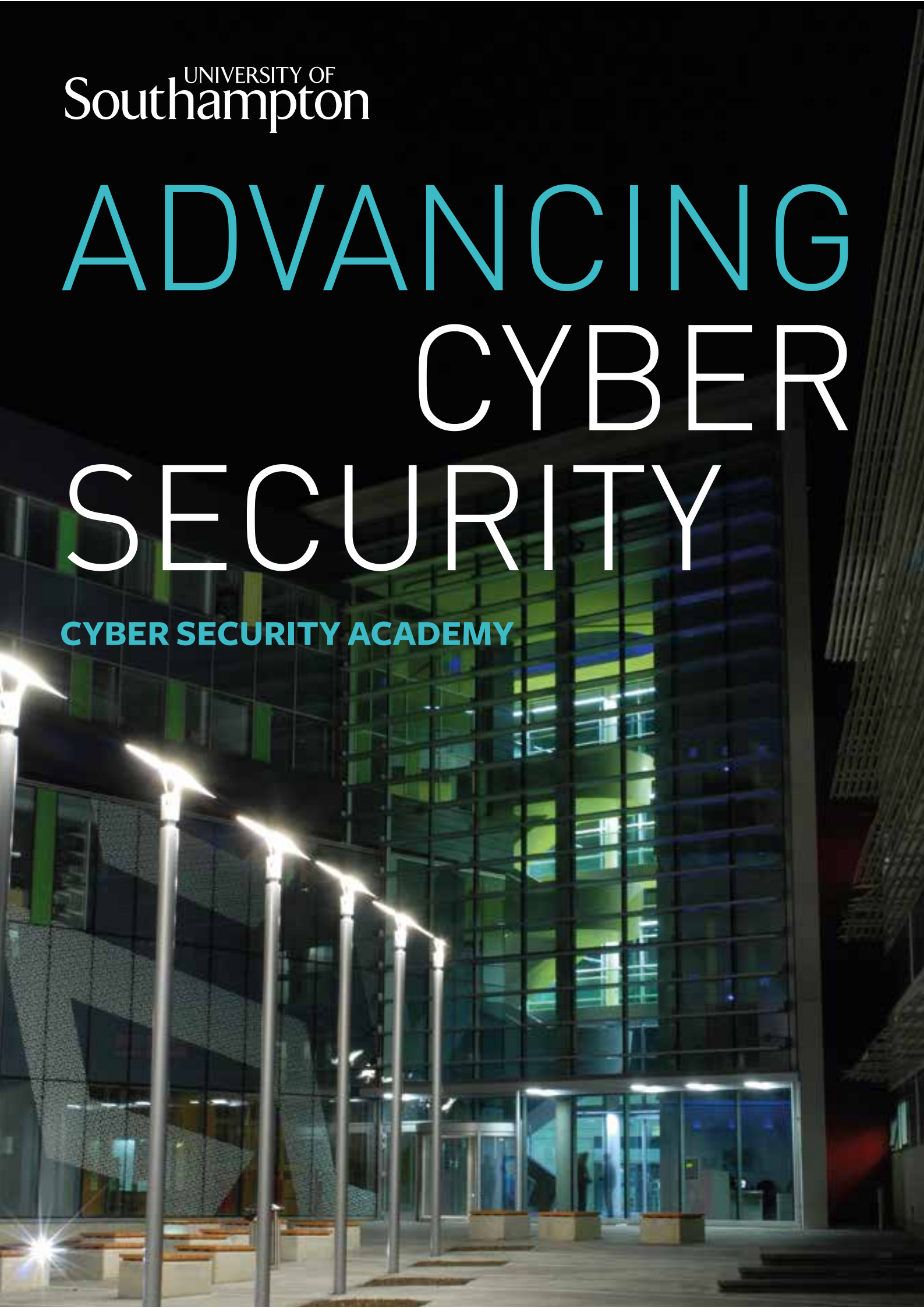
