How to participate in the CDT in Cyber Security

As a student

Background: Ideal students have cyber security interests which span disciplines already. Although it would be desirable for this to have been reflected in undergraduate study, we know this isn't usually possible. So a Computer Science student who has undertaken independent study in legal aspects would be an excellent fit, or a Social Science student who has 'A'-level maths and has written smartphone apps, say, would also be ideal.

Funding and Fees: The CDT has about 16 places available in each cohort. Funding is available for 12. Funding will be subject to normal EPSRC rules. UK and EU students are eligible for full-fee studentships. In addition, UK students are eligible for an annual stipend (for four years) of just over £16,000 each year. Overseas students are welcome, and will need to pay the full Oxford University fees and college fees if accepted. Outstanding overseas students may win a University scholarship.

Requirements: Places (and funding) will be awarded on a competitive basis, according to academic merit. This means you should have an excellent academic record so far. The minimum requirement will be a 2.i (or overseas equivalent) in a relevant undergraduate degree, or a Distinction at Master's level. Those with a first class degree, a strong Master's qualification, a very clear motivation for studying cyber security, or strong relevant work experience will generally be nearer the top of the priority list. The full admissions policy is available on our web site.

Before you apply, you are welcome to contact the CDT office for advice - and a visit, if circumstances allow. A quick revew of your CV should be able to determine if your application will be competitive.

How to apply

Applications will be via the University's normal web-based process. You can find the link from our website.

As part of the application process, you will need to supply a CV, academic transcripts, and three academic references. In addition you will need to provide a personal statement. This should be 1000-1500 words, and explain why you want to study cyber security, and how an inter-disciplinary approach will be a benefit in this context. *You do not need to make a detailed research proposal, but your statement should show some understanding of possible research topics in one or more of the themes described above. A prose re-statement of your CV is not what we are looking for.*

Deadlines *are published on the web site.*

The CDT and many of the funded studentships are supported by:

EPSRC
Engineering and Physical Sciences
Research Council

As a company, as a sponsor or supporter

- **by sponsoring a mini-project:** this could be anything from suggesting an idea, or providing data or knowhow, all the way through to having a student work on-site with you for nine weeks. If the mini-project goes well for both sides, you might agree to support the student through the next three years of their research.
- **by hosting a field trip or a 'deep dive' or masterclass:** the CDT is keen to give the students a broad experience of 'real life' cyber security, enabling them to see how the ideas and challenges they study in an academic environment are translated (or not) into practice.
- **by substantive sponsorship**: the CDT can accept more students than it has funding for. Sponsoring, or co-sponsoring a student throughout their four years of study demonstates a commitment to advanced research in cyber security. Likewise, donations in kind - of software, data, and other resources - can be invaluable for keeping research focussed on practical and achievable goals.

Sponsors are invited to participate in the CDT's Advisory Board, and to interact with the students as much as posssible through open days when students showcase their work, and an annual dinner.

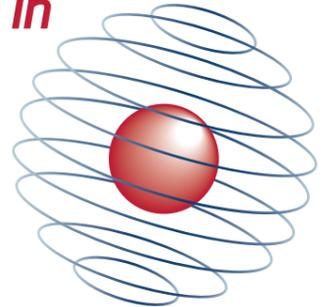## Contact Us

www.cybersecurity.ox.ac.uk/cdt

Director: **Prof. Andrew Martin**
Andrew.Martin@cs.ox.ac.uk

Administrator: **David Hobbs**
cdt@cybersecurity.ox.ac.uk

Phone: +44 1865 610644

UNIVERSITY OF OXFORD

CENTRE *for* DOCTORAL TRAINING *in* CYBER SECURITY

Overview

Centre for Doctoral Training in Cyber Security: a new programme at the University of Oxford, leading to the degree of DPhil (Oxford's PhD)

As the technologies of cyberspace come to inhabit all parts of everyday life, Cyber Security has become everyone's problem. We face a growing collection of adversaries who are agile, opportunistic, and increasingly strategic, developing an ecosystem of suppliers involved in delivering elements of attack capability. They seek to defraud consumers, exploit their trust, or invade their privacy; to misappropriate corporate secrets and intellectual property; to disrupt the operation of the state or critical infrastructure. Our CDT sets out to educate a new generation of research leaders as well as the highest tier of security professionals, who appreciate the real-world challenges which arise from security needs in existing and emerging contexts, equipped with both the expertise and adaptability to address those needs. They will need to become as agile in their thinking as the attackers are – and as resourceful in defence as their counterparts are in attack.

