BSC (HONS) SECURITY, INTELLIGENCE AND CYBER

Institute of Business, Industry and Leadership

Academic Level:	6	**Credits:**	360
UCAS Code:	N444		
Awarding Body:	University of Cumbria		
Delivery Site:	Lancaster		
Programme Length:	Standard registration period (full time) - 3 years		
Mode of Delivery:	Blended		
Pattern of Delivery:	Full time		
	Total weeks of study	30 weeks	
	Delivery pattern:	2x 15-week semesters comprised of 12x teaching weeks, 2x assessment weeks and 1x assessment/module prep week	
	Standard semester dates:	Yes	
Programme Webpage:	https://www.cumbria.ac.uk/study/courses/undergraduate/bsc-hons-security-intelligence-and-cyber/		

Entry Criteria
The University's standard criteria for admissions apply. Please refer to the Applicant Information pages of the University website for more information. For RPL, please refer to the University website. Detailed criteria for admission to this programme can be found on the programme webpage: https://www.cumbria.ac.uk/study/courses/undergraduate/bsc-hons-security-intelligence-and-cyber/

PROGRAMME AIMS AND OUTCOMES

Programme Aims

By the end of this programme learners will be able to:

1. Apply a specialised and diverse base of graduate knowledge, understanding and skills developed during the programme in the context of security, intelligence and cyber protection
2. Utilise a range of analytical and research methodologies critically, allowing you to undertake ethically sound, professional, evidence- based empirical research
3. Translate theory into professional practice
4. Employ critical, analytical and research skills to progressively develop your intellectual capacities, career management skills and digital capabilities to undertake professional, ethically informed and evidence-based intelligence analysis
5. Evaluate and communicate evidence effectively. Interpret, assess and present evidence and intelligence clearly within legal, operational and organisational frameworks
6. Develop creative, adaptable problem-solving decision makers who can draw on critical awareness with an understanding of the importance of continuous professional development
7. Generate a lifelong, pro-active approach to innovative practice, developing transferable skills into working practice
8. Promote ethical tactical awareness following professional standards in your decision making.

Programme Outcomes – Knowledge and Understanding

The programme provides opportunities for you to develop and demonstrate the following:

After 120 credits of study (CertHE) you will be able to demonstrate:

K1. An understanding of the interrelationship between security, intelligence and cyber protection environments

K2. A fundamental understanding of principals, ethics and values within decision-making in professional environments

K3 A recognition of risk management skills through the identification of vulnerabilities and the implementation of strategies to assess, manage, and mitigate potential threats

K4 An appreciation of how the digital landscape shapes perceptions and interpretations of risk

K5 An awareness of how intelligence supports decision making in protective security and commercial environments.

After 240 credits of study (DipHE) you will be able to demonstrate:

K6. An understanding of the principles of research design, data collection and application of accepted methods of interpretation and evaluation

K7. An application of risk assessments in a risk management context

K8. An understanding of the role of security in protecting digital environments

K9. A recognition of legal and ethical frameworks governing intelligence and security

K10. An ability to analyse policies which support organisational resilience.

After 360 credits of study (BSc Hons) you will be able to demonstrate:

K11. The complex evaluation of data to support analysis and critical arguments within threat assessment and managerial regimes

K12. A comprehensive appreciation of the security challenges and implications arising from advanced technologies including artificial intelligence

K13. A critical understanding of vulnerability factors affecting security, intelligence and cyber environments

K14. An ability to produce advanced risk management, resilience, and continuity within interconnected frameworks

K15. An ability to critically analyse governance and policy structures and security assurance mechanisms in public and private settings

K16. A systematic and critical understanding of a specialised area of intelligence, security or cyber.

Programme Outcomes – Skills and other Attributes

The programme provides opportunities for you to develop and demonstrate the following:

After 120 credits of study (CertHE) you will be able to demonstrate:

S1. The application of theoretical concepts in differing operational contexts

S2. An ability to select, analyse, interpret and draw inferences from a range of intelligence sources in security and cyber protection environments

S3. An understanding of the consequences of inefficient physical or cyber security

S4. Skills in data collection and analysis from varying sources using ethical and professional means

S5. Application of a range of techniques to initiate, prepare and undertake critical analysis of information and to propose solutions or further enquiry in a professional security, intelligence or cyber context.