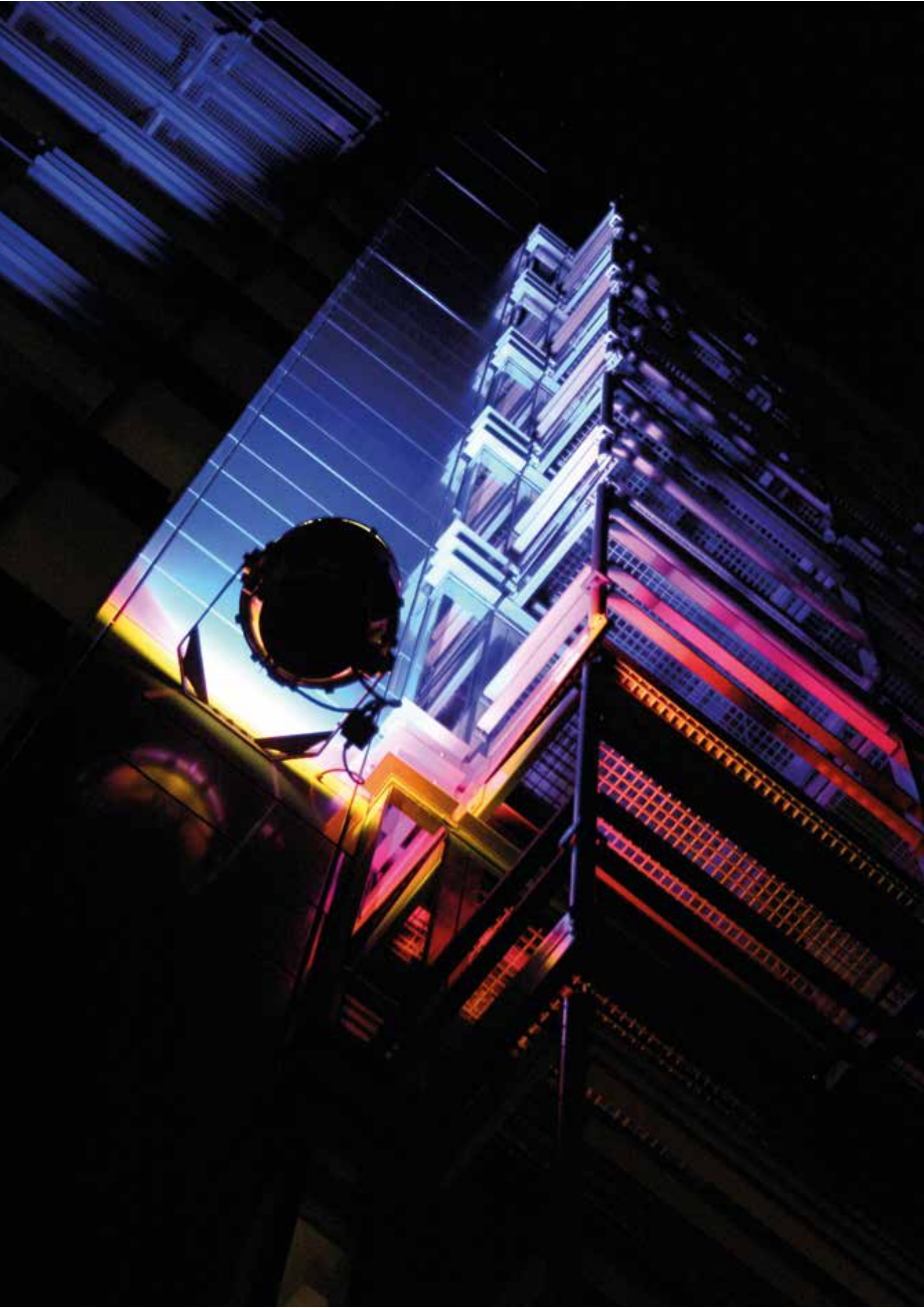


