fundamentals
Human Behaviour/Psychology		IT Law and Ethics

Frequently Asked Questions

19. What is the Disability Support Service?

The college is committed to providing equal access to education and equal opportunities for students with disabilities. NCI encourages students to be open about their disability and to discuss their individual needs with the Disability Officer. It is very important that students disclose a disability early in the academic year to ensure that necessary supports are provided. By delaying disclosure of a disability, students may be missing out on essential supports which can help with everything from participation in lectures right through to sitting exams.