in association with
National Cyber
Security Centre

Engineering and
Physical Sciences
Research Council

Academic Centre of Excellence in **Cyber Security Research**

Developing our capability in cyber security

Academic Centres of Excellence in Cyber Security Research

Updated July 2020

Contents

Ministerial Foreword: Jeremy Fleming, Director, GCHQ....3

Academic Centres of Excellence in Cyber Security Research....4

Key areas of expertise and specialism....5

University of Birmingham....8

University of Bristol....10

University of Cambridge....12

Cardiff University....14

De Montfort University....16

University of Edinburgh....18

Imperial College London....20

University of Kent....22

King’s College London....24

University of Lancaster....26

Newcastle University....28

Northumbria University....30

University of Oxford....32

Queen’s University Belfast....34

Royal Holloway, University of London....36

University of Southampton....38

University of Surrey....40

University College London....42

University of Warwick....44

Contact Address Book....47

Glossary of terms....51

Developing our knowledge and capability to secure cyber space

Much has changed since the first Academic Centres of Excellence in Cyber Security Research (ACE-CSR) call was launched in late 2011. The UK’s first National Cyber Security Strategy was in its infancy; the concept of a National Cyber Security Centre (NCSC) had not even been conceived, and cyber security research in UK universities was often fragmented along the fault lines of academic disciplines.

Fast forward to 2020, two successive Cyber Security Strategies and a decade of sustained government investment have seen the UK develop into an international Cyber Power. This has led to enormous advances in the nation’s ability to benefit from the opportunities of new technologies and in keeping its citizens safe online. The NCSC has played a central role in that and is now a thriving organisation, with a broad customer base and a record of innovative ways of working, backed by deep expertise.

In 2012, an initial group of eight universities were recognised as Academic Centres of Excellence in Cyber Security Research. This has now grown to an active community of 19 universities encompassing hundreds of academics and spanning disciplines as diverse as computer science, engineering, psychology, sociology, maths, law and humanities.

The impact of their work has been far-reaching: from expert academic input to government policy, to training the next generation of researchers through vibrant Doctoral training programmes; from the establishment of mutually beneficial partnerships between ACEs-CSR and private sector companies, to the promotion and recognition of the UK’s academic research excellence on an international stage. The ACE-CSR universities are testament to what can be achieved when the public, private and academic sectors unite to achieve a common goal. It is this sense of innovation, enthusiasm, shared endeavour and deep expertise which is the hallmark of the ACE-CSR community.

I would like to thank colleagues in the NCSC and our partners in the Engineering and Physical Sciences Research Council (EPSRC) for their collaboration and leadership in this space. I am grateful to industry leaders who continue to look for ways to harness academic research, support researchers and develop our research base. And finally, I would like to thank and congratulate the Vice Chancellors and their senior leaders for their continued investment in and support of the ACEs-CSR within their universities, as well as all the academic and support staff for their ongoing dedication to this important discipline.

The challenges facing us are immense, but the excellence demonstrated by the ACE-CSR universities gives me confidence we are in a strong position to build on the success to date and cement the UK’s position as a world leader in creating a safe, resilient and prosperous cyber nation.

Jeremy Fleming,
Director GCHQ

Academic Centres of Excellence in Cyber Security Research

Academic Centres of Excellence in Cyber Security Research (ACEs–CSR) have been part of the UK Government's National Cyber Security Strategies since 2011 and continue to play a key role in helping Government make the UK secure and resilient in cyberspace.

The ACEs–CSR are based at UK universities which have been recognised as having an established critical mass and pedigree of good quality cyber security research. The initiative is led by the National Cyber Security Centre (NCSC), which is a part of GCHQ and is the UK's Technical Authority for cyber security, and the Engineering and Physical Sciences Research Council (EPSRC), which is a part of UK Research and Innovation (UKRI).

From small beginnings, the community of ACEs-CSR has grown to 19 universities which regularly meet, hold conferences, collaborate, challenge and support one another. In partnership with public and private sector organisations, our aim is to build and maintain a flourishing community of commissioners, producers and consumers of internationally-leading research where everyone works together for the common good.

Developing our capability in cyber security

By recognising the ACEs-CSR, the UK Government aims to:

- Enhance the quality and scale of academic cyber security research and postgraduate training undertaken in the UK.
- Make it easier for potential users of research to identify the best cyber security research and postgraduate training that the UK has to offer.
- Develop a shared vision and objectives among all those involved in cyber security research in the UK.
- Showcase UK academia's internationally-leading research expertise.

This document contains details of all 19 ACEs–CSR and is intended to be a useful reference guide to help stakeholders and potential customers understand the broad range of work happening in the centres. If you would like to discuss your research needs or find out more about what is on offer, please contact the centres directly.

Key areas of expertise and specialism

Page	Name of centre	Key Areas of expertise/specialism
08 - 09	University of Birmingham	• Design of secure systems • Security of embedded systems • Cloud computing security • Privacy technologies for individuals • Network security and malware • Analysis and verification of systems
10 - 11	University of Bristol	• Cryptography • Cyber-Physical Systems • Human Factors • Adversarial Behaviours • Privacy & Online Rights • Network Security • Software Security • Secure Software Lifecycle • Hardware Security • Risk Management & Governance
12 - 13	University of Cambridge	• Socio-technical security, including human factors, user authentication, education • Hardware security and anti-tampering • Network and operating system security • Strategic technologies including processors, architectures, compilers, operating systems • Methodologies including static and dynamic analysis • Cybercrime, frauds and phishing • Privacy and anonymisation • Compromising electromagnetic emanations
14 - 15	Cardiff University	• Artificial Intelligence-driven Security Operations & Incident Management • Malware & Attack Technologies • Risk Management & Governance • Human Factors – susceptibility, individual differences and organised cybercrime • Privacy and Online Rights • Web Security • Network Security • Cyber-physical systems security and resilience • Distributed systems security
16 - 17	De Montfort University	• Cyber physical systems: Industrial control systems, autonomous systems • Risk assessment • Security operations and incident management • Privacy and online rights • Human factors • Formal methods
18 - 19	University of Edinburgh	• Law & Regulation • Human Factors • Privacy & Online Rights • Malware & Attack Technologies • Cryptography • Formal Methods in Cyber Security • Operating Systems & Virtualisation Security • Software Security • Web & Mobile Security • Hardware Security • Physical Layer and Telecommunications Security • Cyber Security and AI

Page	Name of centre	Key Areas of expertise/specialism
20 - 21	Imperial College London	• Software security and the use of formal methods for software and systems security • Security and Resilience of Cyber-Physical Systems • Network analysis, anomaly detection and security operations • Privacy
22 - 23	University of Kent	• Authentication and Authorisation • Communication and Network Security • Security Testing and Verification • Socio-technical Security • AI and Security (AI for security and security of AI) • Digital Forensics and Online Harms • Information Hiding • Quantum Cyber Security
24 - 25	King’s College London	• AI Security and Privacy • Human-centred Security and Privacy • Security Verification and Testing • National Cyber Security Policy • Cyber Deterrence and Defence
26 - 27	Lancaster University	• Security of Large-Scale Networks: • Security of Cyber Physical Systems and Infrastructures: • New forms of Privacy and Identity: • Cyber Security Behaviours:
28 - 29	Newcastle University	• Risk Management and Governance • Human factors • Privacy & Online Rights • Adversarial Behaviours • Cryptography • Distributed Systems Security • Authentication, Authorization & Accountability • Cyber-Physical Systems
30 - 31	Northumbria University	• Human, Organisational and Regulatory Aspects • Network Security • Authentication, Authorisation and Accountability
32 - 33	University of Oxford	• Analysis and verification of software and security protocols • Systems security; trustworthiness and usability • Inter-disciplinary cyber security, policy and governance
34 - 35	Queen’s University Belfast	• Secure hardware and embedded systems • Post-quantum cryptography and advanced cryptography architectures • Security Intelligence - AI for cyber security and mobile security • Networked security systems • Analytics-based monitoring & forensics in new network architectures • Industrial Control Systems and Operational Technology security • Cyber security research translation, innovation, commercialisation and policy advisory
36 - 37	Royal Holloway, University of London	• Cryptography • Social aspects of information security • Software and systems security • Trustworthy autonomous systems
38 - 39	University of Southampton	• AI and ML based data analytics for cyberattack detection and defence, and malware analysis; • Analysis and design of trustworthy software; • Blockchain and Distributed Ledgers; • Cyber identity; • Cyber risk analysis; • Data privacy; • International cyber law; • Provenance, trust and data assurance • Safety-and-Security by Design; • Secure embedded systems; • Secure web technologies; • Security of cyber-physical systems and the Internet of Things; • Security of Critical Infrastructures, transport networks, automotive systems, and smart energy systems (smart home, smart building, smart grid, etc).
40 - 41	University of Surrey	• Cryptography and Formal Methods • Distributed and Networked Systems
42 - 43	University College London	• Anonymous communications • Cryptocurrencies and blockchains • Cryptography and cryptanalysis • Cyber safety • Economics of security • Ethical, legal, and policy aspects of security • Network security • Privacy-enhancing technologies • Program verification and analysis • Security and privacy in Artificial Intelligence • Security in ubiquitous computing • Software and systems security
44 - 45	University of Warwick	• Privacy and Online Rights • Cyber-physical systems security • Authentication, Authorisation & Accountability • Risk Management and Governance • Distributed Systems Security • Physical Layer Security and Telecommunications

University of Birmingham

The School of Computer Science

Who we are

The University of Birmingham Academic Centre of Excellence in Cyber Security Research is comprised of 36 researchers: 15 academics, four postdoctoral researchers and 17 PhD students. It is also home to the UK's only Cyber Security Research Chair (appointed by HP). We are dedicated to research that strengthens our security infrastructures, developing secure systems and protocols that safeguard and protect privacy.

The Birmingham ACE-CSR is also home to a funded automotive security lab, which includes a 2015 Range Rover Evoque and security diagnostic equipment. In the last four years, Birmingham ACE-CSR has been awarded £5.2 million in research funding from EPSRC, NCSC, EU Commission, HP and Samsung. We also have projects in two of the EPSRC-NCSC-funded Research Institutes: the Research Institute in Trustworthy Interconnected Cyber-physical Systems (RITICS), and the Research Institute in Secure Hardware and Embedded Systems (RISE).

What we do

We work in conjunction with a number of national regulatory agencies, government departments, funding bodies and initiatives such as Rail Safety and Standards Board, GCHQ, NCSC and DCMS. We participate in global collaborations with national and international academic colleagues and partners from across a range of businesses, including Jaguar Land Rover, HP, Huawei, Yubico Inc., Security Innovation, Microsoft, IBM, Google, Deloitte, BT and the National Grid as well as regional partners such as ZF TRW.

Our Work

Our expertise lies within a broad range of areas of computer security. We also have multidisciplinary expertise in areas such as law and ethics, behavioural science, and psychology. Through this holistic approach we have built an international reputation for our research.

Our research areas include:

Applied Cryptography: The Centre is developing cryptography techniques aimed at securing vehicles, messaging apps and voting systems, as well as engaging in active research in methods for post-quantum cryptography.

Automotive Security: Together with industry leaders, we are improving the current and future security of next generation electronic vehicles, which integrates wireless interferences to operate immobilisers, wireless locks and GPS. Hundreds of millions of vehicles by 33 manufacturers that cover more than 150 models made between 2000 and 2017 have migrated to more secure systems as a result of vulnerabilities identified by our research. The flaws could have allowed a suitably equipped car thief to either unlock a car or disable its immobiliser and start the engine. This research has led to the improvements in the cryptographic designs used in most vehicle immobiliser and remote keyless entry systems worldwide.

Cloud Security: Our researchers are exploring mechanisms which would allow organisations to encrypt their data before it is hosted in cloud-based storage systems. This would enable them to safeguard it from security threats and breaches, using hardware roots of trust to allow the cloud to operate securely on data.

Electronic Voting: We are focusing on creating procedures that will detect potential fraud and coercion in future electronic voting systems to ensure they do not compromise democratic processes.