UNIVERSITY OF
Southampton

ADVANCING CYBER SECURITY

CYBER SECURITY ACADEMY





An industry/University partnership to advance cyber security through world class research, teaching excellence, industrial expertise and training capacity.

We are working with our partners developing a dynamic technopole based in the South of England delivering global impact:

Research

World class, strategic project work contributing to a more secure cyberspace

Cyberspace Innovation

Applying research to provide solutions to real cyber security problems

Education

Delivering the next generations of cyber security professionals

Training

Keeping experienced professionals current and cyber security aware

Outreach

Ensuring schools and community engage in best cyber security practice

Core partners

UNIVERSITY OF
Southampton



[dstl]

NORTHROP GRUMMAN

Roke

Part of the
Chemring Group

Part of CyberInvest



HM Government

Partnership

We operate a tiered membership scheme enabling engagement for companies of all sizes. This, coupled with a policy of involving companies from across the spectrum of industrial sectors, ensures that the whole industrial and commercial community is included.

Members of the Academy benefit from a multi-million pound shared research programme, consultancy from globally respected experts, access to educational programmes from a world-class university, recruitment and placement opportunities and significant training for professionals and IT operatives.

Companies are invited to join the academy at the most appropriate level to their needs. For this reason we run a tiered scheme ranging from sponsorship of a student-related activities to full engagement as a core partner.

We are delighted to have established partnerships with DSTL, Northrup Grumman & Roke Manor Research as our Founding Core members.

“We will focus on raising the cost of mounting an attack against anyone in the UK, both through stronger defences and better cyber skills. This is no longer just an issue for the IT department, but for the whole workforce. Cyber skills need to reach into every profession.”

The Rt Hon Philip Hammond MP

Chancellor of the Exchequer

The Cyber Security Academy is a focal point of expertise and will become the hub of a vibrant community of high value companies and institutions.

Driving innovation and delivering significant value, the academy is nationally recognised and will exercise global influence. World-class academic staff engaged in research, teaching, training, outreach and consultancy are supported by a professional team focusing on innovation, technology transfer, and opportunities with industry.

The Cyber Security Academy is based at the Academic Centre of Excellence for Research in Cyber Security (ACE-CSR) at the University of Southampton and provides a vibrant and innovative environment for member companies.

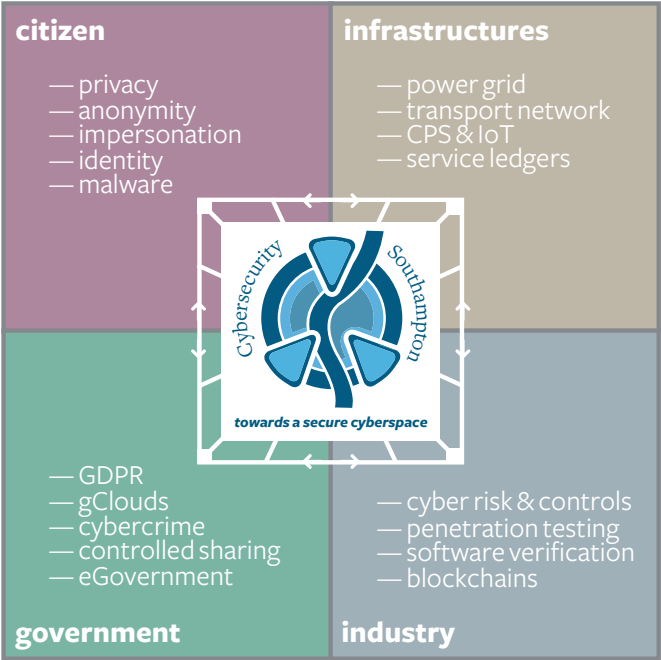
Academic staff members and postdoctoral researchers will work interactively with members on agreed research themes in a shared research consortium scheme. A doctoral training centre is planned with a substantial annual intake of PhD students.

Cyber Security Academy



The Academy will provide a stream of cyber security professionals at all levels of qualification; will train the existing workforce through an industry relevant training programme in Cyber Security and will promote public engagement and schools outreach.

Policy and direction is set by the Strategy Board which is the highest governance body in the Academy. All



core members have a seat on this board ensuring full involvement in the direction of research and the overall strategy of the Academy.

An external Advisory Board will connect the Academy to its government, economy industry and society stakeholders, act as an advocate for it, and regularly review its activities.