After 240 credits of study (DipHE) you will be able to demonstrate:

S6. Analytical skills, including discovering, retrieving and disseminating data, interpreting and drawing inferences from data, and identifying important patterns and representing these

S7. Considered application of information gathering measures in a dynamic environment

S8. The application of transferrable academic skills such as communication skills, time management, reflective practice and teamwork in professional environments

S9. An ability to use industry standard concepts to provide cyber defence and emergency standard response

S10. An ability to produce clear evidence-based outputs to inform strategic decision making

After 360 credits of study (BA/BSc Hons) you will be able to demonstrate:

S11. Application of a range of innovative and creative problem-solving skills to a range of theoretical and practical contexts

S12. An ability to operate with autonomy, responsibility and resilience in uncertain environments

S13. Formulation of researchable issues within security, intelligence and cyber contexts, critically evaluating evidence from a range of sources and drawing appropriate conclusions

S14. The capability to challenge existing knowledge and construct evidence-based arguments

S15. An ability to develop innovative strategic responses to defined problems in security, intelligence or cyber professions

S16. Critical reflection on learning, performance and professional identity.

PROGRAMME FEATURES

Programme Overview
A degree in Security, Intelligence and Cyber prepares students to understand and respond to some of the most significant challenges facing modern society. As digital technology shapes government, business and everyday life, the requirement for professionals who can protect society, infrastructure and systems, acquire and analyse intelligence, and respond to cyber and other threats is growing. This programme provides students with a strong foundation in cybersecurity, operational intelligence practice, security strategy and risk management with a legal, ethical and moral stance. Students will be equipped to use Artificial Intelligence in a professional manner to complement their own skillset. The BSc (Hons) Security, Intelligence and Cyber is designed around strong and continuous engagement with industry, ensuring that students encounter authentic professional practices, current sector challenges, and employer expectations throughout their studies. The programme blends key elements of relevant disciplines providing an interdisciplinary programme with a strong vocational focus on the knowledge, understanding and skills demanded to professionally provide security, intelligence and cyber expertise in contemporary practice. Security is an inherent aspect of societal and professional life: without security, people, organisations, information and national interests would not be protected from harm, loss, damage and the onward ramifications of such events. Security supports organisations in safeguarding property, operations, reputation, continuity and resilience. Security supports social stability, economic growth, and public confidence. Governments rely on strong security systems to protect critical infrastructure, borders, intelligence, and democratic institutions from hostile actors and emerging threats. Security is also essential in the digital world. As society becomes increasingly dependent on technology, cyber security protects networks, data, and systems from hacking, ransomware, and online fraud. A key framework is the Government Functional Standard GovS 007: Security, which sets the minimum requirements for managing security across government. It covers governance, risk management, personnel security, physical security, information security, cyber security, and incident response. Proportionate, risk-based security controls and maintains accountability through clear leadership and assurance processes. These key phrases are represented throughout the programme documents, providing a reassurance for students as to the value and validity of studying this programme The National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC) provide guidance on protective security and cyber resilience. Their standards emphasise threat assessment, secure behaviours, access control, resilience planning, and protection of critical national infrastructure. The UK governments National Cyber Security Centre (NCSC) publishes a Cyber Security Body of Knowledge (CYBOX) a framework for knowledge in the Cyber Security. The current version centres on 21 knowledge areas grouped across themes of human security, systems security, infrastructure,

attacks, and defence. Analysis of these programme modules shows how they align through areas of risk management, digital forensics, human and premises security, and intelligence-based modules confirming that the three pillars of security, intelligence and cyber are mutually supportive of operations in and across disciplines.