Industrial control systems: We are working alongside national organisations and industrial partners in the energy and railway sectors, to identify and eliminate points of cyber attack and increase the security systems of critical infrastructure.

Industrial Control and Railway Systems Security: We are working to assist industry in developing secure products and assuring the security of industrial supply chains, working in collaboration with the UK Rail Research and Innovation Network to secure railway assets.

Internet of Things: We are examining the issues of internet-enabled devices such as cars, thermostats, door locks, traffic lights, trains, TVs and dialysis machines. This investigation covers the architectures and systems through which devices are accessed and information is shared, as well as the analysis of vulnerabilities in specific devices.

Privacy for Society: We are developing systems which aim to offer privacy to individuals and allow for the targeted investigations of criminals such as terrorists, without breaching the privacy of the majority of members of society.

Security of Machine learning: We are evaluating machine learning algorithms that are driving many new technologies, such as home virtual assistant devices (e.g. Alexa and Siri), autonomous vehicles and robots, and are building defences against attacks on these devices that could compromise the safety of their users.

Key areas of expertise and specialism
- Design of secure systems
- Security of embedded systems
- Cloud computing security
- Privacy technologies for individuals
- Network security and malware
- Analysis and verification of systems

University of Bristol

Bristol Security Centre

Who we are

The University of Bristol ACE-CSR is composed of the Bristol Cyber Security (BCSG) and Cryptography Groups (CG). Together, we foster leading international and interdisciplinary programmes of research. This work extends through collaboration with the GCHQ-funded Heilbronn Institute, Smart Internet Lab and Schools of Management, Sociology, Law and Psychology. The Centre plays a leading role in several major initiatives including CyBOK, REPHRAIN, PETRAS, RISE, RISCS and RITICS, and trains future cyber security leaders through its EPSRC Centre for Doctoral Training on Trust, Identity, Privacy and Security in Large-scale Infrastructures.

Research is supported by UKRI (EPSRC, ESRC), the European Commission, and direct investment from industry as well as government departments and organisations such as the National Cyber Security Centre.

BCSG research addresses security and privacy in large hyper-connected infrastructures, with a focus on three interlinked strands: cyber-physical systems, especially critical national infrastructures and Internet of Things (IoT); software security; adversarial and non-adversarial behaviours pertaining to cyber security. The group is highly interdisciplinary, embedding computer scientists with behavioural, social and crime scientists to tackle the human and technological challenges to cyber security, with outputs in major security and privacy, software engineering and human factors-focused conferences and journals.

Research in the CG spans theoretical and practical aspects of cryptography. This combined way of working has led to numerous advances that would not otherwise have been possible. Outputs span all venues of the International Association of Cryptologic Research (IACR), including ASIACRYPT, EUROCRYPT, and CRYPTO, as well as the sub-conferences CHES, FSE, PKC, and TCC.

What we do

A strong ethos of rigorous experimental and empirical research underpins the Centre's research focus. This is facilitated by two state-of-the-art research facilities:

- Critical National Infrastructures (CNI) Testbed: a class-leading cyber security testbed for studying CNI and IoT security, with a wide variety of devices and components to model a range of networks and deploy and test the effectiveness of security tools.
- Hardware Development and Analysis Laboratory: supports work in the applied field of cryptographic engineering.
- A privacy-enhancing technologies testbed to be developed as part of REPHRAIN, the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online.

Research in the CG is focused on supporting the hard problems on which it is based, and the hardware and software needed to implement secure systems. Research topics include foundational research and number theory; design and formal security analysis of cryptographic primitives, protocols, and applications; cryptography implementation in hardware and software, and; traditionally cryptanalytic and implementation-style attacks on cryptographic targets.

Research in BCSG focuses on security and vulnerability analysis of cyber-physical systems; software security research; human and organisational factors; usable security and privacy; data science approaches to cybercriminal activities and countermeasures, including applications in key areas such as online child protection, mitigating mass-marketing fraud, social engineering and disruption of online cybercriminal structures.

Our Work

A few of our completed and active projects include:

Why Johnny doesn't write secure software: A diverse range of people now develop software for phones, websites and IoT devices used by millions of people – previously the domain of those with training. Little is currently known of the security behaviours and decision-making processes of Johnny – our pseudonym for such a developer. This project develops an empirically grounded theory of secure software development, focussing on vulnerabilities arising from Johnny's mistakes, why these mistakes occur and how to mitigate them by promoting secure behaviours.

Cyber Security Body of Knowledge (CyBOK): A major National Cyber Security Programme project, aligning cyber security with established sciences by distilling knowledge from over 100 internationally recognised experts, defining the field's interdisciplinary foundations. CyBOK has been designed to address the workforce gap by informing and underpinning education and professional training for the cyber security sector, through a range of resources including extensive knowledge areas and curriculum mapping support for universities applying for NCSC Degree Certification.

Post-Quantum Cryptography: Quantum Computation represents an important long-term threat to cryptography, where practical quantum computers will render various existing designs (e.g. RSA) insecure. The development and deployment of post-quantum designs resilient to this threat is an ongoing challenge to which CG contributes.

High Assurance Cryptography: Cryptography is almost within the trusted computing base of a given system, meaning a demand for high levels of assurance about correctness of associated implementations, as any incorrectness may degrade the level of security provided. It is attractive to prove that any security assumptions made by design are supported by implementation. Innovations in proof techniques and tools as well as the analysis of security properties of the platforms (such as information leakage) on which implementations execute is ongoing within CG's research priorities.

Key areas of expertise and specialism
- Cryptography
- Cyber-Physical Systems
- Human Factors
- Adversarial Behaviours
- Privacy & Online Rights
- Network Security
- Software Security
- Secure Software Lifecycle
- Hardware Security
- Risk Management & Governance

University of Cambridge

Department of Computer Science and Technology

Who we are

The University of Cambridge ACE-CSR, located at the Department of Computer Science and Technology, includes 12 staff members, complemented by world-leading domain experts across the university, particularly in the Judge Business School, the Engineering Department and the School of the Humanities and Social Sciences.

Frank Stajano, Professor of Security and Privacy and Head of the Cambridge ACE-CSR, says: "Cyber security is a fundamental enabler of the digital society: our collective safety and wellbeing depends on it. Cyber is not a "feature" but a holistic emerging property of a complex system.

"Our vision is that success in cyber security comes from addressing it as a systems issue. Our strongest asset as a cyber security research institution is our unique combination of depth and breadth: at Cambridge we benefit from a renowned core of systems security expertise but, through the rest of the University, we have ready access to world-class experts from other disciplines, ranging from risk management to resilient systems and from socio-economics to criminology and law.

We are therefore uniquely placed to critically analyse and contribute to all aspects of the cyber security problem.

"Without false modesty, few other academic institutions in the country, or in the whole of Europe, have the mix of skills, knowledge and creative people to pursue cyber security as a systems problem as effectively as the University of Cambridge."

What we do

The University of Cambridge has been responsible for world-leading work on digital network protection since before the internet existed: it was at Cambridge, for example, that the now universal practice of protecting the password file with hashing was first conceived and deployed in 1966 and that the Needham-Schroeder protocol, precursor to Kerberos and to the now ubiquitous Windows Active Directory, was invented.

Our recent and current work touches on areas of great impact for society, such as securing global infrastructure and the building blocks of the digital world, and the interaction between people and computers.

Our Work

We founded the Cambridge Cybercrime Centre in 2015 as a multi-disciplinary initiative between computing, criminology and law. We leverage our neutral academic status to collect substantial datasets on cybercrime and mine them for information on criminal activity. We have built one of the largest and most diverse data sets that any organisation holds. We share this hard-to-obtain data with other academics under a strong ethical and legal framework.

We run outreach initiatives such as hacking seminars and high-profile cyber security competitions. We founded the international Cambridge 2 Cambridge CTF competition in 2015, in collaboration with MIT, and the national Inter-ACE CTF in 2016, as our contribution towards closing the skills gap in cyber by raising a new generation of cyber defenders. C2C, renamed "Country to Country", has now expanded to four continents and we continue to serve on its steering committee.

The entrepreneurial spirit of Cambridge academics and graduates has created hundreds of start-up companies, of which several are in the security space.

- Xensource, founded by former Computer Lab staff, on whose Xen hypervisor now runs Amazon's EC2 cloud (the world's largest), was acquired by Citrix for $500M in 2007.
- nCipher, a company founded by a Computer Lab graduate that made cryptographic accelerators, was bought by Thales for $100M in 2008.
- Cronto, co-founded by an academic staff member of the Cambridge ACE-CSR, licenses its secure online banking device to major international banks and was acquired by VASCO for $20M in 2013.
- Bromium, which provides endpoint security through virtualisation and was founded by some of the original Cambridge founders of Xensource, was acquired by HP in 2019.

And, although not security-specific, we also created the Raspberry Pi – the most successful British computer of all time, with over 30 million units sold. Besides founding start-up companies, Cambridge ACE-CSR members have attracted very significant grants towards cyber security research from both industry and government agencies, from UK and abroad.

Of the many Cambridge security projects that have had significant impact worldwide, one in particular stands out as exceptional: CHERI, in development since 2010 in collaboration with SRI International and with support from DARPA. CHERI is a hardware-software-semantics co-design, providing a capability extension to RISC instruction set architectures. It offers fine-grained memory safety all the way from processor to compiler.

ARM, which makes the CPUs in 95% of the world's smartphones, has adopted CHERI in its experimental Morello high-end superscalar processor. In 2019, UKRI announced the £170M Digital Security by Design programme to explore potential applications of CHERI, which it funded in collaboration with ARM, Microsoft and Google.

Key areas of expertise and specialism
- Socio-technical security, including human factors, user authentication, education
- Hardware security and anti-tampering
- Network and operating system security
- Strategic technologies including processors, architectures, compilers, operating systems
- Methodologies including static and dynamic analysis
- Cybercrime, frauds and phishing
- Privacy and anonymisation
- Compromising electromagnetic emanations

Cardiff University

Centre for Cyber Security Research

Who we are

With interdisciplinary expertise from computer science, psychology, criminology and international relations, the Cardiff University Centre for Cyber Security Research (CCSR) offers a holistic, integrated and theoretically informed approach to human and technical cyber security. The Centre includes 18 permanent academic staff and currently supports a further 33 researchers within its postdoc and PhD community.

In the last decade, the CCSR has received significant University backing to grow the core team, and has attracted over £10 million in external grant income from UKRI (including EPSRC, ESRC and InnovateUK), as well as from industry partners. We work with local and international collaborators across all sectors to carry out research that tackles real challenges and excites and inspires our next generation of cybersecurity professionals. We host Airbus' only Centre of Excellence in Cyber Security Analytics. The CCSR leads an EPSRC Doctoral Training Partnership Hub in Cyber Security Analytics, which develops skilled PhD students to research the applications and implications of new and emerging technologies through the fusion of AI, cybersecurity and risk, from both a human and algorithmic perspective.

What we do

Cardiff University is a leading UK academic research unit for cyber security analytics. We focus on the fusion of data science/analytics and artificial intelligence methods, with interdisciplinary insights into cyber risk, threat intelligence, attack detection and situational awareness. Within this scope we have a number of core research themes including:

- Artificial Intelligence-driven Security Operations & Incident Management – early detection and automated responses to cyber attacks.
- Risk Management & Governance – focusing on goal-oriented risk, process and impact modelling, linked to data-driven intelligence.
- Human Factors – individuals' susceptibility to attack, cognitive aspects, and organised cybercrime.
- Cyber Physical Systems Security and Resilience – detecting digital and physical indicators of compromise and mitigating attacks.
- Privacy and Distributed Systems Security – ensuring privacy by design, whether in machine learning-based systems, or improving transparency and trust in distributed (e.g. Cloud) and autonomous (e.g. vehicular) systems.