Contact us today to join the Cyber Security Academy or request more information.

PROFESSIONAL TRAINING COURSES

Cyber Security for Key Decision Makers

provides a round overview of cyber security and cyber risk for the top executives who are called to make cyber-related decisions in their companies.

Foundations of Cyber Security

aimed mainly at computer scientists and engineers with no systematic body of knowledge of cyber security, it delivers a wide-spectrum, comprehensive programme covering the key aspects of cyber security.

Programming blockchains

aimed at software designers, engineers and developers, it provides hands-on training to programme both public blockchains (like Ethereum) and private blockchains (like HyperLedger).

Creative thinking

drives the audience through the necessary steps and relative techniques to bridge the gap between the conception of a research idea, to the formulation, critique and presentation of a coherent research plan.

Data protection and the GDPR

covers the basics of data protection law, state-of-the-art privacy protection techniques, best practices for data protection risk assessments and personal data governance within organisations.



Defensive programming

illustrates the best modern programming techniques to leverage current hardware security features and produce robust and hacking-resistant code.

Penetration testing

covers the main techniques for penetration testing, with particular focus on reverse engineering the protection of web-based systems.

Professor Vladimiro Sassone is the Roke/RAEng Research Chair in cyber security, and the University's Cyber Security Research Director. The Academy is actively seeking new members from a range of industrial sectors.



For further information:
cyber.ecs.soton.ac.uk



EDUCATION

Three education levels:

MEng in Computer Science with Cyber Security

4 years UG programme aimed at providing the next generation of Cyber Security leaders.

MSc in Cyber Security

1 year UG programme aims at providing the broadest range of Cyber Security to university graduates.

MSc in Cyber Risk

1 year PG programme based in the School of Management learning about Enterprise Risk.

PhD

PG degree aimed at training future Cyber Researchers

Part time MSc to be offered from 2018.



Certified Master's in Cyber Security

Certification of Master's Degrees Providing a General, Broad Foundation in Cyber Security



Certified Master's in Cyber Security

Certification of Integrated Master's Degrees in Computer Science and Cyber Security

THE SOUTHAMPTON CYBER SECURITY ACADEMY

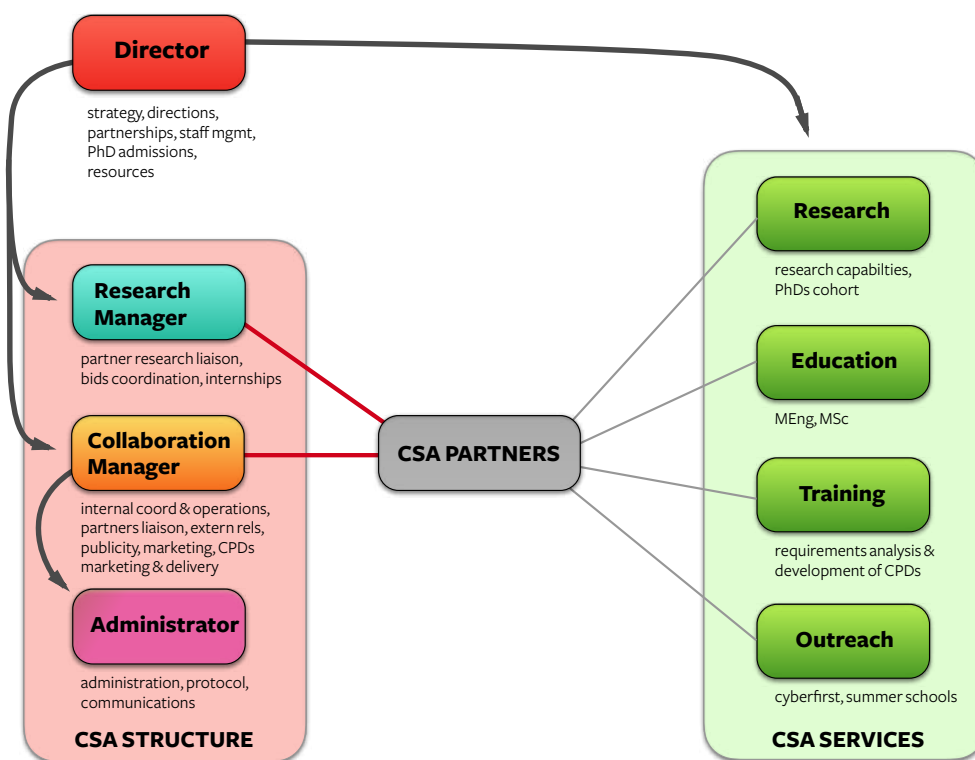
The University of Southampton is proudly engaged in a partnership with key cyber security partners to deliver research, innovation, education, training and outreach. The Cyber Security Academy (CSA) is a rare UK example of academia reaching out to industry systematically, the first and possibly so far the only instance of HMG's CyberInvest scheme.

