Cyberspace Operations

MSc/PgDip/PgCert

The Cyberspace Operations course is designed to develop professionals to support manoeuvre in cyberspace, in contested operations and as part of integrated planning. Students will be UK Military and other Government personnel charged with supporting operations in cyberspace, in their current or anticipated role. The course will specifically focus on responses to serious present and emerging threats in the information domain. The course enables the student to understand the context of the cyber domain. Whilst a technical understanding is an advantage, this course enables students from a variety of backgrounds to understand the drivers and constraints within cyber operations and how many roles need to integrate to provide an effective and cohesive operation. The course specifically evaluates the current doctrine and planning procedures across a variety of military and civilian contexts. It also evaluates the impact of cyber on control systems, leadership and decision making in the command and control environment.

Who is it for?

This course suits military and other government personnel charged with supporting operations in cyberspace, in their current or anticipated role.

Course structure

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 three components: a taught component comprising of ten, 10 credit modules (PgCert/PgDip/MSc); a 20 credit module; an 80 credit research project assessed by dissertation (MSc).

Individual project

Students taking the MSc/PgDip complete a 20 credit project, focused on a work-based problem. This allows the student to develop and demonstrate the application of knowledge and skills acquired in the taught modules to a practical problem in the context of a continually changing cyber environment.

Future career

This qualification will take you on to become one of the next generation of individuals 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 leaders.

Example modules

Modules form only part of the course, with the project(s) and theses making up the balance. Please see the course structure for details.

The list below shows the modules offered in the 2019-20 academic year, to give you an idea of course content. To keep our courses relevant and up-to-date, modules are subject to change – please see the webpage for the latest information.

Compulsory:

- Cyber Attack – Threats and Opportunities,
- Cyber Systems Thinking and Practice,
- Cyberwarfare in Intelligence and Military Operations,
- Foundations: Management of Cyber,
- Incident Management,
- Social Technologies,
- Understanding Risk. .

Elective (select 30 credits):

- Applied Cyber Concepts Project (20 credits),
- Critical Networks and Process Control (10 credits),
- The Human Dimension (10 credits).

Choose a further 10 credits from the following modules:

- Data-led Decision Support (10 credits),
- Emerging Technology Monitoring (10 credits).

Duration:
PgCert: up to three years part-time,
PgDip: up to four years part-time,
MSc: up to five years part-time.

(For MOD status students the duration may vary, subject to annual review.)

Start date:
September.

Location:
Shrivenham.

Entry requirements:
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 ten year's relevant experience in a related role.

Contact details

T: +44 (0)1793 785220
E: cdsadmissionsoffice@cranfield.ac.uk

For further information please visit
www.cranfield.ac.uk/co