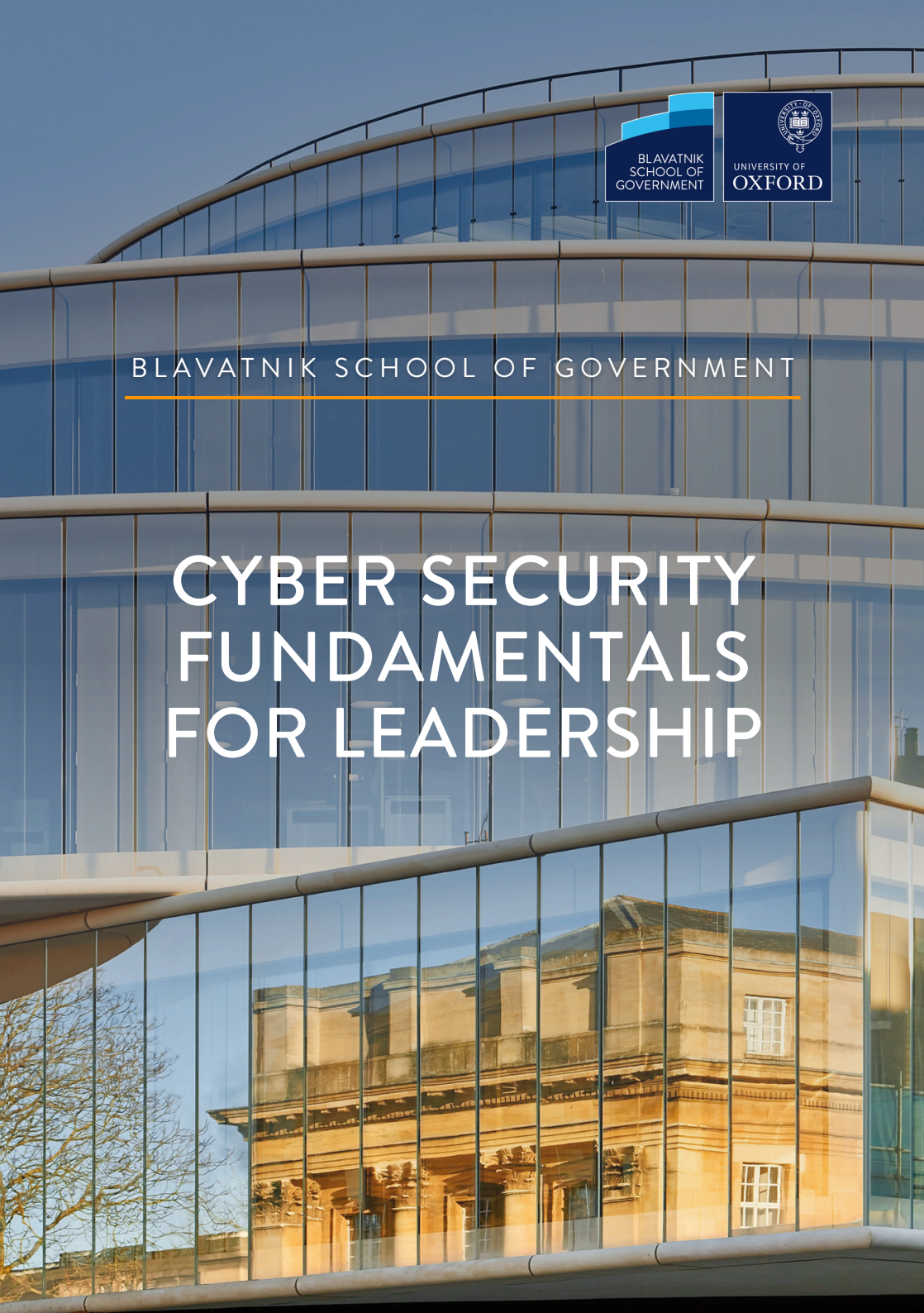

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD
BLAVATNIK SCHOOL OF GOVERNMENT
CYBER SECURITY FUNDAMENTALS FOR LEADERSHIP

WELCOME FROM PROFESSOR CIARAN MARTIN

In today's digital age, cyber security is no longer the sole domain of technical experts; it's a leadership imperative. Having spent much of my career at the intersection of national security, technology and public policy, I've seen how cyber threats can undermine trust and disrupt operations. That's why I'm proud to lead this course at the Blavatnik School of Government.

