Postgraduate Programme Specification

Session	2025/26	**Last Modified**	02/07/2025
Named Award Title	MSc Cyber Security		
Award Title for Each Award	MSc Cyber Security MSc Advanced Computer Security [without core modules] PG Dip Advanced Computer Security PG Cert Advanced Computer Security		
Date of Approval	30/05/2025		
Details of Cohort Applies to	All students entering or progressing on the programme from January 2023		
Awarding Institution	University of the West of Scotland	**Teaching Institution(s)**	University of the West of Scotland
Language of Instruction & Examination		English	
Award Accredited by		NA	
Maximum Period of Registration		For full time students the normal period of registration is 18 months, and the maximum period is 24 months. For part time students the normal period of registration is 24 months, and the maximum period is 36 months.	
Duration of Study			
Full-time	1.5 years	**Part-time**	3 years
Placement (compulsory)			
Mode of Study	☒ Full-time ☒ Part-time		
Campus	☐ Ayr ☐ Dumfries	☒ Lanarkshire ☒ London ☐ Paisley	☐ Online / Distance Learning ☒ Other (specify) Lanarkshire and London * In the London campus, the

			teaching for this programme will be delivered over T1, T2 and T3 in a given academic year, whereas in the Lanarkshire campus T1 and T2 are used for teaching this programme.
School	**Computing, Engineering and Physical Sciences**		
Divisional Programme Board	**Computing**		
Programme Leader	Dr. Althaff Mohideen		

Admissions Criteria
Candidates must be able to satisfy the general admission requirements of the University of the West of Scotland as specified in Chapter 2 of the University Regulatory Framework together with the following programme requirements:

Appropriate Undergraduate Qualifications:
Applicants will typically possess a degree or equivalent. In the absence of a degree, where entry requirements do not conform to the general entry requirements, other evidence can be considered on an individual basis in line with Regulations 2.13 – 2.36 (Recognition of Prior Learning – RPL / Recognition of Credit).

Candidates must possess an undergraduate degree (preferably with a focus on Computing) that is considered to be at least comparable to a UK second-class honours degree from a recognised institution.

Other Required Qualifications/Experience
Candidates who have other academic, vocational, or professional qualification, and candidates who have at least two years of relevant industrial experience may also be considered for admission. A decision on a candidate's eligibility to register will be made on a case-by-case basis by the Programme Admissions Officer.

Candidates may be required to attend an interview. The Recognition of Prior Learning Guidelines (as laid down in the University's Recognition of Prior Learning Handbook) will be applied. We welcome applications from international students with equivalency of qualifications.

Candidates may seek admission to the MSc Cyber Security via Cyber CPD pathway. Further information and guidance on the Cyber CPD can be obtained from the CPD division.

Further desirable skills pre-application
It is expected that candidates' qualifications/or experience will be in a variety of domains cognate with Cyber Security.

General Overview
This highly specialist programme is designed for graduates who want to gain knowledge and skills in advanced topics in data and network security to combat 21st-century cyber threats. It

focuses on developing theoretical knowledge and practical, hands-on skills to pursue a career in the growing cybersecurity market. Taught in the purpose-built laboratories, the curriculum will cover computer systems and network security, cyber-attacks and defence, intrusion detection and prevention, data security, IoT security, network monitoring, threat intelligence and incident response. The curriculum is built on a strong foundation of knowledge in cyber security and computer networks and industry standards.
The students will undertake an individual project as part of the postgraduate degree which will allow the students to carry out a substantive work-based project on a topic of their interest, falling under CyBok knowledge areas, either in the University or, where possible, in a company.
The programme delivery will draw on strong links with industry in its learning, teaching and professional development, incorporating real-world learning through industry case studies, guest lecturer involvement and supported industry projects

Typical Delivery Method
On Campus via classes, labs etc

Any additional costs
There are no additional costs

Graduate Attributes, Employability & Personal Development Planning
This programme has been specifically designed considering the UWS Graduate Attributes of Universal, Work ready, and Successful. Details to these attributes is available at UWS Graduate Attributes webpage.
Students will be supported in accordance with the Personal Development Planning and Policy Framework of the University. Personal Development Planning is embedded within the programme with links to each module. PDP will be introduced at the beginning of the programme and will be supported with regular workshops for the class. A range of coursework exercises will be identified and used to give students the opportunity to reflect upon their performance and plan for the next cycle of PDP. The demonstration of the ability to carry out PDP will be a requirement for progression from the PgD to the MSc part of the programme.