UK Intelligence standards require intelligence practice to be lawful, objective, evidence-based, ethical, proportionate and necessary, practiced within the realm of the Intelligence Cycle and respective of relevant legislation in all spheres of practice. This is not only represented in our intelligence-focused modules but across the project, research, security and cyber elements, ensuring practitioners are fully prepared for multi-agency, cross-sector activities.

Studies are complemented by the university's simulation rooms and virtual reality equipment which allow the delivery team to replicate real-world situations and challenges as closely as possible in a learning environment. This combination of digital learning, practical simulations and exploration of emerging technologies provides a hands-on experience in addressing the widest variety of threat to individuals, businesses, the state and society itself. Critical thinking, problem solving, teamwork and a dynamic mindset provided through this approach to learning are sought-after skills in these sectors.

Each module integrates clearly defined industry touch points, such as practitioner-led content, real-world case studies, live or simulated industry briefs, and applied assessments. This approach ensures that theoretical learning is consistently contextualised within contemporary professional environments, enhancing employability, professional confidence, and work-readiness.

The levels of study can be seen as taking students from an introductory practitioner focus discovering the foundational elements of intelligence practice, the evolution of threat and defence, security protections, embracing physical and cyber protective regimes to the end of Level 4 drawing all these threads together with a real-world focus in the Applied Project. Level 5 sees students exploring in more depth to gain a tactical understanding of accessing, interpreting and utilising digital oriented intelligence, implementing security measures, examining the causes of threat and vulnerabilities, and developing an awareness of how societal reactions influence security measures. This culminates in the Operational Skills module before evolving into a final year strategist, drawing your knowledge and understanding together with modules addressing how vulnerability increases risk, exploring the threat and consequences of espionage, sabotage and terrorism in the twenty-first century and analysing national and international responses. The demonstration of your mastery of graduate attributes is evidenced in your final year dissertation research project.

The three pillars of security, intelligence and cyber can be seen as threads throughout the programme providing distinct topic knowledge and understanding whilst combining to allow students to draw on a breadth of understanding to become truly multi-disciplinary in their practice, commensurate with complex interrelated policy, strategy design and problem-solving in a multiparty, multi variable environment. The three threads are influenced by global events and perspective. The nature of security, intelligence and cyber protective matters and the global nature of threats requires practitioners to be equally comfortable operating in local and international regions. Care is taken that the learning materials in this programme will facilitate this.

Current practitioners are as important as future workforce. All modules in this programme are available on a stand-alone basis, allowing prospective learners to undertake Higher Education studies pertinent to their position. The opportunity to undertake degree level education in module-sized portions combined with the potential to have existing learning recognised through recognition of prior learning makes this programme accessible to a diverse range of candidates.

Graduates are well prepared for careers in government agencies, law enforcement, cyber security risk management on national and international basis. This programme offers an engaging, career focused pathway for students with an interest in protecting infrastructure, supporting national security and addressing complex global challenges.

Learning and Teaching

Teaching

As a learner at the University of Cumbria, you are part of an inclusive learning community that recognises diversity. You will have opportunities to learn by interacting with others in a collegiate, facilitative and dynamic learning environment. Teaching, assessment and learner support will allow equal and equitable opportunities for you to optimise your potential and develop autonomy. The University of Cumbria has developed a Learning, Teaching and Assessment Plan with the aim of ensuring that:

> "Learning, teaching and assessment at the University of Cumbria will be active, applied and authentic. Drawing upon a powerful sense of place, a deep intellectual tradition of pedagogic thought within Cumbria, and an unswerving commitment to partnership working, the UoC learning and teaching model provides a distinctive, enabling framework to unlock innovation in programme design and delivery and prepare our graduates for sustainable success in their workplace, their community and the world".