Our Work

Some example projects from our research themes include:

Artificial Intelligence-driven Security Operations & Incident Management:
Our research has led to the first machine learning models to predict cyber attacks on online social networks and the desktop PCs you would see in every home and office. Part-funded by an EPSRC grant, and taken forward into industrial applications with investment from Airbus, this work has allowed us to make in-roads into proactively blocking and preventing attacks, rather than reacting and repairing. Funding from InnovateUK will enable us to enhance the adoption of AI-driven cyber, by explaining how AI has decided there is a malicious presence on the network to security operations experts, and resilience to adversarial subversion of these methods, as well as changing malware behaviours over time.

This work has also been tested in the context of IIoT devices and Industrial Control Systems – detecting indicators of compromise and modelling/mitigating the impact of attacks through goal-oriented risk and process modelling, cyber incident-response, and lightweight security solutions. We have translated our research on monitoring physical symptoms into a commercial solution, supported by the CyberASAP scheme. We lead the safety-critical systems theme in PETRAS – the National Centre of Excellence for IoT Systems Cyber Security.

Human Factors: Threats to cyber security often have techniques to exploit human susceptibility at their core. Our current projects include developing a fundamental understanding of the role played by human cognition. For example, perception, attention, memory, judgement, and decision making is a critical first step in understanding points of weakness and of suggesting ways to safeguard individuals, companies and institutions. We conduct laboratory and field-based human factors research, often in collaboration with key industry partners, to tackle the increasing occurrence of people falling victim to progressively sophisticated cyber attack techniques. Individual and social cognition also plays a role in understanding the goals and motivation of the originators of the cyber threat. An ongoing ESRC grant is enabling us to study a range of malicious human behaviours in the context of transnational organised crime, and to better understand how to propose online social network interventions to disrupt activity.

Privacy and Distributed Systems Security:
We provide solutions that extract use out of the data that users consent to provide, or to protect privacy as much as possible while guaranteeing a utility level. We are currently working on protecting against sensitive disclosures from published machine learning models.
The ongoing EPSRC PACE: Privacy-Aware Cloud Ecosystems project addresses security and privacy requirements of environments where multiple cloud computing providers need to work collaboratively to offer services to a user.

Key areas of expertise and specialism

- Artificial Intelligence-driven Security Operations & Incident Management
- Malware & Attack Technologies
- Risk Management & Governance
- Human Factors – susceptibility, individual differences and organised cybercrime
- Privacy and Online Rights
- Web Security
- Network Security
- Cyber-physical systems security and resilience
- Distributed systems security

De Montfort University

Cyber Technology Institute

Who we are

The Cyber Technology Institute at De Montfort University (DMU) is one of the three research institutes in the School of Computer Science and Informatics, with strong synergies with the other institutes: the Centre for Computing & Social Responsibility (CCSR) on privacy and ethics, and with AI on its application in the cyber security context. Our ACE-CSR core members consist of 10 cyber security focused staff in the CTI, with additional members from the CCSR and the DMU Business & Law Faculty. The other 20 academics in the CTI work in cyber security as well as in strongly affiliated areas such as smart systems, formal methods, and automotive systems.

We have strong industry links through an Industrial Advisory Group (IAG) consisting of Airbus, BT, Deloitte UK and Rolls Royce. The IAG provides regular input to research, enterprise, and teaching in the CTI. The CTI is an Airbus Centre of Excellence in SCADA cyber security and forensics, and an active member of RISCS and RITICS. It has specialist laboratories for teaching and research, including a training Security Operations Centre (SOC) recently built in collaboration with Deloitte.

What we do

The CTI is a collaborative research hub which focuses on the development of knowledge and technologies to ensure a smart, safe and secure cyberspace.

Our research covers many aspects of cyber security, with a few areas of particular focus. The majority of these areas provide outcomes that are directly applicable in industry and other organisations.

Our work

Activity in Incident Response is supported by the CyRan mobile cyber range, as well as the SOC that has been instrumented to facilitate the observation of human factors. The AIR4ICS project (NCSC/RITICS) developed agile methods for incident response specifically in industrial control systems. Cyber security in such systems in general is another area of focus, broadening this out also to wider consideration of critical infrastructure.

Significant research activities centre around risk assessment. The ACTIVE project (InnovateUK) developed methods for optimising cyber investment decisions based on cyber intelligence sharing and cyber risk measurement. Board level cyber security decision making is also supported through gamification in the SCIPS serious game, which connects cyber investment to a cyber attack playing out in tandem.

An ongoing project looks at privacy risk and impact assessment, in collaboration with data protection professionals working across a wide variety of contexts. This has led to experimental research to measure privacy effects, complementing earlier foundational research in privacy metrics, including in smart cities and for genomic data. Our research into human error in cyber security has had notable impact in industry and healthcare.

We work in collaboration with academics in economics, criminology, law and psychology in the interdisciplinary investigation of cyber crime. In particular, DMU led the EPSRC project EMPHASIS in which six universities investigated ransomware from multidisciplinary angles. Synergy with world leading AI research at DMU occurs in the application of machine learning techniques in intrusion detection systems and malware analysis.

Core members of the ACE-CSR also work on distributed ledger technology and its cryptographic underpinnings, with applications in authentication and electronic business.

Key areas of expertise and specialism
- Cyber physical systems: Industrial control systems, autonomous systems
- Risk assessment
- Security operations and incident management
- Privacy and online rights
- Human factors
- Formal methods

University of Edinburgh

Cyber Security, Privacy and Trust Institute

Who we are

The University of Edinburgh's ACE-CSR unites a diverse set of researchers under the umbrella of the Cyber Security, Privacy and Trust Institute. Our core expertise is in the School of Informatics, the largest computing department in the UK. Beyond Informatics, cyber security research takes place in Design, Engineering, Maths, Sociology, Law, Politics & International Relations and Social & Political Sciences.

We have several connected inter-disciplinary groups. CeSeR (Centre for Security Research) considers critical security studies, policy and governance, including privacy and surveillance. SCRIPT (Scottish Research Centre for IP and Technology Law) considers relationships among law, ethics, commerce and society. The long-running ISSTI (Institute for Study of Science Technology and Innovation) addresses relevant sociological questions, extended by the recently founded Edinburgh Futures Institute with its established Chair in the Ethics of Data and AI. The University of Edinburgh is a founding partner of the Alan Turing Institute, linking to security and ethics research there.

Our ACE-CSR connects to other Scottish Universities through SICSA (Scottish Informatics and Computer Science Alliance), and the Scottish Government supported SICSA Cyber Nexus project. This feeds into Scotland's Cyber Resilience programme, helping develop the regional skills base and solving problems for industry, public sector and government.

What we do

We tackle research questions raised by current technologies and longer-term problems raised by future and emerging technologies. Typically, our research approach flows from fundamentals to application, concentrating on finding correct and robust solutions and often exploiting multi-disciplinary knowledge.

We have a range of national and international industry partners. Our translational and applied research are supported by a dedicated commercialisation team in the Bayes Centre, an innovation hub for Data Science and AI, and also by Edinburgh Innovations, the University's innovation subsidiary.

We offer an MSc and two PhD programmes in Cyber Security, Privacy and Trust. Our four-year PhD programme is a partnership scheme which embeds external innovation training and internships.

Our work

In our current large projects, we are investigating:

- Security-by-construction, applying programming languages, logics and data science to cyber-physical systems such as autonomous vehicles and surgical assistance robots, and to future computer architectures.
- Foundations and applications of distributed ledger, including new cryptocurrencies, smart contracts with cryptographic and formal assurance, and e-voting protocols.
- Network architectures for 5G and 6G, including assurance frameworks with built-in monitoring, AI-based network management, and physical layer security enabled by optical wireless systems.
- Internet-of-Things, including intelligent algorithms that can detect and counteract cyber threats in home IoT, and how cloud-and-edge AI systems can support human trust and ethically-sensitive design.
- Cyber risk associated with emerging FinTech, using data-driven designs to optimise next generation mobile services for banks, trading and insurance firms.
- Sociotechnical security solutions, such as using PETs (Privacy-Enhancing Technologies) to tackle adversarial online influences and privacy violations, and devising governance approaches for biometric and online technologies that sense, learn and interact with emotions and moods.
- Quantum cyber security, finding replacement algorithms which resist future quantum computer attacks, as well as applying current quantum devices to provide new, stronger security solutions.

Key areas of expertise and specialism
- Law & Regulation
- Human Factors
- Privacy & Online Rights
- Malware & Attack Technologies
- Cryptography
- Formal Methods in Cyber Security
- Operating Systems & Virtualisation Security
- Software Security
- Web & Mobile Security
- Cyber Security and AI

Imperial College London

Imperial College London

Engineering Secure Software Systems

Who we are

Imperial was one of the first recognised Academic Centres of Excellence in Cyber Security Research and has played a significant role in the national cyber security programme. We are leading the Research Institute in Verified Trustworthy Software Systems (VeTSS) and the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS) and help run the PETRAS National Centre of Excellence for IoT Systems Cybersecurity.

The Imperial College London ACE-CSR is a broad group comprising over 25 members and several associate members across three departments. We cover an extensive research portfolio that converges on developing methods, tools and techniques for Engineering Secure and Resilient Software Systems.

The ACE-CSR is led from within the Institute for Security Science and Technology (ISST), which coordinates and applies interdisciplinary research and innovation to national security and resilience challenges. ISST draws upon more than 150 internal affiliates, as well as visiting fellows from across government and industry, giving the ACE-CSR the opportunity to enable and coordinate research initiatives and programmes across the entirety of the College.

What we do

Over the period 2011-2016 our members held over 75 grants worth £35.5 million and graduated over 25 doctoral students, with many more ongoing. The work is often conducted in collaboration with public and private sector partners and many of the projects involve collaborations with other universities worldwide.

Our research activities range over a broad spectrum, from quantum techniques to computational privacy and adversarial machine learning, from physical layer security to mobile security and cloud environments, from practical deployments to formal methods and analysis. Broad themes of work include:

- Software security and the use of formal methods for software and systems security
- Security and Resilience of Cyber-Physical Systems
- Network analysis, anomaly detection and security operations
- Privacy

Our work

Under RITICS, we used optimisation techniques to evaluate different defensive strategies against various attackers, and looked at the role of diversity in defending against zero-day attacks. This has led to multiple international collaborations and an award-winning publication.

Our work on the security of cyber-physical systems has led to new techniques to defend sensor environments against malicious data injection attacks and to sensor deployment assessment methods at various levels of risk. We have significantly improved the scalability of risk analysis techniques based on attack graphs and are investigating new methods for network resilience and reconfiguration in response to attacks.

Statistical cyber security work has explored the use of graph theory, time series analysis, change detection, self and mutually exciting stochastic processes, latent factor models and cluster analysis for building predictive models of normal and adversarial behaviour. Collaborative work has been performed together with government research labs and industrial partners including EY and Microsoft.

We have taken a global lead on using Intel's SGX technology for trusted execution, building substantial expertise and funding. We explored if Intel SGX is vulnerable to new types of attacks, and how it can be used to protect legacy applications and design new secure applications.

Our work in providing certified verification of client-side web programmes has developed JSIL, an intermediate language well-suited for JavaScript verification, to which we compile JavaScript programs; JS-2-JSIL, a correct compiler from JavaScript to JSIL, currently being used by Amazon; and JSVerify, the first verification tool for JavaScript, which will be used for proving different classes of trace properties of JavaScript programs.

We have designed a suite of tools for formal analysis, verification and testing of GPU programs and compilation tools. The tools have been used to find various defects in a number of compilers from major vendors including, AMD, Apple, ARM, Intel, NVIDIA and Qualcomm, and formed the basis of a spin-out company called GraphicsFuzz which was acquired by Google in 2018.

We have uncovered design flaws and severe vulnerabilities on real-world mobile systems, including the Android operating system, Amazon Services and commodity IoT devices. In response, our work has introduced tools, methods and end-to-end systems to improve privacy and strengthen security.