Employability skills are be built into the programme at a variety of points in many different ways. Industrial and research methods employed in smart network development will be a frequent theme of examples in class and in the laboratory exercises. Generic skills that are transferable to many fields of employment are embedded throughout the programme and are listed in some detail in the module descriptors. All the core modules will ensure that research-informed materials are delivered with research skills demonstrated wherever appropriate. There will also be specialist teaching input from industry wherever possible ensuring up-to-date content for certain topics.

The University Student Link service is available to help all students with advice, resources and assistance in many areas affecting employability. Personal planning, personal finance, time management, career advice, interview preparation and assistance with preparing CVs are some of the areas they can assist with. Services include advice and support on career planning, graduate recruitment, placement, part time work, summer jobs and volunteering. For full time students in particular, the Careers adviser works with staff to deliver a series of workshops aimed at helping graduates seek employment.

Work Based Learning/Placement Details

Opportunities for industry focused learning activities have been built into some of the modules of the programme enabling students to engage with employers. These include 'live' case studies, problem-solving scenarios, and individual work-related projects. Some industry and research-based placement will be offered in the programme.

Attendance and Engagement

In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time.

For the purposes of this programme, academic engagement equates to the following:

Attendanc and Engagement in all scheduled learning activities for this programme.

Equality and Diversity

The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code.

In alignment with the University's commitment to equality and diversity, this programme actively promotes equal opportunities for students from all backgrounds and with diverse learning needs. Learning materials will be delivered via the Virtual Learning Environment (VLE) in electronic formats that support flexible access and allow for content manipulation to suit individual requirements.

Module coordinators are responsible for ensuring that all University-created materials use inclusive and culturally sensitive language. However, it should be noted that some external resources, such as textbooks or websites, may contain outdated or non-inclusive terminology. Students will be informed of this where applicable.

The programme adheres to the University's regulations and guidance on inclusive learning and teaching practices. Students are encouraged to consult the relevant module coordinator to discuss any specific needs. This will enable appropriate arrangements to be made regarding assistive technologies, support services, or assessment adjustments, in line with University policies.

Module coordinators will also ensure that all teaching resources are appropriate to the mode of delivery for each module. For laboratory-based modules, where access to physical devices or hardware may not be possible, suitable alternatives such as emulators and virtual software will be provided to ensure that all students have equitable access to essential tools and resources.

Programme structures and requirements, SCQF level, term, module name and code, credits and awards (Chapter 1, Regulatory Framework)

Learning Outcomes

SCQF LEVEL 11 - Postgraduate Certificate (PgCert) Learning Outcomes	
Knowledge and Understanding	
A1	Demonstrate good knowledge of advanced computer security
A2	Demonstrate a critical awareness of the capabilities of relevant technologies
A3	
A4	
A5	
Practice - Applied Knowledge and Understanding	
B1	Apply a range of principal tools and technologies covered in the modules to identify cyber threats and remediation in advanced computer security.
B2	Effectively use a variety of tools to undertake penetration testing.
B3	Understand the fundamentals of system security in relation with weaknesses and vulnerability.
B4	
B5	
Communication, ICT and Numeracy Skills	
C1	Gather, analyse and Interpret advanced computer security information using ICT methods.
C2	Communicate information effectively with different audiences using a range of appropriate methods and channels.
C3	
C4	
C5	
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Evaluate the impact of cyber threats through laboratory work.
D2	Demonstrate an advanced working knowledge of recent advances in advanced computer security and present findings in report format.
D3	
D4	
D5	
Autonomy, Accountability and Working with Others	
E1	Demonstrate leadership and/or partnership in the planning and delivery individual work and group work.
E2	Demonstrate a high level of understanding of the needs of the business and how to work with colleagues to design and deploy advanced computer security strategies.

