BOURNEMOUTH UNIVERSITY

KEY PROGRAMME INFORMATION

Originating institution(s) Bournemouth University	**Faculty responsible for the programme** Faculty of Media, Science and Technology
Final award(s), title(s) and credit BSc (Hons) Cyber Defence and Intelligence – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 / 120 (60 ECTS) Level 6 credits	
Intermediate award(s), title(s) and credits Dip HE Cyber Security – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 credits Cert HE Computing – 120 (60 ECTS) Level 4 credits	
UCAS Programme Code(s) (where applicable and if known)	**HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load.** 100376
External reference points • The UK Quality Code for Higher Education (2024); • The Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies (2024); • Subject benchmark statements – Computing (2022); • BCS – The Chartered Institute for IT Academic Accreditation Guidelines • United Nations Sustainable Development Goals (SDGs) • National Cyber Security Centre • The Cyber Security Body of Knowledge www.cybok.org.	
Professional, Statutory and Regulatory Body (PSRB) links n/a	
Places of delivery Bournemouth University, Talbot Campus	
Mode(s) of delivery Full-time Full-time sandwich	**Language of delivery** English
Typical duration 3 years full time 4 years full time with 30 weeks placement Sandwich placement	
Date of first intake September 2026	**Expected start dates** September
Maximum student numbers n/a	**Placements** 30 weeks, optional
Partner(s) n/a	**Partnership model** n/a
Date of this Programme Specification June 2026	
Version number v1.0-0926	
Approval, review or modification reference numbers E252608	
Author Professor Nan Jiang, Dr Fudong Li, Dr Wei Koong Chai	

PROGRAMME STRUCTURE

Programme Award and Title: BSc (Hons) Cyber Defence and Intelligence								
Year 1/Level 4 Students are required to complete 6 core units								
Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/ minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Computer Fundamentals	Core	20	50%	50%		36	3.0	100734 100735
Mathematics for Computing	Core	20	50%	50%		36	1.0	100400
Programming	Core	20	50%	50%		36	1.0	100956
Introduction to Cyber Security	Core	20		100%		36	1.0	100376
Network Essentials	Core	20		100%		36	1.0	100365
Computing and Society	Core	20		100%		36	1.0	100631 100367
Progression requirements: Requires 120 credits at Level 4 **Exit qualification:** Cert HE Computing (requires 120 credits at Level 4)								

Year 2/Level 5
Students are required to complete 6 core units

Unit Name	Core/ Option	No. of Credits	Assessment Element Weightings			Expected Contact hours per unit	Unit Version No.	HECoS Code (plus balanced or major/ minor load)
			Exam 1	Cwk 1	Cwk 2			
Ethical Hacking	Core	20	50%	50%		36	1.0	100376
Machine Learning	Core	20		40%	60%	36	2.0	100992
Security Operations (SecOps)	Core	20		100%		36	1.0	100376
Data Structures and Algorithms	Core	20	30%	70%		36	1.0	100956
Network and Cyber Management	Core	20		100%		36	1.0	100365 100376
Technological Innovations in Cyber Security	Core	20	30%	70%		36	1.0	100360 100373

Progression requirements: Requires 120 credits at Level 5

Exit qualification: Dip HE Cyber Security (requires 120 credits at Level 4 and 120 credits at Level 5)

Optional placement year in industry/business:
Students who successfully complete the required 30 weeks placement will be awarded a degree in sandwich mode.

Year 3/Level 6
Students are required to complete 4 core and 1 option.

Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/ minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Cyber Threat Intelligence	Core	20		100%		36	1.0	100376 (major) 100755 (minor)
Systems Engineering	Core	20		100%		36	1.0	100188
Digital Futures	Core	20		100%		36	1.0	100373 100440
Individual Project	Core	40		100%		21	1.0	100358 (major) 100812 (minor)
Cybercrime	Option	20		100%		36	2.0	100376 100387
Human Computer Interaction	Option	20		100%		36	1.0	100736
Deep Learning and Applications	Option	20		100%		36	1.0	100992 100359

Exit qualification: BSc (Hons) Cyber Defence and Intelligence

Sandwich UG award: Requires 120 credits at Level 4, 120 credits at Level 5, 120 credits at Level 6 and successful completion of a placement year.