Our learning environment is firmly based on the University's learning and teaching model, comprising:

- Signature pedagogy – Place-based Engaged Learning
- Graduate attributes – Agile and Adaptive, Collaborative and Networked, Critically Curious, Digitally Fluent and Innovative and Creative
- Enhancement themes – Authentic Assessment, Digital Augmentation, Learning Optimisation and Universal Design for Learning
- Our approach to student engagement – Belonging through Partnership

On this programme, each year/level comprises of 5 modules; one 40 credit module which runs for the whole year, plus two 20 credit modules each semester. At each level you can expect to undertake three module sessions during each 12-week semester of study. At each level of learning this is broken down as follows:

- Level 4 you will typically have 12 contact hours per week, split into three sessions of 4 hours duration.
- Levels 5 and 6, sessions are of 3 hours duration, resulting in 9 contact hours per week.

Module sessions at all levels will include lectures, seminars, group work, individual tasks and discussions.

A detailed module learning plan will be issued for each module, providing fine detail on the topic areas to be covered during each session, the teaching approach and methods to be used and preparatory guidance for the following session. Additionally, personal academic tutorial sessions will be arranged; you will have four of these in your first year and two in both your second and final years. In your final year of study, you will also receive a minimum of three research project supervision meetings associated with your dissertation in addition to the outlined teaching arrangements.

Independent Learning

When not attending scheduled learning activities you will be expected to continue learning independently through self-study. Guidance will be provided as you develop your own learning management approach.

Digital Capabilities

Digital capabilities represent an integral part of this programme.

You will be supported with any core functional skills through course material accompanying online guidance via the Student Hub Library and Digital Skills pages.

Specific modules such as SIAC4004 Digital Threats and Cyber Protection and SIAC5004 Digital Intelligence in a Connected World are centred on the digital environment, reflecting the environment security, intelligence and cyber professionals operate in. All modules integrate digital learning environments, immersive VR training rooms to prepare you for recognising and addressing threat. The ethical use of Artificial Intelligence (AI) and Large Language Models (LLM) has become an inherent part of professional practice, reflected in course content and delivery. Digital platforms facilitate the provision of realistic simulations, intelligence analysis scenarios and collaborative case studies on local, national and international basis, mirroring the networked nature of real-world security, intelligence and cyber work.

Strong emphasis is placed on legal, regulatory, proportionate and ethical practice in intelligence gathering, data analysis and threat detection and forecasting.

By combining digital learning and responsible practice graduates are equipped with both technical skills and ethical judgement required in contemporary practice.

You will be supported with any core functional skills with accompanying online guidance via the Student Hub Library and Digital Skills pages.

Teaching Staff

All staff bring significant experience in relevant industries to complement their academic practice. Continuing engagement with industry, research and active in publication, expert comment and advisory positions allows the development and delivery of the programme to be linked to industry practice and career requirements.

Assessment

Formative Exercises are an integral part of all modules, linked closely to the module content and formative assignments. These allow you to develop your assessments styles, assess the levels of knowledge and understanding in an environment which provides constructive feedback opportunities to support your academic performance in demonstrating your grasp of the subject matter and application in practice.

The authenticity of learning and assessment materials is paramount in programme design, complimenting your developing subject matter skills and understanding with an ability to apply this in a 'real-world' setting.

Overview of methods of assessment used on the programme

Year 1 (level 4)

Written assignments

Verbal presentations

Simulation exercises

Teamworking vignettes

Year 2 (level 5)

Reports to mimic professional documents, e.g. proposals for action, analysing events with associated recommendations to avoid repetition. Inquiries into events.

Portfolios comprising various elements of work to evidence your knowledge and understanding

Documents analysing and recommending problem solutions

Exercises to replicate emergency situations allowing you to reflect on performance and experience teamwork in dynamic environments

Year 3 (level 6)

Research proposals and reports

Oral Presentations

Essays

Reports

Feedback

Formative feedback will be associated with the exercises in a timely manner, designed to enable you to incorporate matters identified in your summative assignments.

Written, structured feedback will be provided for all summative assessments. The feedback and feedforward are aligned to the assessment brief, learning outcomes and marking guide for the specific assessment. Whatever the assessment outcome, feedback will be positive, constructive and developmental, to enable you to be able to improve continually on all aspects of your work.