E3	
E4	
E5	

Postgraduate Certificate (PgCert) Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
11	COMP11079	Fundamentals of Digital Forensics	10	☒	☐	☐	
11	COMP11081	Governance, Risk Mgt and Compliance	10	☒	☐	☐	
11	COMP11086	Cyber Security: Law and Ethics	10	☒	☐	☐	
11	COMP11094	Network Penetration Testing	10	☒	☐	☐	
11	COMP11089	Malware Analysis	10	☒	☐	☐	
11	COMP11076	Advanced Network Security	10	☐	☒	☐	
11	COMP11097	Penetration Testing Programming	10	☐	☒	☐	
11	COMP11077	Applied Cryptography	10	☐	☒	☐	
11	COMP11082	Incident Response	10	☐	☒	☐	
11	COMP11099	Threat Intelligence	10	☐	☒	☐	
11	COMP11017	Research Design and Methods	10	☒	☒	☐	
11	COMP11080	Foundations of Cyber Security	10	☒	☒	☐	

Footnotes for Core Modules

Justification on Knowledge and Understanding learning outcomes of PgCert and how learning outcomes of the core modules deliver them:

From SCQF Level 11

Demonstrate and/or work with:

• Knowledge that covers and integrates most, if not all, of the main areas of a subject discipline – including their features, boundaries, terminology and conventions.

• A critical understanding of the principal theories, principles and concepts.

• A critical understanding of a range of specialised theories, principles and concepts.

• Extensive, detailed and critical knowledge and understanding in one or more specialisms, much of which are at or informed by developments at the forefront.

• A critical awareness of current issues in a subject/discipline and one or more specialisms.

From the QAA Masters Benchmark in Computing

5.1 The study of computing at master's degree level is typically characterised by:

• An ability to evaluate the technical, societal and management dimensions of computer systems

• A knowledge and understanding of advanced aspects of computer security tools and their use

• A combination of theory and practice, with practice being guided by theoretical considerations

• A strong emphasis on the underlying discipline and/or applications

• The mastery of the practical methodology of the relevant area of computing, whether for general application in software development or in specialised applications relating to the storing, processing and communication of information

• An understanding of, and attention to, the many and varied aspects of quality

• An understanding of professional, legal, social, cultural and ethical issues related to computing and an awareness of societal and environmental impact.

Based on the above, we believe that our following suggestions are a reasonable expectation of outcomes from our modules:

A1. Demonstrate good knowledge of advanced computer security;

A2. Carry out work that evidences a critical understanding of the practical aspects of advanced computer security provision.

A3. Show a critical awareness of the capabilities of relevant cyber technologies.

Postgraduate Certificate (PgCert) Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Option Modules							

Level 11- Postgraduate Certificate (PgCert)
Criteria for Award
Please refer to UWS Regulatory Framework for related regulations

There is no specific progression decision needed after the first trimester, as all students are registered for the MSc. The Postgraduate Certificate is available as an exit award:

Postgraduate Certificate (PgCert) Advanced Computer Security.

The students will be informed and encouraged to progress towards PgDip or Masters

PgCert – 60 Credit points of which a minimum of 40 are at SCQF 11 and none less than SCQF level 10