The CSA has been formed to address the cyber security threats we experience daily, starting from the frequent attacks to individual privacy, to the rampant rise of ransomware, to the most sophisticated nation-sponsored cyber campaigns. As an industry-funded initiative, the CSA has a substantial and varied consortium-based research agenda. As part of the recently re-accredited NCSC's 'Academic Centre of Excellence for Cyber Security Research', the Academy's members include DSTL, Northrop-Grumman, and Roke Manor Research.

Offering PhD, MSc and MEng level degrees and a growing 'Professional Development' programme, the CSA involves researchers from Computer Science, Engineering, Law, Management, Mathematics, Nano-Electronics, Psychology, Sociology and Web Science. The breadth of this research expertise demonstrates the importance which the Academy places on the human, organisational and technical aspects of the cyber security threat, as well as the interrelationships between them.

A comprehensive, industry driven research programme has been devised and the Academy is building research teams which will be directed by industry- and university-based supervisors across a wide range of research themes. We believe that a broad-based, positive engagement with companies and organisations in this exciting and dynamic research environment is the most effective way to deliver a multidisciplinary cyber security message.

CYBER SECURITY ACADEMY



The CSA is organised as in the picture above. The Director functions as a link between partners and the University, and is responsible to both for the formulation and delivery of the CSA programme. The management team is completed by a Research Manager and a

Collaboration Manager, who are the immediate points of contact for the partners. Through such structure, depicted at the left-hand side of the diagram, the partners utilise the CSA services, represented on the right-hand side of the diagram.

RESEARCH TOPICS

RBAC simplifies policy specification and the management of user rights using a two tier management, it groups users into roles and assigns permissions to each role. Administrative role-based access control (ARBAC) is a policy mechanism for controlling how changes can be made to the RBAC policy by various administrators.

Risk Management research focuses on risk analysis and decision-making using quantitative modelling and real-time Big data techniques applies to FinTech and Cyber-Risk research fields, via state-of-the-art high performance computing facilities.

Distributed Ledger Technology aka blockchain, is a main focus and research direction of ours. The fascinating properties of decentralisation, data control and integrity make blockchain a disruptive technology for a variety of application domains, from distributed and cloud computing, to the Internet-of-Things. Through the work we are carrying out, Southampton is quickly emerging as an international knowledge centre on DLT, entertaining new collaborations with industry in the UK and public administrations in Europe and beyond.

FAAS is a main application of blockchain to cloud computing is to underpin the Federation-as-a-Service solution. It is an innovative solution to federate cloud systems ensuring privacy-preserving management of service/data, optimised resource utilisation, decentralised and democratic federation governance. Blockchain offers decentralised computational infrastructure to build cloud federations upon with trust-less data integrity and availability guarantees.