Cyber Security Fundamentals for Leadership is designed specifically for decision-makers who shape strategy, allocate resources and bear responsibility for resilience. You don't need a technical background to benefit from this course, but you do need a commitment to understanding the risks your organisation faces, and the tools available to manage them.

If your ambition is to develop a sustainable cyber security strategy that helps to build a culture of safety and resilience within your organisation, I hope you'll join us on the course.

Warm regards,

Professor Ciaran Martin
Course Director

Before joining the Blavatnik School of Government, Professor Ciaran Martin was the founding Chief Executive of the National Cyber Security Centre, part of GCHQ, leading a fundamental shift in the UK's approach to cyber security in the second half of the last decade. He successfully advocated for a wholesale change of approach towards a more interventionist posture. This was adopted by the Government in the 2015 National Security Strategy, leading to the creation of the NCSC in 2016 under his leadership. Over the same timeframe, the UK has moved from joint eighth to first in the International Telecommunications Union's Global Cybersecurity Index and the NCSC model has been studied widely and adopted in countries like Canada and Australia. Ciaran's work, which led to him being appointed CB in the 2020 New Year's Honours list, has also been recognised and honoured in the United States and elsewhere across the world.

CYBER SECURITY FUNDAMENTALS FOR LEADERSHIP

Start date:
5 October

Duration:
8 weeks

Location:
Online

Cost: £855

DRIVE CONFIDENT DECISION-MAKING IN A COMPLEX CYBER LANDSCAPE.

In our data-rich world, cyber security is a key part of modern leadership, and understanding how to address vulnerabilities and create policies to maintain stability is key to organisational success.

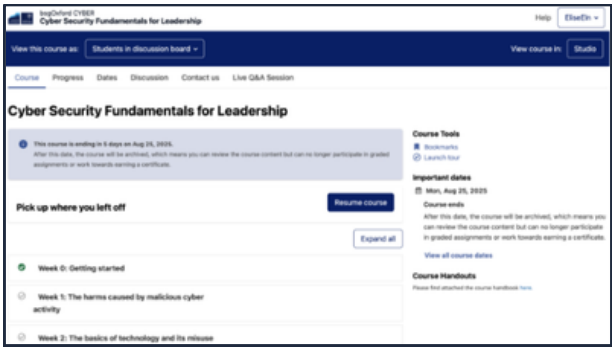
Cyber Security Fundamentals for Leadership is an eight-week online course that equips non-technical professionals with a basic understanding of cyber security, empowering them to effectively manage risks and proactively defend their organisations. Participants will engage with a weekly release of pre-recorded lessons, and two live Masterclasses, benefiting from online learning at their convenience and direct access to Oxford expertise.

WHAT YOU WILL GAIN	IS THIS YOU?
• **Threat awareness and strategic insight:** Develop a robust understanding of the cyber security threats relevant to you, your organisation and your national context. • **Informed technology decisions:** Make smarter, security-conscious choices when procuring and implementing new technologies. • **Incident response readiness:** Build the capacity to respond quickly and effectively to cyber security incidents, minimising disruption and reputational damage. • **Long-term strategy development:** Design a sustainable strategy that aligns with organisational goals and evolves with emerging threats.	• Public sector officials interested in gaining the essential knowledge in safeguarding critical infrastructure and sensitive information • Managers in public or private organisations handling significant amounts of data or operational cyber security risk • Decision-makers or policy-makers interested in developing a holistic approach to cyber security. • Leaders in any organisation that may store personal or sensitive data who need an understanding on the importance of cyber security

WHAT TO EXPECT

Accessing the course

The course runs on the OpenEdX platform, an excellent User Interface, which provides learners with a neat aesthetic and the use of various features such as discussion forums, MCQs, interactive exercises and essay submissions.