SCQF LEVEL 11 - Postgraduate Diploma (PgDip) Learning Outcomes	
Knowledge and Understanding	
A1	Demonstrate an advanced knowledge and critical and comprehensive understanding of the principal theories, concepts and principles related to computer science which underpin cyber security and an awareness of the contemporary issues at the forefront of professional practice.
A2	Demonstrate and advanced knowledge and a critical and comprehensive understanding of the essential principles and practices of the domain including current standards, process, principles and the most appropriate software; the reason for their relevance to professional practice.
A3	
A4	
A5	
Practice - Applied Knowledge and Understanding	
B1	Demonstrate the ability to critically analyse, extend and apply knowledge, skills, practices and thinking.
B2	Apply critical analysis evaluation and synthesis to forefront issues, or issues informed by forefront developments in cyber security and the underpinning computer science discipline.
B3	Identify, conceptualise, analyse and define new and abstract problems given practical constraints.
B4	
B5	
Communication, ICT and Numeracy Skills	
C1	Use a range of ICT applications to support and enhance work and adjust features to suit purpose.
C2	Use communication skills in electronic as well as written and oral form to a range of audiences.
C3	
C4	
C5	
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Develop original, creative and innovative responses to professional challenges, problems and issues.
D2	Deal with complex issues and make informed judgements in situation in the absence of data.
D3	
D4	
D5	
Autonomy, Accountability and Working with Others	
E1	Participate within the legal, ethical and professional framework within which they study.

E2	Plan self-learning and improve performance as a foundation for on-going professional development.
E3	Exercise substantial autonomy and initiative in professional and equivalent activities.
E4	
E5	

Postgraduate Diploma (PgDip) Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
11	COMP11079	Fundamentals of Digital Forensics	10	☒	☐	☐	
11	COMP11081	Governance, Risk Mgt and Compliance	10	☒	☐	☐	
11	COMP11086	Cyber Security: Law and Ethics	10	☒	☐	☐	
11	COMP11094	Network Penetration Testing	10	☒	☐	☐	
11	COMP11089	Malware Analysis	10	☒	☐	☐	
11	COMP11076	Advanced Network Security	10	☐	☒	☐	
11	COMP11097	Penetration Testing Programming	10	☐	☒	☐	
11	COMP11077	Applied Cryptography	10	☐	☒	☐	
11	COMP11082	Incident Response	10	☐	☒	☐	
11	COMP11099	Threat Intelligence	10	☐	☒	☐	
11	COMP11017	Research Design and Methods	10	☒	☒	☐	
11	COMP11080	Foundations of Cyber Security	10	☒	☒	☐	

Footnotes for Core Modules

Justification on Knowledge and Understanding learning outcomes of PgCert and how learning outcomes of the core modules deliver them:

From SCQF Level 11

Demonstrate and/or work with:

• Knowledge that covers and integrates most, if not all, of the main areas of a subject discipline – including their features, boundaries, terminology and conventions.

• A critical understanding of the principal theories, principles and concepts.

• A critical understanding of a range of specialised theories, principles and concepts.

• Extensive, detailed and critical knowledge and understanding in one or more specialisms, much of which are at or informed by developments at the forefront.

• A critical awareness of current issues in a subject/discipline and one or more specialisms.

From the QAA Masters Benchmark in Computing

5.1 The study of computing at master's degree level is typically characterised by:

• An ability to evaluate the technical, societal and management dimensions of computer systems

• A knowledge and understanding of advanced aspects of computer security tools and their use

• A combination of theory and practice, with practice being guided by theoretical considerations

• A strong emphasis on the underlying discipline and/or applications

• The mastery of the practical methodology of the relevant area of computing, whether for general application in software development or in specialised applications relating to the storing, processing and communication of information

• An understanding of, and attention to, the many and varied aspects of quality

• An understanding of professional, legal, social, cultural and ethical issues related to computing and an awareness of societal and environmental impact.

Based on the above, we believe that our following suggestions are a reasonable expectation of outcomes from our modules:

A1. Demonstrate good knowledge of advanced computer security;

A2. Carry out work that evidences a critical understanding of the practical aspects of advanced computer security provision.

A3. Show a critical awareness of the capabilities of relevant cyber technologies.