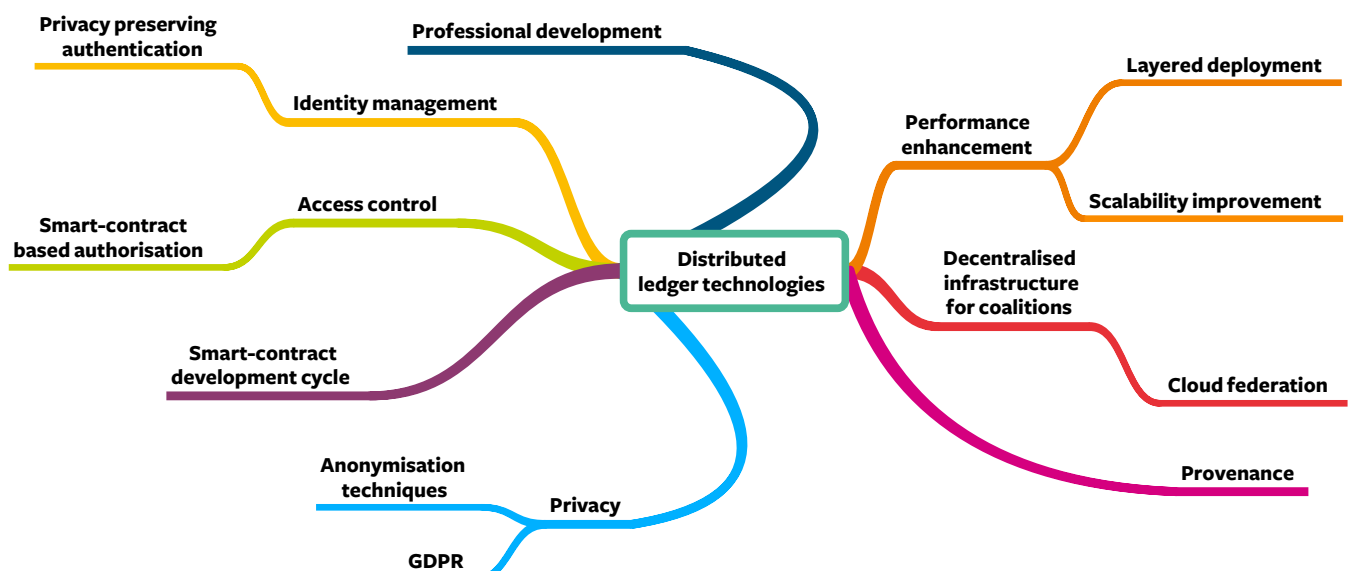
This line of research was to address problems in the public administration space, because some of the

specific requirements of demonstrable data custody and service/data sharing governance normally imposed on governments, typically point directly to the key properties of integrity for data and code afforded by blockchains.

Provenance is the foundation of data quality, capturing the trace of data manipulation over space, time and actors. Provenance becomes critical in application domains such as healthcare where patient safety can be endangered. Based on blockchain technologies, we are focussing on decentralised storage and computation of data provenance to prevent by-design loss and corruption of healthcare data across geographically distributed medical institutions.

Internet-of-Things (IoT), the focus of project Block-IT is a key enabler of new computing systems, but it lacks of a reliable underlying computation infrastructure. Our focus is on using blockchain to underpin distributed IoT devices enabling accountable data storage and management. This line of research targets smart-energy and home automation scenarios aiming at offering blockchain-empowered energy marketplace and autonomous home controllers.

Cyber and the Law works on data situation models relying in part on anonymisation and pseudonymisation practices, and their implications for data protection obligations. The Horizon 2020 FutureTrust project on interoperability of electronic identification and trust services and the interplay between with the General Data Protection Regulation (GDPR) and key data protection principles, such as data protection by design.



Identity and Access Management research focusses on the design of privacy-preserving identity and access management systems that are resilient to cyber attacks. We explore the use of blockchain technology and Intel SGX trusted hardware to guarantee the integrity of users' digital identities and access control policies and of the identity verification and access control protocols. These guarantee both data immutability and integrity and confidentiality of the policy enforcement process.

Health-I focuses on integrating humans into the IoT ecosystem. The project investigates how and where crowdsourcing can be used within an IoT ecosystem to improve trust and user-driven privacy, and provide better human-driven data sharing mechanisms. By using the crowd we build up trust, privacy, & data sharing capabilities in an open and transparent way.