IoT and personal data space privacy and security has also been a focus as part of the EPSRC Databox and Defence Against Dark Artefacts projects. Our extensive data collection and analysis test bed has been instrumental to industry collaborations and bug finding, as well as government policy recommendations in the IoT space.

We are investigating the vulnerability of machine learning systems including both mechanisms that can allow sophisticated attackers to compromise machine learning systems, as well as designing new defensive techniques to mitigate such attacks. We are also applying this in the context of federated machine learning platforms.

Key areas of expertise and specialism
Imperial's work focuses on engineering secure and resilient software systems, including:

- Software security and the use of formal methods for software and systems security
- Security and Resilience of Cyber-Physical Systems
- Network analysis, anomaly detection and security operations
- Privacy

University of Kent

Who we are

Kent Interdisciplinary Research Centre in Cyber Security (KirCCS) was established in 2012. The Centre harnesses expertise from different disciplines across the University of Kent to address current and future cyber security challenges. The interdisciplinary focus of the Centre is reflected by our current 18 Core Members from two academic schools (Computing, Engineering and Digital Arts), and over 50 Associate Members from more than 10 different academic schools covering a wide range of subjects in the sciences, social sciences and humanities.

Since 2012, we have successfully attracted around £10 million of external funding to the University of Kent for cyber security related research projects, many of which have involved interdisciplinary research. Our research has been funded through public sector funders such as UKRI (especially EPSRC and Innovate UK), European Commission, NCSC, Dstl, and by our industrial partners.

What we do

Research at KirCCS has grown significantly since its inception. The Centre's current cyber security capabilities are organised into four main research themes:

- Authentication and Authorisation
- Communication and Network Security
- Security Testing and Verification
- Socio-technical Security and Privacy

In addition to research and enterprise, KirCCS is also actively working and engaging with governmental bodies, industry, schools, NGOs and media on joint projects, innovations, public engagement, outreach activities, professional training and other initiatives in cyber security. For instance, the University of Kent is an academic partner of the Chartered Institute of Information Security (CIISec) and a Network Member of the Academic RiSC, and KirCCS has an appointed membership on UK Government's Biometrics and Forensics Ethics Group.

Based on the success of KirCCS, the University of Kent is in the process of setting up the Institute of Advanced Studies in Cyber Security and Conflict (SoCyETAL), which will cover both cyber security research and educational activities.

Our Work

Authentication and Authorisation: Work in this theme concentrates mostly on Cyber Security Body of Knowledge (CyBOK) Knowledge Areas (KAs) "Authentication, Authorisation & Accountability", especially on user authentication (passwords, biometrics-based authentication, behavioural authentication), authorisation, identity management and verifiable credentials. Some work in this theme focuses on human behaviours in user authentication and some looks at user authentication on mobile devices, thus relating to CyBOK KAs "Human Factors" and "Web & Mobile Security". KirCCS hosts one of the largest research groups working on biometrics in the UK, addressing issues of algorithmic design, mobile platforms, usability and standardisation.

Communication and Network Security: Most work in this theme falls within CyBOK KA "Network Security", and some work relates to other KAs such as "Distributed Systems Security" (e.g. blockchain), "Operating Systems & Virtualisation Security" (e.g. cloud security), "Forensics" (e.g. network forensics), "Cyber Physical Systems" (e.g. IoT security), and "Physical Layer and Telecommunications Security" (e.g. physical-layer identification based on intrinsic device signatures). Work in this theme has benefitted from close collaboration with industrial partners in the telecommunication sector.

Security Testing and Verification: Work in this theme spans across several CyBOK KAs particularly "Software Security" and "Malware & Attack Technologies", but also "Hardware Security", "Web & Mobile Security", "Network Security", and "Cryptography". A major application area in this theme is automatic malware and vulnerability detection via static analysis, conducted mainly by researchers from the world leading PLAS (Programming Languages and Systems) research group of the School of Computing at the University of Kent. Members of the PLAS group also work on providing a formal programming language semantics, to act as an improved foundation for the verification of security properties.

Socio-technical Security and Privacy: Research work in this theme spans several CyBOK KAs especially "Human Factors", "Privacy & Online Rights", "Law & Regulation", "Risk Management & Governance", and "Adversarial Behaviours". This interdisciplinary theme involves most of the Core and Associate Members of KirCCS from all participating schools, and intersects with the three other themes especially with "Authentication and Authorisation" (e.g. usability of password/ biometrics-based authentication systems and identity management systems) and "Communication and Network Security"
In addition to the above four research themes, members of KirCCS have been active in a number of cross-cutting research areas in cyber security, including the following:

- **AI and Security** (including AI for security and security of AI, which can map to almost all technical KAs of CyBOK),
- **Digital Forensics and Online Harms** (including computer forensics, multimedia forensics, cybercrime, online child protection, false information detection and prevention, and cyber threat intelligence),
- **Information Hiding** (including steganography, steganalysis, and digital watermarking),
- **Quantum Cyber Security** (i.e. quantum-resistant cyber security systems based on quantum mechanics).

These cross-cutting research areas can be mapped to a number of CyBOK KAs such as "Forensics", "Security Operations & Incident Management", "Malware & Attack Technologies", and "Adversarial Behaviours".

Key areas of expertise and specialism

- Authentication and Authorisation
- Communication and Network Security
- Security Testing and Verification
- Socio-technical Security and Privacy
- AI and Security (AI for security and security of AI)
- Digital Forensics and Online Harms
- Information Hiding
- Quantum Cyber Security

King’s College London

KCL Cyber Security Centre

Who we are

The Kings College London (KCL) Cyber Security Centre brings together a diverse community of researchers across KCL, working on the socio-technical aspects of cyber security, including academics at the Department of Informatics, the Department of Engineering, the Department of War Studies, the Department of Defence Studies, the Department of Digital Humanities, the Dickson Poon School of Law, and the Policy Institute.

The Centre currently involves more than 40 academics across these departments and a multi-million pound portfolio of projects funded by EPSRC, ESRC, UKRI, InnovateUK, EU Horizon2020, NCSC, US Office of Naval Research Global, US Air Force Office for Scientific Research, European Office of Aerospace Research & Development, Google and PTDF.

What we do

While the KCL Cyber Security Centre provides expertise on most areas of cyber security, it has a critical mass of researchers working on three main research themes and their interrelationships:

1. **AI Cyber Security** – this includes both the use of AI to address cyber security problems as well as the cyber security of AI itself.

   In particular, AI for Cyber Security covers the application of a broad spectrum of AI techniques to cyber security, from data-driven techniques such as Machine Learning, to knowledge-based, symbolic techniques such as Argumentation and Normative Systems. Cyber Security of AI focuses on the security, trust, privacy and transparency guarantees of AI models, as well as of the systems that embed AI models.

2. **Formal Cyber Security** – this includes the theoretical aspects of cyber security, such as theoretical computer science approaches for verification and testing to provide assurance, correctness and technology-readiness of security protocols, security ceremonies, mobile and web applications, and cyber-physical systems and the Internet of Things (IoT).

3. **Strategic Cyber Security** – this addresses the socio-political, strategic and international aspects of cyber security. These include national cyber security policy, military cyber operations, cyber deterrence and defence, cyber diplomacy, cyber intelligence, and cross-cutting issues of risk assessment, management and governance.

Our Work

The following highlight a selected set of both active and recently completed projects at the KCL Cyber Security Centre:

SAIS: Secure AI assistants, funded by EPSRC, will provide an understanding of attacks on AI assistants (AIS) considering the whole AIS ecosystem, the AI models used in them, and all the stakeholders involved. It will focus particularly on the feasibility and severity of potential attacks on AIS from a strategic threat and risk perspective. Based on this understanding, SAIS will propose methods to specify, verify and monitor the security behaviour of AIS and the AI models they embed, based on symbolic AI techniques. These are known to provide richer foundations than data-driven ones for explanations of the behaviour of AI-based systems. It will also co-create security explanations following a techno-cultural method to increase users’ literacy of AIS security.

DADD: Discovering and Attesting Digital Discrimination, funded by EPSRC, is an ongoing project focusing on the undesired effects of personal data use in AI-based systems, particularly discrimination against users because of protected characteristics. DADD is developing a cross-disciplinary understanding of the nature of digital discrimination and its relation to AI bias, and methods to assess discrimination in AI-based systems underpinned by symbolic AI techniques through non-discrimination norms. It considers different levels of access to the AI models in the systems, as well as different kinds of transparency depending on the stakeholders involved.

RePriCo: Resolving Multiparty Privacy Conflicts, funded by EPSRC, focused on multiuser access control decisions and how to support them using AI techniques. The project was the first to create a large-scale empirical base to understand multiparty access control conflicts. This project also proposed a novel way of resolving multiuser access control conflicts based on Argumentation, and the efficacy of the approach was tested in a large-scale experiment with more than 900 participants, which demonstrated that the use of arguments significantly improves the optimality of the decisions made. The outputs were published in the top human-centred security venues (CHI, TOCHI).

Brexit and Cyber Security, funded by NCSC, analysed the potential impacts of Brexit on cybercrime policing and cyber threat intelligence sharing, following a multi-stakeholder approach. The findings were published by the influential and renowned international security and defence think-tank Royal United Services Institute (RUSI) in their flagship journal.

‘Active Cyber Defence: Scaling Up from Government to Nation’, funded by ESRC, explored the UK NCSC’s Active Cyber Defence programme and its potential expansion beyond the public sector. We worked closely with NCSC to develop our independent assessment of the ACD programme, the results of which were reported widely in the press and in government and parliamentary reports.

Key areas of expertise and specialism
- AI Security and Privacy
- Human-centred Security and Privacy
- Security Verification and Testing
- National Cyber Security Policy
- Cyber Deterrence and Defence

Lancaster University

Security Lancaster

Who we are

The Cyber Security Research Centre (CSRC) at Lancaster University is nationally and internationally renowned for its multidisciplinary research that puts the person at the heart of security decisions. We are one of the few centres to tackle human and technological cyber security challenges in socio-technical systems. Since gaining ACE-CSR recognition in 2012, our cyber security community has grown from 10 to more than 26 academics, and comes as a result of strategic investments by Lancaster University, which sees security and cyber-security research as a priority.

Our research philosophy is built around four defining pillars, developed through reflection on our own practices and engaging with the literature:

A socio-technical approach: We consider humans, organisations and technical systems together, enabling us to more insightfully encapsulate the socio-technical aspects of security and establish distinctions between concepts as online/offline, attacker/insider, risk/protection.

Based on grounded, systems-centred research: We undertake studies of large-scale socio-technical settings and validate novel cyber security solutions emerging from our research in real-world settings, or through state-of-the-art facilities, such as our Industrial Control Systems and Software-defined Networking testbeds.

Design with resilience in mind: We design systems able to operate under attacks and our focus on novel resilience approaches keeps attackers out and improves the survivability of large-scale socio-technical systems.

Engage with the very best partners: We combine our expertise with our partners to tackle key cyber security problems and support us in undertaking disruptive, innovative research with considerable, internationally recognised, socio-economic impact.

What we do

Our research in the CSRC is focused around four key themes:

Security of Large-Scale Networks: We perform theoretical and experimental research to increase the resilience, survivability and dependability of networks. Examples of this include the EPSRC/BT Prosperity Partnership, NG-CDI (Next Generation Converged Digital Infrastructure), an ambitious £5 million multi-disciplinary collaborative partnership programme, geared towards creating a radically new architecture for the UK's internet and telecommunications infrastructure. We have cutting-edge facilities to develop and test new products and processes, supported by SDN and NFV testbed facilities, and a CyberThreat Lab developed through collaboration and investment from Fujitsu.

Security of Cyber Physical Systems and Infrastructures: We develop techniques to address security problems of cyber physical infrastructures commonly known as the Internet of Things (IoT), developing new approaches to systems, communications, and understanding an infrastructure's unique risks to develop resilient platforms to support the automation of physical processes in domains such as the nuclear industry. This research is supported by our ICS (Industrial Control Systems) lab that hosts real equipment found in control environments.