You will have the opportunity to connect with your peers through the live sessions and virtual learning environment, which allows you to discuss your career aspirations and make connections that could help you in your progression.

Weekly progress and tasks

The course is partly asynchronous. You are free to progress through the written and video content in your own time within a week, submitting your end-of-week assessment by Sunday evening. See our Workplan for more details.

Masterclasses

Two exclusive masterclasses delivered by Ciaran Martin are also organised at fixed times, and you must connect live for each of these sessions. The masterclasses last for 1.5 hours, during which you explore topical case studies and have the chance to ask Ciaran any questions you might have.

Assessment details

Summative assessments will be spread evenly, with typically no more than one assessment task per week. We aim to avoid significant or challenging pieces of assessment in week 1 to allow sufficient time for you to adapt to the learning environment.

Assignment tasks and weightings

In order to pass the course and qualify for a certificate of completion, you must receive an overall grade of 75% or higher. Your grade will be calculated as follows:

- 10% for completing two summative multiple-choice quizzes in Weeks 2 and 7
- 15% for completing three Facilitator graded discussion forums in Weeks1, 3 and 6;
- 25% for submitting a recorded presentation, and a writtenscenario response in Weeks 4 and 5
- 50% for successfully completing the final project/assignment.

Grading will be based on the rubric in the final assignment section.

Final project

Upon completion of the course, you will produce a cyber strategy allowing you to demonstrate achievement, of course, learning objectives and application of knowledge.

Module information

MODULE 1 CYBER INSECURITY: THE HARMS CAUSEDBY MALICIOUS CYBER ACTIVITY	Teaching you how and why malicious cyber activity causes harm, and the types of harm public sector organisations are likely to encounter.
MODULE 2 THE BASICS OF TECHNOLOGY AND ITS MISUSE	Describes the basics of how technology works. You will be instructed on how technology becomes misused and how security breaches are achieved.
MODULE 3 WHO IS HACKING AND WHY?	Provides perspective on the ways in which hackers think and work.
MODULE 4 BUILDING THE CYBER DEFENCES OF AN ORGANISATION	You will examine how to build an effective cyber operational strategy for a public authority.
MODULE 5 A REAL-LIFE CYBER SECURITY INCIDENT RESPONSE EXERCISE	Involves a simulation and will see you respond effectively to cyber security incident.
MODULE 6 PUBLIC POLICY AND CYBER SECURITY	Develops awareness of the political and geopolitical environment in which cyber security and technology policy operates.
MODULE 7: CYBER SECURITY IN TIMES OF TENSION AND CRISIS	Builds understanding of the wider political and geopolitical factors that affect cyber security risks and threats, and your ability to manage them. You will explore cyber realism in the time of war context derived around an article written by faculty.
MODULE 8: PREPARATION AND FINAL ASSIGNMENT	In the final module, you will prepare a critical incident review. You can expect to identify the risks and harms of cyber security, capture the lessons learned throughout the other modules and make recommendations for the future national policy framework.

Workplan with timeline

WEEK BEGINNING	WEEK 1 5 OCTOBER	WEEK 2 12 OCTOBER	WEEK 3 19 OCTOBER	WEEK 4 26 OCTOBER	WEEK 5 2 NOVEMBER	WEEK 6 9 NOVEMBER	WEEK 7 16 NOVEMBER	WEEK 8 23 NOVEMBER
	COURSE STARTS			Masterclass 1: Friday 30 October			Masterclass 2: Wednesday 18 November	**COURSE DEADLINE** Sunday 29 November
MODULE 1								
MODULE 2								
MODULE 3								
MODULE 4 + MASTERCLASS								
MODULE 5								
MODULE 6								
MODULE 7 + MASTERCLASS								
MODULE 8								

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

TAKE THE NEXT STEP

INTERESTED IN FINDING OUT MORE?

Please get in touch with our recruitment team for more personalised advice.

Email: cybersecurity.online@bsg.ox.ac.uk