Postgraduate Diploma (PgDip) Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Option Modules							

Level 11- Postgraduate Diploma (PgDip)
Criteria for Award
Please refer to UWS Regulatory Framework for related regulations

There is no specific progression decision needed after the first trimester, as all students are registered for the MSc. The Postgraduate Diploma is available as an exit award:

Postgraduate Diploma (PgDip) Advanced Computer Security. The students will be informed and encouraged to progress towards PgDip or Masters

PgDip – 120 Credit points of which a minimum of 90 are at SCQF 11 and none less than SCQF level 10

SCQF LEVEL 11 – Masters Learning Outcomes (Maximum of 5 per heading)	
Knowledge and Understanding	
A1	Demonstrate an advanced knowledge and critical and comprehensive understanding of the principal theories, concepts and principles related to cyber security which underpin the awareness of the contemporary issues at the forefront of cyber security.
A2	Demonstrate and advanced knowledge and a critical and comprehensive understanding of the essential principles and practices of the domain including current standards, process, principles and the most appropriate software; the reason for their relevance to professional practice.
A3	Demonstrate comprehensive knowledge of advanced computer security concepts and carry out work that evidences an extensive and advanced understanding of the practical aspects of cyber security and demonstrate comprehensive awareness of the capabilities of relevant cyber technologies.
A4	
A5	
Practice - Applied Knowledge and Understanding	
B1	Apply critical analysis evaluation and synthesis to forefront issues, or issues informed by forefront developments in cyber security and critically review and assess contributions to the research literature of cyber security.
B2	Identify, conceptualise, analyse and define new and abstract problems given practical constraints to formulate and execute a defined project of research, development or investigation within the area of cyber security and identify and implement relevant outcomes.
B3	Use a range of the principle skills, practices and/or materials within the selected theme(s) of study in a project.
B4	Use and integrate skills, practices and/or materials which are specialised, advanced, or at the forefront of cyber security.
B5	
Communication, ICT and Numeracy Skills	
C1	Deliver a coherent and reflective presentation of an extended piece of project work to an informed audience.
C2	Produce a critical and evaluative written report of a development project.
C3	Use a wide range of routine and specialised skills in support of established practices within the selected themes(s) of study – for example: - make formal presentations about specialised topics to informed audiences. - Use a range of software to support and enhance work at this level and specify refinements or improvements to software to increase effectiveness - Interpret, use and evaluate a range of numerical and graphical data to set and achieve goals or targets
C4	
C5	
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	

D1	Critically analyse and apply a range of computing concepts, principles, and practices in the context of loosely defined problems where information is limited and/or come from a range of sources, exercising judgement in the selection of tools and techniques.
D2	Critically review and consolidate knowledge, skills and practices and thinking within the selected theme(s) of study.
D3	Demonstrate originality and creativity in dealing with professional level computing issues.
D4	
D5	
Autonomy, Accountability and Working with Others	
E1	Participate within the legal, ethical and professional framework within which they study and deal with complex ethical and professional issues in accordance with current professional and/or ethical codes or practices.
E2	Plan self-learning and improve performance as a foundation for on-going professional development.
E3	Practice in ways which demonstrated a clear awareness of own and others' roles and responsibilities.
E4	
E5	

Masters Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
11	COMP11079	Fundamentals of Digital Forensics	10	☒	☐	☐	
11	COMP11081	Governance, Risk Mgt and Compliance	10	☒	☐	☐	
11	COMP11086	Cyber Security: Law and Ethics	10	☒	☐	☐	
11	COMP11094	Network Penetration Testing	10	☒	☐	☐	
11	COMP11089	Malware Analysis	10	☒	☐	☐	
11	COMP11076	Advanced Network Security	10	☐	☒	☐	
11	COMP11097	Penetration Testing Programming	10	☐	☒	☐	
11	COMP11077	Applied Cryptography	10	☐	☒	☐	
11	COMP11082	Incident Response	10	☐	☒	☐	
11	COMP11099	Threat Intelligence	10	☐	☒	☐	
11	COMP11017	Research Design and Methods	10	☒	☒	☐	
11	COMP11080	Foundations of Cyber Security	10	☒	☒	☐	
11	COMP11024	Masters Project	60	☒	☒	☒	

Footnotes for Core Modules

Justification on Knowledge and Understanding learning outcomes of PgCert and how learning outcomes of the core modules deliver them:

From SCQF Level 11

Demonstrate and/or work with:

• Knowledge that covers and integrates most, if not all, of the main areas of a subject discipline – including their features, boundaries, terminology and conventions.