New forms of Privacy and Identity: We explore new forms of identity for technology and humans, working alongside other leading universities and industrial partners on large scale projects like PETRAS (Privacy, Ethics, Trust, Reliability, Acceptability and Security). Lancaster University is also the home to IsoLab, the most advanced environment for studying quantum systems in controlled conditions.

Cyber Security Behaviours: Using a combination of psychology and linguistic techniques, we undertake studies of how specific individuals or groups use the internet, and, conversely, how we can use internet behaviour to make inferences about an individual's actions, both of regular users and adversaries. Examples of this include our research on the detection of insider threats, sophisticated social engineering attacks, noise-aware stylometry and mimicry in online conversations, led by CREST (Centre for Research and Evidence on Security Threats).

Our Work

Some examples from our portfolio of world-class, interdisciplinary research and engagement activities:

EASY-RES: Developing novel control algorithms and innovative Ancillary Services, which will allow the penetration of up to 100% of renewable energy sources in the European energy system. EASY-RES is paving the way for a more sustainable power grid, which delivers energy from renewables, reliably and securely.

H-unique: Driven by casework and ground-breaking research in forensic identification from images in child abuse cases. H-Unique is the first multi-feature automated examination of visible hand anatomy through the analysis and interpretation of human variation. This is a large interdisciplinary project supported by anatomists, anthropologists, geneticists, bioinformaticians, image analysts and computer scientists. Its aim is to accelerate identification, reduce exposure of investigators to indecent images and considerably increase capacity for casework.

Cyber Foundry: The Cyber Foundry is a series of multi-million-pound secure digitalisation projects that will help SMEs across the Greater Manchester and Lancashire regions to defend, innovate and grow their businesses. The GMCF and LCF projects are working with over 250 companies to develop cyber security-based business growth and productivity strategies, and more than 60 companies to develop new products and services.

Business & Engagement and Knowledge Exchange: The team here have extensive experience in business and student engagement and collaborative research. Since 2005, the team have assisted over 1,000 SMEs through funded projects and programmes, to transform ideas into new digital products, processes, services and strategies, providing expert advice to business and public sector bodies.

Key areas of expertise and specialism

- Security of Large-Scale Networks:
- Security of Cyber Physical Systems and Infrastructures:
- New forms of Privacy and Identity:
- Cyber Security Behaviours:

Newcastle University

Newcastle University Cyber Security & Resilience

Who we are

Newcastle University founded its cyber security research initiative in 2010 in response to the increasingly important global scope of cybercrime and the growing need for dependably resilient systems. Recognised as an ACE-CSR in 2013, Newcastle University Cyber Security & Resilience pursues a holistic research vision in this area, from the protection of cyber systems supporting society to the socio-technical aspects of cyber security.

While we have roots in Newcastle University's School of Computing and its Secure and Resilient Systems (SRS) group, our remit is across faculties including, for example, the Newcastle University School of Engineering, the Business School, and the Newcastle Law School.

Our ACE-CSR hosts 10 permanent academics in core cyber security topics, plus a range of academics interested in dependability, model-based engineering and reasoning, artificial intelligence, scalable computing, electrical engineering, medicine, psychology, and law.

What we do

Following the conviction that cyber security does not arise from protecting systems alone, we complement core systems security research with studies in human, organisational and socio-technical aspects of cyber security. Overall, we pursue a vision of 'Protecting Society's Fabric'.

In our systems security work, we investigate cryptographic protocols and their applications, distributed systems security, authentication, authorisation, and accountability, complemented by interests in malware, adversarial behaviour, and forensics.

In this research, we are interested in systems, big and small. Benefiting from the Newcastle Urban Observatory and our purpose-built and sensor-instrumented Urban Sciences Building, we pursue research in the cyber security and privacy of smart buildings and smart cities as well as of cyber-physical systems, in general. At the same time, we have a keen interest in the security and privacy of the Internet of Things (IoT) and its manifold devices.

When it comes to human and organisational aspects of cyber security, we research risk management and governance – for instance, in FinTech. We study privacy and online rights with a range of topics, including privacy-enhancing technologies (PETs) and human behaviour and decision making in face of privacy. We are interested in data protection, transparency and regulatory aspects, especially as applied to AI and algorithms. Finally, we investigate human dimensions of cyber security, in general, especially as manifested in our contributions to the UK Research Institute in Sociotechnical Cyber Security (RISCS).

We benefit from Newcastle's tradition of world-leading research in dependability and formal methods, as well as from rigorous quantitative and evidence-based underpinnings in the research of the human aspects of security and privacy. Our cyber security research is reinforced by Newcastle's growing strength in data science: Newcastle University is home to the National Innovation Centre for Data and partners with the Alan Turing Institute.

Our Work

Our current and recent work includes inter-disciplinary projects, often considering systems as a whole, such as in the following examples:

In **PETRAS**, we investigate privacy, ethics, trust, reliability, acceptability and security of IoT devices, systems and networks. We study smart buildings as whole socio-technical systems, including their inhabitants and their privacy, collected data and their legal and ethical issues.

In the European Research Council project, **CASCAde**, we enable the security assurance of evolving topologies, while preserving confidentiality, considering not only the system as a whole in relation to the attestation of its constituent parts, but also the users and their trust in the overall assurance.

Our work in **CRITiCaL** and **EMPHASIS** aims at conceptualising cybercrime psychologically and criminologically while pitting the strengths of machine learning against it, e.g., with detection of attack vectors, and automated classification of ransomware.

In our **FinTrust** work, we aim at infusing trust in the growing FinTech industry, especially focusing on automation and machine learning algorithms, balancing commercial interest with societal interests and addressing the potential biases of the algorithms involved.

Key areas of expertise and specialism

- Risk Management and Governance
- Human factors
- Privacy & Online Rights
- Adversarial Behaviours
- Cryptography
- Distributed Systems Security
- Authentication, Authorisation & Accountability
- Cyber-Physical Systems

Northumbria University

Cyber Security Research Group

Who we are

The Northumbria University Cyber Security Research Group brings together disciplines from across the university to advance cyber security research. The ACE-CSR comprises of core members of staff from computing and psychology, as well as further associate members who join us from subjects including business, law and design.

We use these diverse perspectives to address challenges in a unique and holistic way, that takes into account context, human behaviours and technology design, to fully address the cyber security vulnerabilities facing individuals, organisations and governments.

The Centre plays an important role in Northumbria's Multidisciplinary Research strategy. The digital and human design theme provides a 'think tank' environment for critical inquiry at the intersections of people, place and interactive digital and other emerging technologies. We also work closely with members of the Centre for Crime and Policing around digital technology and policing as well as law and governance.

What we do

Our ultimate aim is to deliver end to end secure solutions that address the broader human, legal, ethical and societal aspects of security, privacy and trust. Our four research themes are:

Network security and intrusion detection: We focus on cutting edge research into the design and development of end to end secure and reliable network systems. We aim to find solutions using state of the art sonification and visualisation techniques, to detect intrusions and machine learning techniques that mitigate security threats and vulnerabilities while exploring potential biases.

Authentication, authenticity and identity management: Here, the team conducts work on biometric encryption, digital forensics, biometric recognition including face and activity recognition, novel authentication methods, machine learning for media security, image/video authentication and watermarking and secure and trusted identity and access management.

Usable, human-centred sociotechnical security: We focus on a social/psychological approach to human-centred, usable security. The aim is to model cyber security behaviour across a number of contexts, apply psychological models of behaviour change, assess the psychological correlates of digital hoarding, cyber risk and cyber insurance uptake and take an inclusive approach to cyber-security, addressing the issues facing marginalised and stigmatised communities including hate crimes and algorithmic bias.

Forensics, law, digital policing and online rights: We explore digital and sensor forensics, online grooming detection, hate crimes, online privacy including marginalised and stigmatised groups, children and family. We are particularly interested in ethical aspects of big data and AI, the data shadows data analytics can create, and the potential for algorithmic bias in Policing and justice.

Our Work

We are particularly interested in human security behaviours in context – understanding the underlying reasons for the lack of cyber security behaviours and how behaviour change can be motivated.

Research in the **panacearesearch.eu** project is exploring the cyber security behaviours of healthcare workers. The team is designing a toolkit to help hospitals and other facilities explore current behaviours and underlying reasons for such behaviours, to identify ways to motivate people to behave more securely.

Research in the EPSRC project **cSalsa** looks at cyber security behaviours at different life stages, including new cyber vulnerabilities triggered by the retirement transition.

The **CyberGuardian** project has looked at how we can develop peer support to improve the cyber defences of older adults.

One aspect of cyber security is to manage privacy concerns which particularly affect those from vulnerable or stigmatised groups. As more data is collected online about individuals, their 'data shadow' shapes decisions by the justice system. The fear of such data collection may lead to self-censorship for some who fear stigmatisation. Such issues are covered by our EPSRC **intuitproject.org** project.

Fake news and misinformation are increasingly issues that security teams are expected to address. Both technology and people have a role to play in reducing their spread and impact, but when it comes to deep fakes that people will have more difficulty detecting, the need for authenticity of multimedia content to be recognised by technology is paramount. Our work addresses this problem from both the technical and human perspectives.

Our research on bio-inspired machine learning is achieving excellent results with our bio-inspired, flow-based and intelligent Botnet Detection System achieving an average detection accuracy of 99.8% across bot datasets, with a false positive rate of 0%. We are working on the Temporal forensic analysis of digital camera sensor imperfections for picture dating.
This project seeks to establish, for any given digital camera, a model that allows the analyst to estimate the acquisition date of digital pictures.

We involve our students in our research, and the application of that research, running a Cyber Clinic where cyber security students learn ethical hacking and pen testing using Kali Linux. The objective is to connect trained students to industry. We currently work with The North East Business Resilience Centre, which employs some of our Cyber Clinic students as part-time Cybersecurity consultants, and seven Police Forces.

Key areas of expertise and specialism

- Human, Organisational and Regulatory Aspects
- Network Security
- Authentication, Authorisation and Accountability
- Human Centred Security, Privacy and Trust
- Human Factors
- Digital and Multimedia forensics
- Network security and malware detection (CHANGE FROM: network security)
- Steganography

University of Oxford

Oxford University Cyber Security Network

Who we are

The 16 academics in the Oxford ACE-CSR form the hub for the wider cyber security research network in Oxford (over 300 people in 26 administrative units across the University). Research activities encompass the themes of: secure systems and technology; verification and assurance; operational risk and analytics; identity, behaviour and ethics; national and international security and governance; and human aspects of cyber security.

We have particular expertise in bringing different disciplines together, with collaborations spanning the Business School, Sociology, Politics and International Relations, Computer Science, Engineering, Maths and Medical Sciences. We are also driving development of a community of practice for research ethics for cyber security and data-driven research.

What we do

The breadth of our work allows the University to create impact in numerous areas, including the theory of security protocols and their automated analysis, applied cryptography, and steganography, the security of systems, particularly the technical and human factors contributing to trust and security in distributed contexts (including mobile and cloud systems), wireless security, network operations, situational awareness and security, insider threat detection, ad hoc collaboration, privacy and governance, trusted computing, and operations management.

Our researchers have played a key role in the development of the Responsible Research and Innovation field, looking at topics ranging from trust in autonomous robots, to helping individuals make more informed security and privacy decisions. The network also draws on wider expertise in software engineering and verification, quantum computing, management of large datasets and compute resources, medical informatics and privacy, modelling and understanding of risk, and programming language design.

Our Work

In order to solve cyber security problems, we need strong technology combined with an understanding of the context in which it is used, and how people will relate to one another through it. Our research interests find application in areas such as smart power grids, sensor networks, fraud detection, secure web applications, sensor networks, personalised medicine, home networking and services, sustainable ICT, and security standards. Integration across divisions and departments – and beyond the University – have led to projects looking at cyber risk and insurance, software and cloud supply chains, understanding how criminals collaborate online, and a founding membership of the UK's national PETRAS IoT hub.