Full-time UG award: Requires 120 credits at Level 4, 120 credits at Level 5 and 120 credits at Level 6.

AIMS OF THE DOCUMENT

The aims of this document are to:

- define the structure of the programme;
- specify the programme award titles;
- identify programme and level learning outcomes;
- articulate the regulations governing the awards defined within the document.

AIMS OF THE PROGRAMME

BSc (Hons) Cyber Defence and Intelligence is an Office for Students (OfS) funded priority provision specifically designed to address the UK's acute cybersecurity skills shortage. The programme accelerates access to high-tier talent within the key growth-driving sectors (the 'IS-8' sectors) outlined in the UK's Modern Industrial Strategy.

Adopting a progressive, interdisciplinary approach, the curriculum seamlessly integrates advanced Artificial Intelligence (AI) and three intelligence paradigms with core defensive architecture. As a foundational pillar of the University's newly established Defence Cluster, this programme develops highly competent, industry-ready graduates equipped with specialised national security insights and technical expertise. Graduates will be uniquely positioned to harden cyber capabilities and spearhead digital resilience across the defence sector, tactical command networks, and critical national infrastructure, including transportation and communications.

The primary aim of this programme is to produce high-calibre, industry-ready professionals equipped with the multidisciplinary skills required to analyse, defend, and secure the next generation of digital infrastructure and intelligence networks. Sitting at the intersection of operational threat intelligence and advanced technical defence, the programme provides a comprehensive, intelligence-led curriculum.

Specifically, the programme aims to:

- **Deliver a robust foundation** in the core principles of defensive cyber architecture, network security, and cryptography alongside modern computing disciplines including data analytics, machine learning, and secure software development.
- **Foster an intelligence-led mindset** that enables graduates to systematically gather, evaluate, and deploy Cyber Threat Intelligence (CTI) to predict, detect, and mitigate complex cyber adversarial campaigns.
- **Develop advanced technical and investigative skills** through hands-on lab work, threat hunting simulations, and substantial collaborative projects that mirror real-world security operations centre (SOC) and national security challenges.
- **Cultivate professional and ethical responsibility** by embedding a deep understanding of risk management, legal frameworks (such as the Computer Misuse Act and GDPR), data governance, and the ethical implications of offensive and defensive cyber operations.
- **Prepare graduates for diverse careers** across the global security landscape including roles in threat analysis, incident response, digital forensics, and security architecture within the defence sector, government agencies, and commercial enterprises.

ALIGNMENT WITH THE UNIVERSITY'S STRATEGIC PLAN

BSc (Hons) Cyber Defence and Intelligence programme directly advances the BU 2035 Strategic Plan by acting as an industry-connected, OfS-funded priority provision that addresses acute national digital skills shortages. As a foundational pillar of the University's newly established Defence Cluster, the programme embodies the Learning for a Digital World and Place and Partnerships pillars by leveraging BU's £2.3m Cyber Security Competence Centre and regional assets like BattleLab, JP Morgan, Dorset Engineering and Manufacturing Cluster (EMC), South West Regional Defence and Security Cluster (SWRDSC) to deliver hands-on, AI-supported operational training. By seamlessly fusing advanced AI research with tactical defence architectures, the curriculum turns digital innovation into high-impact regional and national security capabilities. Ultimately, this high-demand, portfolio-expanding course secures future student recruitment while cultivating a values-led, ethically grounded technical workforce equipped to safeguard critical national infrastructure.

LEARNING HOURS AND ASSESSMENT

Bournemouth University taught programmes are composed of units of study, which are assigned a credit value indicating the amount of learning undertaken. The minimum credit value of a unit is normally 20 credits, above which credit values normally increase at 20-point intervals. 20 credits is the equivalent of 200 study hours required of the student, including lectures, seminars, assessment and independent study. 20 University credits are equivalent to 10 European Credit Transfer System (ECTS) credits.