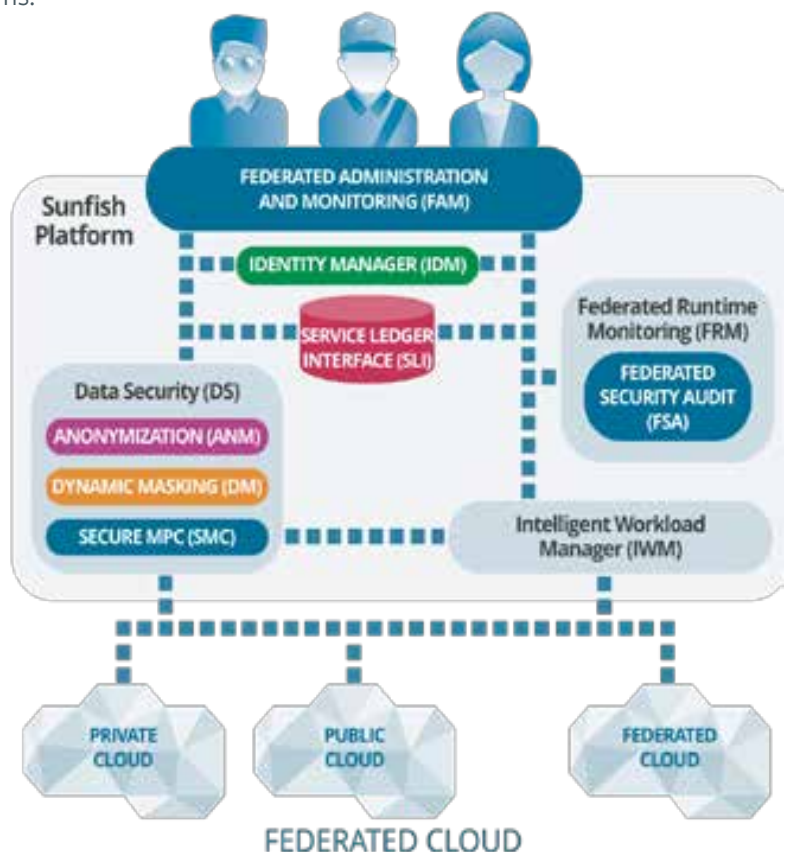
CASTLE is a project funded by the Higher Education Academy to enhance both students' cyber security skills and the University's cyber security posture through supervised penetration testing and a responsible disclosure policy.