The CDT:
- has a multi-disciplinary approach, embracing both technical and social topics
- uses cohort-based learning, so students from different backgrounds learn from each other
- embraces both theory and practice

Deep Dive Days

"Deep Dives" are a supplement to the academic programme of classes, lectures, and seminars. They are an opportunity to interact with someone who practices cyber security daily: technologists, CISOs, security consultants, lawyers, Government risk owners, and more. Some of these are visits and field trips; others take the form of a 'masterclass' in Oxford. Deep dives allow the academic material to be illustrated - and challenged - by exposure to everyday practice. Sometimes, they can become the basis of on-going project work, too.

CDT Programme

The CDT admits a cohort of around 16 students each October.

As a student in the CDT you will spend the first year in a group with the other CDT students in your cohort on an intensive programme of study designed to introduce the dimensions and nature of the challenge of Cyber Security from a range of academic perspectives.

These will include as a core, Cyber Security Principles (Systems and Operations), Usability, Security Risk Management, System Architectures, High-integrity Systems Engineering. There will also be a range of courses in research methods and tools. This understanding will be placed in the context of courses in business processes, policy and governance, international relations, and criminology. You will have access to leading thinkers and practitioners in cyber security.

Following this intensive education, you will spend the summer of the first year undertaking two 'mini projects' in diverse areas, usually involving placement in a company or government organisation. You will normally choose these from a list proposed by supervisors and sponsors. One or both of these mini-projects will typpically form the basis for your long-term research project.

For this substantive project, you will be based in one of the departments contributing to the CDT, and undertake supervised research in the usual manner for a DPhil. The normal duration of this project will be three years, after which you will submit a thesis and be examined in the usual way.

During the three years of the individual research project, you will retain contact with the CDT, returning for skills training, an annual conference, and other events.

Another Cyber Security CDT has been set up at Royal Holloway University of London. The two CDTs share a range of events throughout the year.

Themes

Cyber Security is a big topic: most of the student research projects in the CDT fall into these four themes, but there is room for flexibility too.

Cyber-Physical Security

considers the integration and interaction of digital and physical environments, and their emergent security properties; particularly relating to sensors, mobile devices, the internet of things, and smart power grids. In this way, we augment conventional security with physical information such as location and time, enabling novel security models. Applications arise in critical infrastructure monitoring, transportation, and assisted living.

Real-Time Security

arises in both user-facing and network-facing tools. This theme addresses the technologies which make possible continuous authentication based on user behaviour, evolving access control making decisions based on past behaviour instead of a static policy, visual analytics and machine learning applied network security management, anomaly detection, and dynamic reconfiguration. These pieces contribute in various ways to an integrated goal of situational awareness.

Assurance

Effective Systems Verification and Assurance has been at the heart of Oxford's longstanding strength in formal methods for modelling and abstraction applied to hardware and software verification, proof of security, and protocol verification. In the CDT we place it in a wider process context extending to procurement and supply chain management, as well as criminology and malware analysis, high-assurance systems, and systems architectures.

'Big Data' Security

covers the acquisition, management, and exploitation of data in a wide variety of contexts. Security and privacy concerns often arise here – and may conflict with each other – together with issues for public policy and economic concerns. The scale of the data means that new risk arise, such as those from unexpected de-anonymisation. A major application area for this research is in medical research: the formerly expected boundaries between public data, research, and clinical contexts are breaking down. Complexity comes from the handling of genomic data, autonomous data collection, and the co-management of personal health data.

Year One:
intensive, multi-disciplinary education in cyber security

two *mini-projects*

Years Two – Four:
research with a supervisor in Computer Science, Oxford Internet Institute, Blavatnik School of Government, Oxford e-Research Centre, Saïd Business School, or another Oxford Department

leading to a thesis and the degree of DPhil (Oxford's PhD)