The assessment workload for a unit should consider the total time devoted to study, including the assessment workload (i.e. formative and summative assessment) and the taught elements and independent study workload (i.e. lectures, seminars, preparatory work, practical activities, reading, critical reflection, practice).

Assessment per 20 credit unit should normally consist of 3,000 words or equivalent. Dissertations and Level 6 and 7 Final Projects are distinct from other assessment types. The word count for these assignments is 5,000 words per 20 credits, recognising that undertaking an in-depth piece of original research as the capstone to a degree is pedagogically sound.

STAFF DELIVERING THE PROGRAMME

Students will usually be taught by a combination of senior academic staff with others who have relevant expertise including – where appropriate according to the content of the unit – academic staff, qualified professional practitioners, demonstrators/technicians and research students.

INTENDED LEARNING OUTCOMES – AND HOW THE PROGRAMME ENABLES STUDENTS TO ACHIEVE AND DEMONSTRATE THE INTENDED LEARNING OUTCOMES

PROGRAMME AND LEVEL 6 INTENDED PROGRAMME OUTCOMES

<table>
<tr><td>A: Subject knowledge and understanding

This programme/level/stage provides opportunities for students to develop and demonstrate knowledge and understanding of:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:</td></tr>
<tr><td rowspan="2">A1 Principles, techniques and concepts of Cyber Defence and Intelligence

A2 Enabling technologies for Cyber Defence and Intelligence applications

A3 A rigorous engineering approach to investigating and solving Cyber Defence and Intelligence problems in business context

A4 The management and development of IT solutions to address Cyber Defence and Intelligence or other problems

A5 The professional, legal & ethical responsibilities of Cyber Defence and Intelligence personnel within the organisational, technical and global contexts in which Cyber Defence and Intelligence are applied.</td><td>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):

• lectures (A1 – A5);
• seminars (A1 – A5);
• directed reading (A1 – A5);
• use of the VLE (A1 – A5);
• independent research (for dissertation)(A1 – A5).</td></tr>
<tr><td>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):

• examinations (A1-A5);
• coursework essays (A1 – A5);
• dissertation (A1-A5).</td></tr>
<tr><td>B: Intellectual skills

This programme/level/stage provides opportunities for students to:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level outcomes:</td></tr>
<tr><td rowspan="2">B1 Critically thinking, problem-solving and decision-making to solve Cyber Defence and Intelligence problems;

B2 Analyse, interpret, synthesise and critically evaluate information from current research;

B3 Critically evaluate and justify alternative approaches to solutions development;

B4 Formulate, plan, execute, and report on a Cyber Defence and Intelligence project involving original contributions;

B5 Communicate findings to professional and academic standards.</td><td>Learning and teaching strategies and methods:

• lectures (B1 – B5);
• seminars (B1 – B5);
• directed reading (B1 –B5);
• use of the VLE (B1 – B5);
• independent research (for dissertation) (B1 – B5).</td></tr>
<tr><td>Assessment strategies and methods:

• examinations (B1- B5);
• coursework essays (B1 – B5);
• dissertation (B1 – B5).</td></tr>
<tr><td>C: Practical skills

This programme/level/stage provides opportunities for students to:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:</td></tr>
</table>

C1 Retrieve, select and critically evaluate information from a variety of sources; C2 Critically analyse, specify, design and implement Cyber Defence and Intelligence applications to meet business goals; C3 Select appropriate methods and tools for solving Cyber Defence and Intelligence problems; C4 Plan, monitor and evaluate the progress of a Cyber Defence and Intelligence solution.	Learning and teaching strategies and methods: • lectures (C1 – C4); • coursework essays (C1 – C4); • independent research for empirical dissertation (C1 – C4); • group exercises (C1 – C4). Assessment strategies and methods: • examinations (C1-C4); • coursework essays (C1-C4); • dissertation (C1- C4).
D: Transferable skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas. D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media. D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards. D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning. D5 Distill, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.	Learning and teaching strategies and methods: • lectures (D1 – D4); • seminars (D1- D4); • use of the VLE (D1 – D4); • directed reading (D1- D4). Assessment strategies and methods: • coursework essays (D1 – D5); • examinations (D1 – D5); • dissertation (D1- D5).