• A critical understanding of the principal theories, principles and concepts.

• A critical understanding of a range of specialised theories, principles and concepts.

• Extensive, detailed and critical knowledge and understanding in one or more specialisms, much of which are at or informed by developments at the forefront.

• A critical awareness of current issues in a subject/discipline and one or more specialisms.

From the QAA Masters Benchmark in Computing

5.1 The study of computing at master's degree level is typically characterised by:

• An ability to evaluate the technical, societal and management dimensions of computer systems

• A knowledge and understanding of advanced aspects of computer security tools and their use

• A combination of theory and practice, with practice being guided by theoretical considerations

• A strong emphasis on the underlying discipline and/or applications

• The mastery of the practical methodology of the relevant area of computing, whether for general application in software development or in specialised applications relating to the storing, processing and communication of information

• An understanding of, and attention to, the many and varied aspects of quality

• An understanding of professional, legal, social, cultural and ethical issues related to computing and an awareness of societal and environmental impact.

Based on the above, we believe that our following suggestions are a reasonable expectation of outcomes from our modules:

A1. Demonstrate good knowledge of advanced computer security;

A2. Carry out work that evidences a critical understanding of the practical aspects of advanced computer security provision.

A3. Show a critical awareness of the capabilities of relevant cyber technologies.

Masters Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
				☐	☐	☐	
				☐	☐	☐	

				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Option Modules							

Level 11- Masters
Criteria for Award
Please refer to UWS Regulatory Framework for related regulations

The criteria for the Award of Postgraduate Degree are defined in the University Regulatory Framework.

In line with the Regulatory Framework, for the award of MSc in Cyber Security, at least 180 credit points must be achieved by passing all core modules and masters project of which a minimum of 180 are at SCQF Level 11.

MSc in Advanced Computer Security is awarded when at least 180 credit points are achieved without passing all core modules. for the award of MSc in Advanced Computer Security, at least 180 credits points must be earned by passing the masters project and by passing at least 11 core modules, the credits earned of which a minimum of 180 are at SCQF Level 11.

Distinction will be awarded in line with University Regulations and no imported credit can be used. (Regulations 3.35 & 3.26)

Links: UWS Regulatory Framework; and Student Experience Policy Statement.

Masters – 180 Credit points of which a minimum of 150 are at SCQL 11 and none less than SCQF level 10

Distinction is now Regulations 3.25 & 3.26 UWS Regulatory Framework; and Student Experience Policy Statement

Regulations of Assessment

Candidates will be bound by the general assessment regulations of the University as specified in the University Regulatory Framework.

An overview of the assessment details is provided in the Student Handbook and the assessment criteria for each module is provided in the module descriptor which forms part of the module pack issued to students. For further details on assessment please refer to Chapter 3 of the Regulatory Framework.

To qualify for an award of the University, students must complete all the programme requirements and must meet the credit minima detailed in Chapter 1 of the Regulatory Framework.

Combined Studies
There may be instances where a student has been unsuccessful in meeting the award criteria for the named award and for other more generic named awards existing within the School. Provided that they have met the credit requirements in line with the SCQF credit minima (please see Regulation 1.21), they will be eligible for a Combined Studies award (please see Regulation 1.61). For students studying at Level 11, they will normally be eligible for an exit award of PgCert / PgDip / Masters in Combined Studies.

Version no: 1

Change/Version Control

What	**When**	**Who**
Updated Links: • Academic Engagement Procedure • Equality and Diversity • University Regulatory Framework • Removed invalid links	19/10/2023	C Winter
Guidance Note 2023-24 provided	12/12/23	D Taylor
General housekeeping to text across sections and addition of links and some specific guidance. Addition of Duration of Study and some other text – for CMA.	12/12/23	D Taylor