Graduate Prospects

The University's Graduate Attributes outline the qualities we seek to develop in you to shape your impact in the workplace and society and enable you to respond positively to the grand challenges of the decades to come:

- Agile and adaptable – you will be able to respond positively and productively to shifting landscapes in the world of work and the community
- Collaborative and networked – you will develop valuable professional networks and relationships with peers, employers and practitioners
- Critically curious – you will perceive the world as a global citizen through a critical lens, assessing and evaluating information and perspectives to challenge established thinking
- Digitally fluent – you will be able to engage thoughtfully with existing and emerging technologies to harness digital solutions where they add the most value
- Innovative and creative – you will develop creative solutions to recognised challenges, adding value through thinking 'outside of the box'.

This programme recognises and promotes skills that bridge career sectors. The view that security intelligence is a military and law enforcement tactic is challenged. Theories and models of practice originated in these environments, but the business and commercial sectors have an equal appetite for skilled operators thus providing a multiplicity of career opportunities.

The cyber requirements of all careers are well-established. The content of this programme ensures graduates are well placed to embrace the digital aspect of the workplace.

Students will be prepared for roles in:

- Defence sector
- Military sector
- Charity sector
- Intelligence operatives, analysts
- Threat analysts
- Cyber security
- Emergency response
- Police officer
- Security consultant
- Risk and compliance analyst
- Information security
- Security specialist

MODULES

Year 1			
Code	**Title**	**Credits**	**Status**
SIAC4001	Foundations of Intelligence	20	Compulsory
SIAC4002	Weapons of Fear: The Evolution of Terror	20	Compulsory
SIAC4003	Physical Protection of Facilities and Premises	20	Compulsory
SIAC4004	Digital Threats and Cyber Protection	20	Compulsory
SIAC4005	Applied Security, Intelligence, Cyber Project	40	Compulsory
Students exiting at this point with 120 credits would receive a Certificate Higher Education Security, Intelligence and Cyber			

Year 2			
Code	**Title**	**Credits**	**Status**
SIAC5001	Event and Venue Security Management	20	Compulsory
SIAC5002	Disobedience and Democracy	20	Compulsory
SIAC5003	Risk Societies	20	Compulsory
SIAC5004	Digital Intelligence in a Connected World	20	Compulsory
SIAC5005	Operational Skills for Security, Intelligence and Cyber Careers	40	Compulsory
Students exiting at this point with 240 credits would receive a Diploma Higher Education Security, Intelligence and Cyber			

Year 3			
Code	**Title**	**Credits**	**Status**
SIAC6002	Espionage and Sabotage	20	Compulsory
SIAC6003	Vulnerability and Security	20	Compulsory
SIAC6004	Terrorism in the 21st Century	20	Compulsory
SIAC6005	Global Governance and Policy Making	20	Compulsory
Students exiting at this point with 300 credits would receive a BSc Security, Intelligence and Cyber			
SIAC6001	Dissertation	40	Core

Students exiting at this point with 360 credits would receive a BSc (Hons) Security, Intelligence and Cyber

Additional Module Information

Learning materials are scaffolded throughout the programme providing positive progress through the content from foundational practitioner to critical professional. Progression through the levels of the degree is dependent on students demonstrating the requisite knowledge and understanding. Our aim is to support students throughout the process. Should the required knowledge and understanding not be evidenced students will have the opportunity to revisit the assessment. Intensive support being provided. Progression from level 4 to 5 is dependent upon the student completing a minimum of 100 credits. Progression from 5 to 6 is dependent upon the same criteria.

Key to Module Statuses

Compulsory modules	Must be taken although it may be possible to compensate as a marginal fail (within the limits set out in the Academic Regulations and provided that all core or pass/fail elements of module assessment have been passed).

Timetables

Timetables for the academic year are normally available from the July preceding Semester 1. Please note that while we make every effort to ensure timetables are as student friendly as possible, scheduled learning can take place on any day of the week.