Oxford hosts a Centre for Doctoral Training in Cyber Security, training students in the diverse disciplines which contribute to cyber security, and equipping them to make a lasting research contribution in this cross-disciplinary area. The Global Cyber Security Capacity Centre, founded in 2014, sets out to understand how to deliver effective cyber security within the UK and internationally. By collating best practice stories and case studies, it has developed the Cybersecurity Capacity Maturity Model for Nations (CMM) for improving capacity across the areas of policy, risk management, society and culture, legal frameworks, workforce skills, and security controls. Working with key stakeholders from across the international community, the Centre and its partners such as the World Bank, the Organization of American States, the International Telecommunication Union, the Commonwealth Telecommunications Organisation and the Global Forum in Cyber Expertise, have successfully applied the CMM more than 110 times to over 80 countries.

The Department of Computer Science runs a highly successful Master's programme, including an NCSC-certified MSc in Software and Systems Security. Together, the Professional Programmes for software engineering recruit around 90 students each year to study part-time, whilst retaining professional roles in high technology companies and government departments. This is a crucial aspect of our technology transfer work, and is one of the means by which we develop long-term relationships with external partners for mutual benefit.

Key areas of expertise and specialism

- Analysis and verification of software and security protocols
- Systems security; trustworthiness and usability
- Inter-disciplinary cyber security, policy and governance

ECIT THE INSTITUTE OF ELECTRONICS, COMMUNICATIONS AND INFORMATION TECHNOLOGY
INCORPORATING
CSIT
CWI
DSSC

Queen's University Belfast

CSIT – The Centre for Secure Information Technologies

Who we are

The Centre for Secure Information Technologies (CSIT) is the national Innovation & Knowledge Centre (IKC) for cyber security research. CSIT was awarded a Queen's Anniversary Prize for Higher and Further Education in 2015. Originally established in 2009, the Centre's significant achievements over its initial five-year period have also been recognised by core funders. The EPSRC, Innovate UK and Invest Northern Ireland have confirmed follow-on funding totalling £10.5 million, whilst the University has committed a further £9 million, to sustain CSIT as an IKC and help it raise the bar on translating its world leading research into commercial impact right up to 2022.

We employ over 80 people and have world leading research expertise in areas such as network security, video analytics, cryptography, security informatics, SCADA security, malware detection and embedded security.

Professor Máire O'Neill is Principal Investigator and Dr. Godfrey Gaston is CSIT Director with overall responsibility for the Centre.

What we do

Uniquely for a university, industry experienced engineers and business development people work alongside CSIT academics, researchers and PhD students to facilitate a culture of innovation that is industry focused and measured on economic impact and commercial exploitation.

Operating an Open Innovation model to drive collaboration with member organisations, we carry out contract research, license intellectual property, spin-out companies and have a membership programme where industry can invest in the vision of CSIT and join in developing the research strategy that has the overarching theme of 'secure connected intelligence'.

CSIT is engaged in a number of cyber security collaborative research projects with world leading organisations including Allstate, BAE Systems, Citi, EBay, First Derivatives, Seagate, Thales, numerous SMEs, spin-out ventures (Titan IC Systems (Acquired by NVIDIA in March 2020), Liopa, Ditaca Ltd.) and leading institutes in the USA, South Korea, Japan, India and Europe. CSIT representatives are members of the UK National delegation to the security standardisation Study Group 17 of the International Telecommunication Union (ITU), the UK's Multi-stakeholder Advisory Group on Cyber issues (FCDO), ETSI, the UK AI Council, the Association for Computing Machinery's (ACM) global technology policy council and the Open Network Operating System (ONOS) Security & performance analysis brigade.

Our Work

CSIT has delivered, is co-ordinating and is involved in numerous projects, including:

Research Institute in Secure Hardware and Embedded Systems (RISE) – Led by Professor Máire O'Neill and supported by a staff team based in the CSIT IKC, RISE has achieved broad support from the UK academic community (seven UK universities are now funded via RISE) and has been very successful in engaging industrial partners from major hardware OEMs and technology companies.

SPRITE+ (Security, Privacy, Identity, and Trust Engagement – A NetworkPlus that will deliver a step change in engagement between people involved in research, practice, and policy relevant to trust, identity, privacy, and security (TIPS) with a focus on digital contexts. SPRITE+ will deliver a coherent, coordinated, multi-disciplinary approach, with strong stakeholder relationships at the centre. Professor Sakir Sezer is a Co-Investigator of the network and several CSIT academics participate as Expert Fellows.

COSMIC - Cloud-enabled Operation, Security Monitoring, and Forensics is a current project running in the Research Institute in Trustworthy Interconnected Cyber-physical Systems (RITICS). COSMIC investigates approaches for the seamless and secure transition of legacy-critical industrial control systems to the cloud with improved security, resilience, and failover protection, while also enabling new opportunities to enhance intrusion response and post-event forensics. This work is led by Professor Sakir Sezer and has precipitated CSIT's latest spin-out company Ditaca Ltd.

DCMS – Advisory work on the UK Cyber Security Sectoral Analysis and Understanding the UK cyber security skills labour market projects in 2018, 2020 and beyond.

Innovation programmes delivered to over 100 companies, namely London Office for Rapid Cyber Advancement (LORCA) – the cyber security accelerator programme funded by the Department for Digital, Culture, Media & Sport (DCMS) and delivered by Plexal, Deloitte and CSIT. HutZero – a pre-accelerator programme that seeks to encourage early stage entrepreneurs and wantrepreneurs and generate cyber start-up ideas. Cyber101 – CSIT is a delivery partner on the DCMS funded Cyber Security SME 'Cyber 101' programme. Led by Digital Catapult, Cyber 101 aims to provide workshops on business basics to early-stage cyber security companies across the UK.

CSIT has also delivered industry contract research and development covering malware reverse engineering, Zero Day attacks, vulnerability analysis, fraud detection, network processing hardware design, driver condition detection and driver authentication, crypto implementations and hardware security.

Key areas of expertise and specialism
- Secure hardware and embedded systems
- Post-quantum cryptography and advanced cryptography architectures
- Security Intelligence - AI for cyber security and mobile security
- Networked security systems
- Analytics-based monitoring & forensics in new network architectures
- Industrial Control Systems and Operational Technology security
- Cyber security research translation, innovation, commercialisation and policy advisory

Royal Holloway, University of London

Information Security Group

Who we are

Most of the research in information security at Royal Holloway is undertaken by members of the Information Security Group (ISG), which is one of the world's largest research groups working in information security.

The ISG is one of the oldest groups of its type, having worked on cryptography since the mid-1980s. Royal Holloway was the first institution in the world to offer a degree in information security in 1992. There are now over 4,000 alumni of the course from over 100 countries, many working in senior information security roles in government and industry.

The ISG is a department within the School of Engineering, Physical and Mathematical Sciences. We employ 20 full-time permanent members of staff. We also employ five post-doctoral research assistants, working on a wide range of funded projects. The ISG currently has around 80 PhD students and hosts one of three doctoral training centres for cyber security, funded by EPSRC.

The activities of the ISG are supplemented by research undertaken by colleagues in the Mathematics and Computer Science departments in particular. Our research in information security has been enriched by the recruitment of students with backgrounds in the social sciences and has led to a fruitful collaborations across other schools and departments including Geography, Business and Management, Economics, Electronic Engineering, Law/Criminology, Politics and International Relations, and Psychology.

What we do

The ISG addresses and collaborates across a broad range of areas, from the social, definitional, complexity-theoretic and mathematical foundations of information security, to attacks and efficient implementations to applications and policy. Areas include cryptography, social science, software & system security, malware analysis, network security, automotive security, cyber-physical systems, drone security, the economics of information security, embedded systems, digital forensics, psychological aspects of information security, resource-constrained security, security testing, security standardisation, threat analysis, trusted execution environments, trustworthy autonomous systems, ubiquitous computing and web security.

The area of cryptography has historically been and remains a core strength of the ISG. Cryptographic research within the ISG is focused on cryptanalysis and cryptographic primitives. Areas of cryptographic research include lattice-based and post-quantum cryptography, cryptographic protocols, statistics, access control, hardware implementations of cryptography and information-theoretic security.

Researchers in the ISG pioneer the use of qualitative social science methods such as creative methods of engagements and ethnography in information security. The research is focused on the security needs of under-served and unvoiced communities and groups.

The area of software & systems security is a focus for several members of staff. Key areas include intrusion/anomaly detection and malware mitigation, mobile security, execution integrity verification, secure enclaves and systems engineering.

The area of trustworthy autonomous systems and smart emerging technologies for financial, telecommunications and autonomous vehicular security is a focus. Key areas of expertise include integrated and resource-constrained devices, explainable artificial intelligence, self-testing/validating, digital forensics, cyber physical systems and micro architectural attacks for trusted execution environments.

Our Work

The ISG provides advisory and research services on information security and associated topics, drawing on the expertise of its research staff and, as appropriate, a network of trusted professional associate consultants and external researchers. ISG members have advised over 100 organisations worldwide, including trade unions, activist networks, multinational corporations, government departments, trade and standards associations and SMEs. In 2019 we were founding members of the International Cyber Security Centre of Excellence (INCE-CoE).

Some of our current projects include:

- **Lattice-based cryptography for post-quantum applications** – The ISG is involved in several candidate proposals for the ongoing NIST Post-Quantum Standardisation Process and in analysing the security of such schemes (EPSRC and EU H2020 funded).
- **Lattice-based cryptography for advanced privacy-preserving techniques** – The ISG is involved in efforts to standardise schemes for computing on encrypted data and advises on the security of such schemes. It is also involved in building and analysing other advanced cryptographic primitives that remain secure in a post-quantum world and against even nation-state level adversaries (EU H2020 funded).
- **Post-quantum TPM** – We are involved in an effort to make secure attestation of system state post-quantum secure (EU H2020 funded).
- **Post-quantum and quantum joint protocols** – We are involved in a consortium building joint protocols relying on both post-quantum cryptography and quantum key distribution (InnovateUK funded).
- **Digital forensics** – We are involved in a project with law-enforcement agencies to develop techniques for enhancing the forensic extraction of information from modern encrypted smartphones (EU H2020 funded).
- **Everyday security** – We are working on making services used in the everyday safer, working closely together with communities and other stakeholders (EPSRC funded).
- **Doctoral training** – We host the EPSRC Centre for Doctoral Training in Cyber Security for the Everyday at Royal Holloway.

Key areas of expertise and specialism
- Cryptography
- Social aspects of information security
- Software and systems security
- Trustworthy autonomous systems

University of Southampton

CyberSecurity Southampton

Who we are

The University of Southampton Cyber Research Group aspires to lead the academic agenda towards a secure cyberspace. Our multidisciplinary expertise contributes understanding, knowledge and innovation to the protection of critical infrastructures, users, their data and interests. Our activities connect across electronic, software, hardware, IoT and cyber-physical systems, data analytics and AI for security, data assurance and blockchain, advanced networking and protocol security, situational awareness, cyber risk and threat analysis, cybercrime, social acceptability of cyber regulations, and related education.

Led by Professor Vladimiro Sassone, the centre includes researchers from Computer Science, Engineering, Law, Management, Mathematics, NanoElectronics, Psychology, Sociology and Web Science. This places us in a unique position to respond to the need for UK Government, business and consumers and their infrastructures to become more resilient to cyber attacks.

The Cyber Research Group delivers a wide spectrum of interwoven research, ranging from electronic devices to social and legal aspects, passing through world-leading research on cyber-enabling infrastructures, addressing core cyber security issues through formal and experimental methods.

What we do

Our current research and activities include:

- Supplying secure embedded, IoT, and cyber-physical systems and their design methodologies via integrated hardware software co-design, tool-based approaches.
- Securing the cyberspace by design, analysis, simulation and proof, to protect infrastructures and data, users and their interests.
- Enhancing the security and trustworthiness of computer hardware.
- Developing AI, deep and reinforcement learning based advanced data analytics for cyber attack detection and defence at the software, hardware, and system level.
- Supporting policy and strategy makers, government, industry and society at large to enhance the national and international cyber security capacity.
- Forming partnerships with industry, government agencies, and local communities in order to further our institutional mission more effectively.
- Adopting a holistic and multidisciplinary approach, which takes into full account human aspects and behaviour, as well as social and legal acceptability issues.