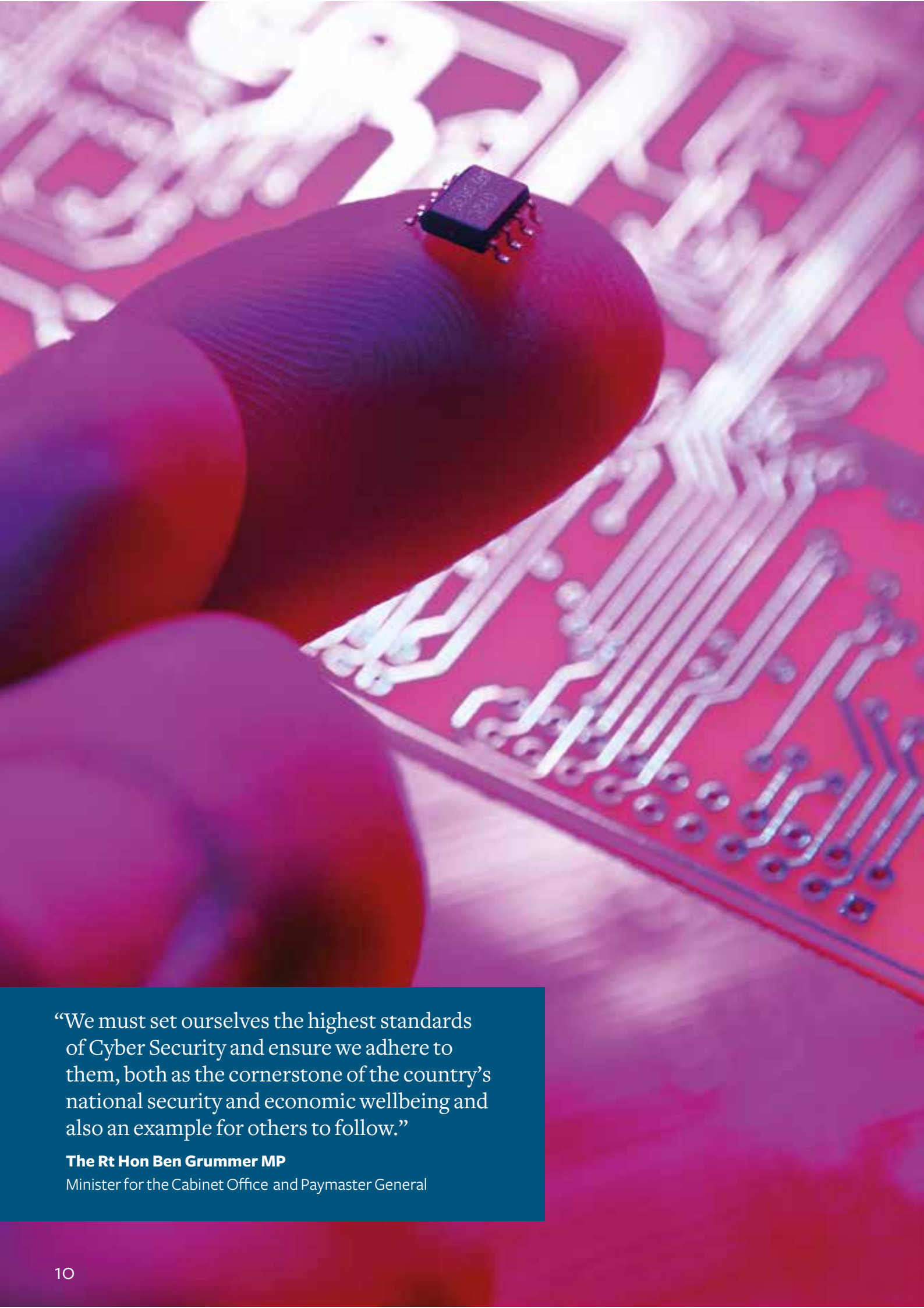
Software Verification & Validation in cyberspace is the focus of project ADVANCE. This is developing a unified tool-based framework for automated formal verification and validation of cyber-physical systems.

GDPR research explores the applicability of GDPR in real terms, with reference to the currently known anonymisation techniques. Our conclusion is that new algorithms are needed if we need to be GDPR compliant. Specifically, we explore advanced indexing to endow differential privacy with resilience to attacks based on repeated queries, through our new notion of context controls.

Government related activities consist of working with government agencies across Europe and beyond to address privacy and security requirements in the public administration. Our current efforts centre on distributed ledgers as computational infrastructure to provide data integrity guarantees.

In the recent past worked with the government on the cyber security of the Internet-of-Things, of the UK Smart Metering Programme as well as the effectiveness of Cyber Essentials. We have established solid working relationships with several agencies including the Cabinet Office, the Foreign and Commonwealth Office, the Information Commissioner's Office, the Italian Ministry of Economy and Finance and the National Crime Agency.





“We must set ourselves the highest standards of Cyber Security and ensure we adhere to them, both as the cornerstone of the country’s national security and economic wellbeing and also an example for others to follow.”

The Rt Hon Ben Grummer MP

Minister for the Cabinet Office and Paymaster General



Professor Vladimiro Sassone

Roke/RAEng Research Chair in Cyber Security

Cybersecurity Academy, Director

University of Southampton

SO17 1BJ United Kingdom

Tel: +44 23 8059 9009

cyber.ecs.soton.ac.uk

Email: V.Sassone@soton.ac.uk

facebook and twitter @CybSecSoton



Dr Andrea Margheri

Research Manager

Cyber Security Academy

University of Southampton

SO17 1BJ United Kingdom

Email: A.Margheri@soton.ac.uk



Sarah Martin

Collaboration Manager

Cyber Security Academy

University of Southampton

SO17 1BJ United Kingdom

Tel: 023 80595891

Email: S.L.Martin@soton.ac.uk