Our Timetabling team work hard to ensure that timetables are available as far in advance as possible, however there may be occasional exceptions such as in the case of teaching which falls outside of the usual academic calendar. The UoC academic calendar runs from August to July, so timetabling information for programmes which include teaching sessions in August may not be published until closer to the August delivery.

ADDITIONAL INFORMATION

Student Support

The Student Enquiry Point is a simple way to contact Student Services. Using the Student Enquiry Point tile on the Student Hub you can submit an enquiry to any of the Student Services teams, which includes:

- Careers and Employability
- Chaplaincy for faith and spiritual wellbeing
- Mental Health and Wellbeing
- Digital Skills
- Disability and Specific Learning Difficulty (SpLD)
- International Student Support
- Library
- Money Advice Service
- Safeguarding
- Skills@Cumbria
- Sports and Fitness Facilities
- University Student Accommodation

As a student at the University of Cumbria you automatically become a member of the Students' Union. The Students' Union represents the views and interests of students within the University.

The Students' Union is led by a group of Student Representatives who are elected by students in annual elections. They also support approximately 400 Student Academic Reps within each cohort across the entire University. The Students' Union represent the views of their cohort and work with academic staff to continuously develop and improve the experience for all University of Cumbria students. You can find out more about who represents you at www.ucsu.me.

You can email at any time on studentvoice@cumbria.ac.uk.

Course Costs

Tuition Fees

Course fees can be found here at the course webpage: https://www.cumbria.ac.uk/study/courses/undergraduate/bsc-hons-security-intelligence-and-cyber/

Additional Costs

The following course-related costs are not included in the fees:

Students will require Broadband access and appropriate devices in relation to both blended and independent study. Associated expenditure for broadband and personal device is broad and personal choice-influenced.

Exceptions to the Academic Regulations

This programme operates in accordance with the University's Academic Regulations and Academic Procedures and Processes.

External and Internal Benchmarks

Benchmarks are drawn from a range of sources to provide the best possible alignment for the breadth of interlinked topics forming this programme.

- National Cyber Security Strategy https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030
- Government Functional Standard GovS 007: Security Standards & Principles Government Functional Standard GovS 007: Security - GOV.UK
- National Occupational Standards (NOS) IT (Cyber Security) https://ukstandards.org.uk/en/nos-finder/TECIS600201/identify-cyber-security-threats-and-vulnerabilities
- National Occupational Standards (NOS) Resilience and Emergencies National Occupational Standards (NOS) for Resilience and Emergencies
- National Occupational Standards (NOS) Spectator Safety NOS Finder - National Occupational Standards
- National Occupational Standards (NOS) Legal Advice NOS Finder - National Occupational Standards
- Quality Assurance Agency for Higher Education (QAA) Subject Benchmark Statement Politics and International Relations (2023) Subject Benchmark Statement - Public Policy and Public Administration
- QAA Subject Benchmark Statement Computing (2022) Subject Benchmark Statement: Computing
- QAA Subject Benchmark Statement Criminology (2022) Subject Benchmark Statement - Criminology
- QAA Subject Benchmark Statement Law (2023) Subject Benchmark Statement - Law
- QAA Subject Benchmark Statement Policing (2022) Subject Benchmark Statement - Policing
- QAA Subject Benchmark Statement Social Policy (2019) Subject Benchmark Statement – Social Policy
- QAA Subject Benchmark Statement Public Policy and Public Administration (2025) Subject Benchmark Statement - Public Policy and Public Administration
- UoC Academic Regulations and Academic Procedures and Processes

Disclaimer

This programme has been approved (validated) by the University of Cumbria as suitable for a range of delivery modes, delivery patterns, and delivery sites. This level of potential flexibility does not reflect a commitment on behalf of the University to offer the programme by all modes/patterns and at all locations in every academic cycle. The details of the programme offered for a particular intake year will be as detailed on the programme webpage: https://www.cumbria.ac.uk/study/courses/undergraduate/bsc-hons-security-intelligence-and-cyber/

Date of Programme Specification Production	February 2026
Date Programme Specification was last updated	July 2026