LEVEL 5/DipHE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level/stage provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
A1 Principles, techniques and concepts of Cyber Defence and Intelligence	Learning and teaching strategies and methods: • lectures (A1, A2, A4, A5); • seminars (A1, A2, A4, A5);

A2 Enabling technologies for Cyber Defence and Intelligence applications A4 The management and development of IT solutions to address Cyber Defence and Intelligence or other problems A5 The professional, legal & ethical responsibilities of data science and AI personnel within the organisational, technical and global contexts in which Cyber Defence and Intelligence are applied.	• directed reading (A1, A2, A4, A5); • use of the VLE (A1, A2, A4, A5). Assessment strategies and methods: • examinations (A1, A2, A4, A5); • coursework essays/presentations (A1, A2, A4, A5); • coursework design and implementation (A1, A2, A4, A5).
B: Intellectual skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
B1 Critically thinking, problem-solving and decision-making to solve Cyber Defence and Intelligence problems; B2 Analyse, interpret, synthesise and critically evaluate information from current research; B3 Critically evaluate and justify alternative approaches to solutions development; B5 Communicate findings to professional and academic standards.	Learning and teaching strategies and methods: • lectures (B1 – B3, B5); • seminars (B1 – B3, B5); • directed reading (B1 – B3, B5) use of the VLE (B1 – B3, B5). Assessment strategies and methods: • examinations (B1 – B3, B5); • coursework essays/presentations (B1 – B3, B5). • coursework design and implementation (B1 – B3, B5).
C: Practical skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources; C2 Analyse, specify, design and implement Cyber Defence and Intelligence applications to meet business goals; C3 Select appropriate methods and tools for solving Cyber Defence and Intelligence problems;	Learning and teaching strategies and methods: • lectures (C1 – C3); • seminars (C1 – C3); • group exercises (C1 – C3). Assessment strategies and methods: • examinations (C1-C3); • coursework design and implementation (C1 – C3).
D: Transferable skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:

D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas. D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media. D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards. D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.	Learning and teaching strategies and methods: • lectures (D1 – D4); • seminars (D1 – D4); • use of the VLE (D1 – D4); • group exercises (D1 – D4). • directed reading (D1 – D4). Assessment strategies and methods: • examinations (D1 – D4); • coursework essays/presentations (D1 – D4). • coursework design and implementation (D1 – D4).

LEVEL 4/Cert HE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level/stage provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
A1 Principles, techniques and concepts of Cyber Defence and Intelligence A4 The management and development of IT solutions to address Cyber Defence and Intelligence or other problems A5 The professional, legal & ethical responsibilities of Cyber Defence and Intelligence within the organisational, technical and global contexts in which Cyber Defence and Intelligence are applied.	Learning and teaching strategies and methods: • lectures (A1, A4, A5); • seminars (A1, A4, A5); • directed reading (A1, A4, A5). Assessment strategies and methods: • examinations (A1, A4, A5); • coursework essays/presentations (A1, A4, A5). • coursework design and implementation (A1, A4, A5).
B: Intellectual skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
B1 Structured problem-solving and decision-making to solve Cyber Defence and Intelligence problems; B2 Gather, interpret, and summarise information from current research B5 Communicate findings to professional and academic standards.	Learning and teaching strategies and methods: • lectures (B1, B2, B5); • seminars (B1, B2, B5); • directed reading (B1, B2, B5). Assessment strategies and methods: • examinations (B1, B2, B5); • coursework essays/presentations (B1, B2, B5).