- Fostering excellence in research, depth in impact, and educating top-class cyber security experts.

Our Work

We engage in externally funded, high-quality research and outreach activities with NCSC/GCHQ, FCO, NCA, Bank of England, the Cabinet Office, the Metropolitan and Hampshire Police forces, and other public administrations across the world. Our partnership with government agencies and industry leaders include Dstl, Northrop-Grumman, Roke Manor Research, and the South East Regional Cyber Crime Unit (SEROCU). Together with these partners, we founded and operate a Cyber Security Academy, whose objectives span from research and consultancy to outreach, training and knowledge transfer. Furthermore, we are part of the SPRITE+ consortium, the EPSRC's national Trust, Identity, Privacy and Security NetworkPlus, where our specific responsibilities include leading on the development of cyber security training.

Professor Sassone holds a Royal Academy of Engineering Research Chair in Cyber Security and was scientific leader of H2020 project SUNFISH on federating clouds, whose partners include the UK and the Italian governments. Professor Sassone also held grants BlockIT and CS-SED, focusing on the application of blockchain technologies to data privacy and assurance in smart-energy applications, devices and data.

Professors Surridge and Sassone secured the H2020 project CyberKit4SMEs, aimed at developing a toolkit to help SMEs improve their cyber stance. Part of the ideas here arose from Surridge and Sassone's previous work on Cyber Essentials in project CSCE.

Dr. Aniello and Professor Sassone secured two Defence Accelerator projects from the MoD, CyPrIAAAn and OCCAM-RT, focusing on developing predictive cyber analytics and situational awareness against multi-stage cyber attacks.

Dr. Halak secured two fellowships from the Royal Academy of Engineering, focusing on securing hardware supply-chain and on developing AI-based countermeasures to device tampering.

Professors Butler and Sassone and Dr. Aniello secured the EPSRC grant HD-Sec to work on security verification of capability hardware. Professor Butler's previous project aims to develop a unified tool-based framework for automated formal verification and validation of cyber-physical systems.

Dr. Karafili was awarded the prestigious Marie Curie Individual Fellowship funded by EU H2020 program for her project AF-Cyber (Logic-Based Attribution and Forensics in Cyber Security), and is part of the CyberASAP (Cyber Security Academic Startup Accelerator Programme) funded by DCMS with Innovate UK & KTN.

Key areas of expertise and specialism

- AI and ML based data analytics for cyberattack detection and defence, and malware analysis;
- Analysis and design of trustworthy software;
- Blockchain and Distributed Ledgers;
- Cyber identity;
- Cyber risk analysis;
- Data privacy;
- International cyber law;
- Provenance, trust and data assurance
- Safety-and-Security by Design;
- Secure embedded systems;
- Secure web technologies;
- Security of cyber-physical systems and the Internet of Things;
- Security of Critical Infrastructures, transport networks, automotive systems, and smart energy systems (smart home, smart building, smart grid, etc).

University of Surrey

Surrey Centre for Cyber Security

Who we are

Surrey Centre for Cyber Security (SCCS) brings together teams focused on innovative research in cyber security across the University of Surrey. Established in 2014, we currently have 17 core academics with established track records in key technical areas of cyber security. Our broader activity encompasses a further 25 associate members with interdisciplinary expertise in AI, Communication Systems, Engineering, Psychology, Criminology, Business and Law. We have strong links with Surrey's 5G Innovation Centre, Surrey Space Centre, and the Centre for Vision, Speech and Signal Processing.

SCCS research and PhD projects are supported by various funding bodies including EPSRC, EU, InnovateUK and industry, and including our Centre for Doctoral Training in Future Connected Technologies, supported by EIT Digital and industrial partners. We also offer an Information Security MSc programme which was certified by the NCSC in 2014. In 2019 a modern 200-seat laboratory was built to support our practical research and teaching activities.

What we do

SCCS research is concerned with technical foundations of cyber security, the design and development of cyber security technologies and their applications to real-world systems.

We are internationally known for our work in applied cryptography, security verification and distributed systems, with strong backing in trusted computing and networks.

Our research focuses on the design of secure and resilient technologies. Applications are in many domains, including electronic transactions and digital identity, electronic voting, smart ticketing and transportation, and future communications and networks.

We collaborate with leading international groups for research, training and networking. Current collaborations include leading universities and research institutes in Australia, India, Israel, USA and Europe.

We maintain strategic research collaborations and projects with key industry players in cyber security technologies and their applications. Partnerships include Amazon, ARM, BT, Facebook/Novi, Galois, HP Labs, IBM Research, IOTA, MasterCard, Mozilla, NCC Group, Nomadic Labs, Saab, Stellar Development Foundation, Tendermint, Thales, VISA, Vodafone, and Yubico.

Members of SCCS are active members of ETSI, ISO SC27, Trusted Computing Group, FIDO Alliance and LORA Alliance.

Our Work

Applied cryptography – Liqun Chen works on anonymous attestation and post-quantum cryptography and is internationally known for her work on applied cryptography. Robert Granger and David Gerault work on cryptanalysis. Mark Manulis works on privacy-oriented cryptography and on authentication protocols. Other protocols work includes distance bounding and contactless payments (David Gerault and Ioana Boureanu) and anonymous smart-ticketing (Helen Treharne). Blockchain and distributed ledgers – Gregory Chockler works on Byzantine agreement and foundations for secure data replication in permissioned distributed ledgers. Steve Schneider, Mark Manulis and John Collomosse work on DLT applications to digital identity, archiving, information brokering and electronic voting.

Communications and networks – Ioana Boureanu and Helen Treharne work on LoRaWAN protocols. Haitham Cruickshank works on security and routing in heterogeneous networks including 5G. Mark Manulis works on communications in fleets of consumer drones, and on secure satellite ranging and cyber security in new space. Helen Treharne works on train-to-cloud communications and Zhili Sun works on reliable satellite communications.

Distributed systems – Gregory Chockler leads research on foundations and applications of trustworthy distributed computing, fault-tolerance, scalable data storage, and cloud computing. Brijesh Dongol works on inter-process communications and applications to robotic systems. Lee Gillam works on cloud resilience, security and performance. Nishanth Sastry develops systems and architectures around mobile edge computing.

Formal Modelling and Verification – Ioana Boureanu works in formal security analysis, provable security, and formal verification via model-checking. Taolue Chen works on verification through probabilistic model-checking. Santanu Dash works in secure software, malware detection and software engineering. Brijesh Dongol applies formal techniques to concurrent objects and weak memory models for transactional memory. Constantin Catalin Dragan works on provable security and verification using Easycrypt. Steve Schneider works on model-checking and theorem-proving approaches. Helen Treharne works on formal verification of protocols such as V2X using Tamarin.

Trusted systems – Ioana Boureanu works on hardware roots of trust for combatting proximity frauds. Liqun Chen leads the H2020 FutureTPM project exploring next generation TPM-based solutions incorporating robust and formally verified quantum-resistance cryptographic primitives. Steve Schneider leads research on verifiable electronic voting. Helen Treharne and Mark Manulis work on cloud architectures for password-less authentication.

Social media – Nishanth Sastry leads research on the production, distribution and consumption of online content in social media, for example focusing on patterns aiming to detect and understand harmful contents

In addition to the above, some socio-technical aspects of cyber security at Surrey include Mikołaj Barczentewicz's (Surrey Law and Technology Hub) work on law and policy solutions to problems of data security and privacy, and Mike McGuire's work on criminology, cybercrime, and technology in the justice system.

Key areas of expertise and specialism

- Applied Cryptography
- Formal Modelling and Verification
- Authentication, Authorisation and Accountability
- Privacy Enhancing Technologies
- Network Security
- Distributed Systems

University College London

Computer Science Department

Who we are

University College London's (UCL) ACE-CSR includes 24 academics across six research groups within the Computer Science Department including Information Security Research Group, Science of Cyber Security Research Institute, Systems and Networking Research Group, Software System Engineering Research Group, Jill Dando Institute of Security and Crime Science, and Department of Science, Technology, Engineering and Public Policy.

Cyber security research is one of UCL's strategic research priorities and the Centre of Excellence aims to help make the UK Government, business, and consumers more resilient to cyber-attacks by extending knowledge and enhancing skills in cyber security. In particular, our mission is to:

- Encourage collaboration and expand the level of innovation
- Enhance the UK's cyber knowledge base through original research
- Provide top quality graduates in the field of cyber security
- Support NCSC's cyber defence mission

What we do

The ACE-CSR conducts a broad range of research in cyber security and in conjunction with the Department of Security and Crime Science works on understanding cyber safety and preventing cybercrime. UCL is educating future cyber security professionals through its MSc and PhD programmes. The MSc in Information Security is a one-year programme where international security experts teach a balance of established theory and cutting-edge practice, equipping graduates with the broad expertise necessary to succeed in information security.

Our Work

We research and solve real-life problems across a broad range of areas. A few illustrative examples include the ELVEN project, the work at the Dawes Centre for Future Crime and PETRAS, as well as our Centre for Doctoral Training in Cybersecurity.

Robust software is resistant to "meddling". It possesses a form of correctness attraction that allows it to continue to produce its intended responses in spite of transient errors or adversarial efforts to affect it. The ELVEN project, funded by Facebook, is investigating the role that entropy loss via program execution plays in robust code. ELVEN is using program analysis to map entropy loss regions in software and relate this to robustness behaviour. The longer-term aim is to automate the addition of robustness to programs and hardware designs.

Another project we led aimed to better understand the potential crime threats associated with consumer IoT devices, understand what is communicated to consumers about security prior to their purchase, examine the factors that consumers care about, and estimate what effect labels, that communicate details of device security, might have on consumer choice. A market surveillance exercise with 270 devices, which involved a review of the materials that were available prior to purchase, revealed that none provided details of the duration over which security updates would be provided, only 10% provided advice on cyber hygiene, and only 5% detailed the security of the cloud services used. A systematic review of the academic literature revealed that crime threats associated with the consumer IoT included burglary, stalking, identity theft and online sex offending. Our studies on consumer choice indicated that consumers would be willing to pay more for secure devices, and that some security labels would be more effective than others. This work informed DCMS's Secure by Design agenda.

Last but not least, our Centre for Doctoral Training (CDT) in Cybersecurity, opened in 2019, is an innovative and exciting collaboration bringing together research teams in three UCL departments, to increase the capacity of the UK to respond to future information and cyber security challenges. Through an interdisciplinary approach, the CDT trains cohorts of highly skilled experts drawn from across the spectrum of Engineering and Social Sciences, to become the next generation of UK leaders in industry and government, public policy, and scientific research. The CDT equips the students with a broad understanding of all sub-fields of cybersecurity, as well as specialised knowledge and transferable skills to be able to operate professionally in business, academic, and policy circles. Overall, the CDT has an ambitious portfolio of projects and over 40 members of faculty with internationally excellent expertise across all aspects of cybersecurity.

Key areas of expertise and specialism

- Anonymous communications
- Cryptocurrencies and blockchains
- Cryptography and cryptanalysis
- Cyber safety
- Economics of security
- Ethical, legal and policy aspects of security
- Network security
- Privacy-enhancing technologies
- Program verification and analysis
- Security and privacy in Artificial Intelligence
- Security in ubiquitous computing
- Software and systems security

University of Warwick

Cyber Security Global Research Priority

Who we are

The University has a long history of undertaking research in what now falls under the umbrella of cyber security. Today, cyber security at the University spans many departments and is coordinated through the Cyber Security Global Research Priority (GRP).

The University's GRP programme provides a platform for multidisciplinary research in key areas of international significance, encouraging cross-departmental collaboration and enabling our researchers to work together across departmental and disciplinary boundaries on issues of global importance. The ACE-CSR brings world-renowned academics from many disciplines together to address a broad range of cyber security challenges.

