Cyberspace Operations MSc

www.cranfield.ac.uk/cyops

The Cyberspace Operations programme is designed to develop professionals to support military manoeuvre in cyberspace, in contested operations and as part of integrated planning.

Who is it for?

Students will be military and other government personnel, charged with supporting operations in cyberspace in their current or anticipated role. These staff may also be one or more of the following:

- Managers or leaders in a cyber environment who need to understand information risk and respond to cyber threats,

- procurement staff commissioning critical or sensitive projects,

- policy and planning staff interested in computer network and security operations,

- personnel interested in social media and associated concepts such as cyber mobilisation, and

- those charged with accreditation and assessment of security measures.

Your career

This qualification will take you on to become one of the next generation of operators who can support manoeuvres in cyberspace, in contested operations and as part of integrated planning.

Additionally, it provides you with both the theoretical and practical understanding of cyberspace within an organisation, thereby enabling you to become one of the next generation of military leaders.

Cranfield Careers and Employability Service

Cranfield's Career Service is dedicated to helping you meet your career aspirations. You will have access to career coaching and advice, CV development, interview practice, access to hundreds of available jobs via our Symplicity platform and opportunities to meet recruiting employers at our careers fairs. Our strong reputation and links with potential employers provide you with outstanding opportunities to secure interesting jobs and develop successful careers. Support continues after graduation and as a Cranfield alumnus, you have free life-long access to a range of career resources to help you continue your education and enhance your career.

Overview

Start date
September

Duration
MSc: 11 months full-time or up to three years part-time; PgDip: up to two years part-time; PgCert: up to two years part-time

Qualification
MSc, PgDip, PgCert

Study type
Full time MOD students only / Part-time

Structure
The course is delivered via blended learning, with a mixture of residential and online teaching, and project based learning

Campus
Cranfield University at Shrivenham

Entry requirements
Due to the nature of the subject matter in this course, a UK or 5EYES enhanced security clearance will be required.

A first or second class honours degree; or 3rd class degree with three years' relevant experience; or pass degree with five years' relevant experience; or HND/C with seven years' relevant experience.

Exceptional candidates may be accepted with seven years' relevant experience, where this experience is gained in information security, information operations, information risk or a related role.

Owing to security classification and course purpose, only UK Government-sponsored and security-cleared students with a justifiable interest in cyberspace operations will be enrolled on the CSOps named award or its two modules on planning in the full spectrum context and cyber in the C2 battle.

Security clearance for Shrivenham
Some Cranfield University courses are delivered at the Defence Academy of the United Kingdom, Shrivenham which is a Ministry of Defence (MoD) site. All applicants to courses that are wholly or partially delivered at Shrivenham must already hold a security clearance or higher or be willing to undertake security clearance processing.

Please visit our security clearance page for further information.

Fees

Please see **www.cranfield.ac.uk/fees** for detailed information about fee status, full-time and part-time fees as well as deposit requirements and bursary and scholarship information.

Course details

The course is taught through a flexible blend of compulsory residential courses, online Virtual Learning Environment (VLE) activities and interaction and project-based learning.

It has two components:

- A taught component comprising twelve 10-credit modules (PgCert/PgDip/MSc)
- and a dissertation (MSc).

The course is delivered via blended learning, with a mixture of residential and online teaching, and project based learning.

Modules

Keeping our courses up-to-date and current requires constant innovation and change. The modules we offer reflect the needs of business and industry and the research interests of our staff. As a result, they may change or be withdrawn due to research developments, legislation changes or for a variety of other reasons. Changes may also be designed to improve the student learning experience or to respond to feedback from students, external examiners, accreditation bodies and industrial advisory panels.

To give you a taster, we have listed below the compulsory and elective (where applicable) modules which are currently affiliated with this course. All modules are indicative only, and may be subject to change for your year of entry

Compulsory modules

All the modules in the following list need to be taken as part of this course.

Foundations of Cyber

Cyberwarfare in Intelligence and Military Operations

Cyber Law

Cyber Deception

Elective modules

Select seven from the list below

Understanding Risk

Cyber Attack - Threats and Opportunities

Social Technologies

Data-led Decision Support

Emerging Technology Monitoring

Incident Management

The Human Dimension

Critical Networks and Process Control

Systems Thinking for Organisational Viability

Term dates

Orientation Week:	
September 2024 – October 2024	
Term One:	
October 2024 – December 2024	
Term Two:	
January 2025 – March 2025	
Term Three:	
April 2025 – July 2025	
Term Four:	
July 2025 – September 2025	

Class profile 2023/24

Gender:	
Male 87% - Female 13%	
Age range:	
20 - 55 years	
Number of nationalities:	
1	
Nationality:	
UK: 100%	
Class size:	
52	