	• coursework design and implementation (B1, B2, B5).
C: Practical skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
C1 Retrieve, select and interpret information from a variety of sources; C3 Select appropriate methods and tools for solving Cyber Defence and Intelligence problems;	Learning and teaching strategies and methods: • lectures (C1, C3); • seminars (C1, C3); • group exercises (C1, C3).
	Assessment strategies and methods: • examinations (C1, C3); • coursework essays/presentations (C1, C3). • coursework design and implementation (C1, C3).
D: Transferable skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
D2 Gather, select, and interpret a range of experimental and fieldwork data and present professionally using appropriate media. D3 Structure and communicate ideas professionally to appropriate professional and academic standards. D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.	Learning and teaching strategies and methods: • lectures (D2 – D4); • seminars (D2- D4); • use of the VLE (D2 – D4); • directed reading (D2- D4).
	Assessment strategies and methods: • coursework essays/presentations (D2 – D4). • coursework design and implementation (D2 – D4). • examinations (D2 – D4).

Programme Skills Matrix

Units	Programme Intended Learning Outcomes	A 1	A 2	A 3	A 4	A 5	B 1	B 2	B 3	B 4	B 5	C 1	C 2	C 3	C 4	D 1	D 2	D 3	D 4	D 5
L6	Cyber Threat Intelligence	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
L6	Systems Engineering	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
L6	Cybercrime	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
L6	Deep Learning and Applications	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X
L6	Human Computer Interaction	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X
L6	Digital Futures		X		X	X		X	X		X	X				X	X	X	X	X
L6	Individual Project	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
L5	Ethical Hacking	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
L5	Machine Learning	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
L5	Security Operations (SecOps)	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
L5	Data Structures and Algorithms		X		X	X		X			X	X	X	X		X	X	X	X	
L5	Network and Cyber Management	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
L5	Technological Innovations in Cyber Security	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
L4	Computer Fundamentals	X			X	X	X	X			X	X		X			X	X	X	
L4	Mathematics for Computing	X			X	X	X	X			X	X		X			X	X	X	
L4	Programming	X			X	X	X	X			X	X		X			X	X	X	
L4	Computing and Society				X	X	X	X			X	X		X			X	X	X	
L4	Introduction to Cyber Security	X			X	X	X	X			X	X		X			X	X	X	
L4	Network Essentials	X			X	X	X	X			X	X		X			X	X	X	

ADMISSION REGULATIONS

The entry requirements can be viewed on the university website: Courses | Bournemouth University

PROGRESSION ROUTES

Recognition arrangements provide formally approved entry or progression routes through which students are eligible to apply for a place on a programme leading to a BU award. Recognition does not guarantee entry onto the BU receiving programme only eligibility to apply. In some cases, additional entry criteria such as a Merit classification from the feeder programme may also apply. Please see the recognition register for a full list of approved Recognition arrangements and agreed entry criteria.

ASSESSMENT REGULATIONS

The regulations for this programme are the University's Standard Undergraduate Assessment Regulations.

WORK BASED LEARNING (WBL) AND PLACEMENT ELEMENTS

Students, under the guidance of lecturers and the Placement Office, are required to complete a sandwich year with a 30-week minimum placement requirement before level 6.

The placement is assessed on a pass/fail basis using the log book and employer appraisal. The 30-week sandwich placement must be completed between levels 5 and 6 and is a requirement for progression to level 6 for the successful completion of the sandwich mode award.

Placement draws on some or all of the units studied on the first two levels of the programme. It provides the opportunity for the student to develop their abilities and understanding of cyber security related subjects, as well as providing a platform for successful entry into the profession following graduation. It applies and develops understanding and skills acquired in Levels 4 and 5 which makes a major contribution to the understanding of the final level units, and further develops final projects or dissertation research by utilising the context of the work experience as appropriate and enhances students' prospects of future employment.

Refer to 4K – Placements: Policy and Procedure for more detail.