Our aim is to be a world-leading, single-institution, multidisciplinary research group for cyber security and to create new knowledge and understanding that will improve cyber security through active partnership with key stakeholders, and have national and international impact.

What we do

Human, Organisational & Regulatory Aspects: A significant proportion of our work lies in this area of the Cyber Security Body of Knowledge (CyBOK). Our work on Privacy and Online Rights spans technological developments, implementation and governance. Our work on Privacy Enhancing technologies (PETs) is supported by NCSC funding for a doctoral studentship and summer internship programme over the past three years and grants including a Royal Society Wolfson Research Merit Award held by Professor Graham Cormode. Professor Carsten Maple is a PI on the Trustworthy National Digital Identity Systems project funded by the Bill and Melinda Gates Foundation, which involves developing privacy-enhancing techniques for national digital identity systems. Following successful foundational EPSRC projects, Professor Irene Ng is seeing her work from the Hub-of-All-Things, DROPS and Contrive projects being implemented through the global start-up Dataswift. The work of Sorell and Aldrich covers the transparency, ethics, and democratic values of privacy, secrecy and security. Dr. Matt Spencer is the recipient of an EPSRC Future Leaders Fellowship and is currently investigating the social processes through which knowledge and trust are negotiated in the security profession through the Scaling Trust project.

Systems Security: Our work in Systems Security includes a large number of projects in Authentication, Authorisation & Accountability. Professor Feng Hao was awarded an EPSRC grant in April 2020 on End to End Authentication of Caller ID in Heterogeneous Telephony Systems. Our portfolio of work on authentication, access control and identity management includes Authentication and Access Control in IoT Systems and Pattern of Life Analytics for Authentication. Professor Chang-Tsun Li recently completed the IDENTITY project for Computer Vision Enabled Multimedia Forensics and People Identification and is taking this work forward with Dr. Victor Sanchez-Silva and Professor Maple through the Real-time Detection of Concealment of Intent for Passenger Screening project.

Infrastructure Security: The University has considerable expertise in securing infrastructure through a range of applications. This includes our work on Resilient IoT at the Edge, a project which aims to collect good design patterns, taking advantage of existing National Cyber Security Centre (NCSC) secure design patterns and build on related Warwick research in resilient architectures for cyber security. Building upon ground-breaking implementation of secure and private communications in vehicular communications, the University is part of a consortium delivering the £8 million project, AirQKD. This project, led by BT, will develop and implement quantum key distribution in connected and autonomous vehicle systems.

Our Work

The ACE-CSR attracts funding from a variety of sources, reflecting the importance of cyber security research to a number of stakeholders, gaining funding for more than 100 projects in the past four years. We also receive substantial funding from commercial partners. For example, in 2018, the National Automotive Innovation Centre opened on the University of Warwick campus. The Centre, which is a beacon for automotive research bringing together the brightest minds from industry and academia, to develop future vehicles and mobility solutions, is a £150 million investment between Jaguar Land Rover, Tata Motors, WMG and the University of Warwick, with an additional £29.5m funding from the UK Research Partnership Investment Fund (UKRPIF), through Research England.

The University is a founding core partner of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity. There have also been numerous projects undertaken at the University funded through PETRAS, including Evaluating Trustworthiness of Edge-Based Multi-Tenanted IoT Devices (TEAM), led by Dr. Arshad Jhumka. TEAM is developing a framework that will enable the deployment of trusted edge-based multi-tenanted IoT networks where applications are of varying criticality.

The University is also a founding partner in the Alan Turing Institute and undertakes a range of work in this regard. The work is conducted through Turing's Defence and Security programme and includes the work of Professors Rob Proctor and James Smith on Bayesian predictive models of violent extremist threat building upon Smith's Chain Event graphs work that has been widely applied to criminal activity. Within the programme, Dr. Fahmy is undertaking leading work in hardware accelerated data analytics.

Key areas of expertise and specialism

- Privacy and Online Rights
- Cyber-physical systems security
- Authentication, Authorisation & Accountability
- Risk Management and Governance
- Distributed Systems Security
- Physical Layer Security and Telecommunications

Contact Address Book

University of Birmingham

Professor Mark Ryan,
Director, School of Computer Science
ace-csr@cs.bham.ac.uk
+44 (0) 121 414 7361

University of Birmingham,
Edgbaston,
Birmingham,
B15 2TT

sec.cs.bham.ac.uk

University of Bristol

Dr. Daniel Page,
csdsp@bristol.ac.uk

Professor Awais Rashid,
bcsg-enquiries@bristol.ac.uk

University of Bristol,
Department of Computer Science,
Merchant Venturers Building,
Woodland Road,
Bristol,
BS8 1UB

University of Cambridge

Professor Frank Stajano,
Head, ACE-CSR;
Fellow, Trinity College;
Professor of Security and Privacy,
frank.stajano@cl.cam.ac.uk
+44 (0) 1223 763 500

University of Cambridge,
Department of Computer Science and Technology
(The Computer Laboratory),
William Gates Building,
15 JJ Thomson Avenue,
Cambridge,
CB3 0FD.

http://www.cl.cam.ac.uk/projects/ace-csr/

Cardiff University

Professor Pete Burnap,
Director,
Centre for Cyber Security Research,
burnapp@cardiff.ac.uk

Cardiff University,
Cardiff CF10 3AT

https://www.cardiff.ac.uk/centre-for-cyber-security-research

De Montford University

Professor Eerke Boiten,
Director, Cyber Technology Institute,
eerke.boiten@dmu.ac.uk

School of Computer Science
and Informatics,
De Montfort University,
Leicester
LE1 9BH

www.dmu.ac.uk/cti/

The University of Edinburgh

Professor David Aspinall,
Director
David.Aspinall@ed.ac.uk
+44 (0)131 650 5177

Dr. Vesselin Velichkov,
Deputy Director
vvelichk@ed.ac.uk
+44 (0)131 650 2697

Dr. Ahmed El-Rayis,
Commercial Director
A.El-Rayis@ed.ac.uk
+44 (0)773 651 4165

The University of Edinburgh
https://www.ed.ac.uk/cyber-security-privacy/

Imperial College London

Professor Emil C Lupu,
Security Science Fellow
Institute for Security Science and Technology,
securityscience@imperial.ac.uk

Imperial College London South
Kensington Campus
London,
SW7 2AZ

https://www.imperial.ac.uk/cyber-security/

University of Kent

Professor Shujun Li
Director of KirCCS and PI for the Kent
ACE-CSR

Professor Gareth Howells and Professor Julio Hernandez-Castro
Deputy Directors of KirCCS
School of Computing,
University of Kent
Canterbury,
CT2 7NF

kirccs-public@kent.ac.uk
https://cyber.kent.ac.uk/

King’s College London

Dr. Jose Such,
Director,
KCL Cybersecurity Centre,
Department of Informatics,
cybersec-info@kcl.ac.uk

King’s College London,
Bush House,
30 Aldwych,
London,
WC2B 4BG

http://kcl.ac.uk/cybersecurity-centre

Lancaster University

Professor Nicholas Race,
Director,
Cyber Security Research Centre,
Infolab21,
cybersecurityresearch@lancaster.ac.uk

Lancaster University,
Lancaster,
LA1 4WA,

https://www.lancaster.ac.uk/cybersecurity

Newcastle University

Dr. Thomas Gross,
Reader of Systems Security,
PI and Director for ACE-CSR,
Academic Centre of Excellence in
Cyber Security Research,
thomas.gross@newcastle.ac.uk
+44 (0) 191 208 7997

Newcastle University,
Urban Sciences Building,
1 Science Square,
Newcastle upon Tyne,
NE4 5TG

Northumbria University

Professor Lynne Coventry,
Department of Psychology,
University of Northumbria,
Lynne.coventry@northumbria.ac.uk
+44 (0) 191 243 7772

Newcastle upon Tyne,
NE1 8ST

https://www.northumbria.ac.uk/about-us/academic-departments/computer-and-information-sciences/research/northumbria-cyber-security-research-group/

University of Oxford

Professor Andrew Martin,
Professor of Systems Security PI for
ACE-CSR and Director of the CDT in
Cyber Security,
andrew.martin@cs.ox.ac.uk

Katherine Fletcher,
Coordinator,
Cyber Security Oxford network
enquiries@cybersecurity.ox.ac.uk

University of Oxford
Department of Computer Science,
Wolfson Building,
Parks Road
OXFORD
OX1 3QD

www.cybersecurity.ox.ac.uk

Queen’s University Belfast

David Crozier,
Head of Strategic Partnerships,
Centre for Secure Information Technologies,
ECIT Institute,
info@ecit.qub.ac.uk
+44 (0) 28 9097 1700

Queen’s University Belfast,
Queen’s Road,
Queen’s Island,
Belfast,
BT3 9DT

www.qub.ac.uk/csit

Royal Holloway University

Professor Peter Komisarczuk,
Information Security Group,
Royal Holloway University of London,
Peter.Komisarczuk@rhul.ac.uk

Egham Hill,
Egham,
TW20 0EX

https://www.royalholloway.ac.uk/isg

University of Southampton

Professor Vladimiro Sassone,
Director,
Cyber Security Research Centre,
vsassone@soton.ac.uk
+44 (0)2380 599009

University of Southampton,
Southampton,
SO17 1BJ

https://cyber.southampton.ac.uk
facebook and twitter @CybSecSoton

University of Surrey

Professor Steve Schneider,
Surrey Centre for Cyber Security,
University of Surrey,
s.schneider@surrey.ac.uk
+44 (0) 1483 68 9637

Guildford,
GU2 7XH

www.surrey.ac.uk/sccs
Twitter: @SCCS_UniSurrey

University College London

Professor Emiliano De Cristofaro,
Director,
Academic Centre of Excellence in
Cyber Security Research University
College London,
Department of Computer Science,
decristofaro@ucl.ac.uk

Gower Street,
London,
WC1E 6BT

https://www.ucl.ac.uk/cybersecurity-centre-of-excellence/

Warwick University

Professor Carsten Maple,
Professor of Cyber Systems
Engineering,
cm@warwick.ac.uk
+44 (0) 24 7652 4348

University of Warwick,
Coventry,
CV4 7AL

https://warwick.ac.uk/research/priorities/cyber-security/

Glossary of terms

5G	5th generation mobile network
6G	6th generation mobile network
ACD	Active Cyber Defence
ACM	Association for Computing Machinery
AI	Artificial Intelligence
ACE-CSR	Academic Centre of Excellence in Cyber Security Research
CIISec	Chartered Institute of Information Security
CNI	Critical National Infrastructures
CPU	Central Processing Unit
CyBok	The Cyber Security Body of Knowledge
DCMS	Department for Digital, Culture, Media and Sport
DLT	Distributed ledger technology
Dstl	Defence Science and Technology Laboratory
EPSRC	Engineering and Physical Sciences Research Council
ERC	European Research Council
EU	European Union
FCDO	Foreign, Commonwealth and Development Office
GCHQ	UK Government Communications Headquarters
IACR	International Association of Cryptologic Research
IAG	Industrial Advisory Group
ICT	Information Communications Technology
IoT	Internet of Things
MoD	UK Ministry of Defence
MSc	Master of Science, a UK post-graduate qualification
NCA	National Crime Agency
NGO	Non-governmental Organisation
PACE	Privacy-Aware Cloud Ecosystems
PETs	Privacy-Enhancing Technologies
PhD	Post-graduate doctoral qualification available in the UK
RISCS	Research Institute for Sociotechnical Cyber Security
RISE	Research Institute in Secure Hardware and Embedded Systems
RITICS	Research Institute in Trustworthy Interconnected Cyber-physical Systems
UKRI	UK Research and Innovation

in association with
National Cyber
Security Centre

Engineering and
Physical Sciences
Research Council

Academic Centre of Excellence in **Cyber Security Research**

This publication is also available on our website at https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research

Any enquiries regarding this publication should be sent to us at enquiries@ncsc.gov.uk