# ANNUAL REPORT 2025/26

RISCS Research Institute for Sociotechnical Cyber Security

RISCS

# CONTENTS

# FOREWORD

As Blaise, Chief of SIS, set out in her speech on 15 December 2025, 'We are now operating in a space between peace and war' (https://www.gov.uk/government/speeches/speech-by-blaise-metreweli-chief-of-sis-15-december-2025).

This sense of uncertainty, but also of moment and the need to act, was echoed by Air Chief Marshal, Sir Richard Knighton, in the Chief of the Defence Staff's annual lecture at the Royal United Services Institute on the same day. The following month, former Chief Scientific Advisor for National Security and Defence, Prof. Sir Anthony Finkelstein, published his Call to Arms, urging universities to play a more prominent role in defence and security. We've welcomed the subsequent activity and commentary that has flowed from these pleas. RISCS has a prominent role to play here too.

An idea that has resonated so much with me recently is that science and technology 'does not merely support national security but increasingly determines it' (https://profserious.substack.com/p/a-simple-guide-to-national-security).

We can all see and relate to this, and that truth plays out both implicitly and explicitly in national strategies across the globe now. But, of course, it's not just about scientific wisdom and the rate of technological change; **it's the way people and societies interact with technology** that drives the pace of change, that unlocks the social and economic conditions to facilitate a paradigm shift in our capabilities. To just understand the technology is insufficient in cyber security and will ultimately lead to wasted effort and misaligned incentives. Being able to hold that systemic view, to look at the situation through a range of lenses with a rich and welcomed diversity of perspectives and expertise, is how we will move forward against the calls above. For me, that is where RISCS does and will continue to add unique value to our national security and defence priorities, as well as developing the pipeline of future talent and skills we need and the platform from which they can project.

We know it's not enough to have a sophisticated articulation of the problem – we also need to 'get stuff done' to keep up with our adversaries (whether they be a hundred 'duck-sized horses' or one, 'horse-sized duck': https://www.ncsc.gov.uk/news/ncsc-cto-the-tech-market-is-not-working).

As Pip, Technical Director for Social Science at NCSC, notes in her Foreword below, the line of sight you have kept on both storytelling and impact this year has been impressive. I urge us all to build on that in the coming year, to be bold and ambitious in what we can collectively achieve, but also to be deliberate in helping each other to carve out the routes to impact from our impressive multidisciplinary repertoire.

Thank you to the RISCS team and community for all your hard work towards keeping our nation safe online – it is truly world leading.

**Helen Lovekin**
***Head of the Office of the CTO, NCSC***

RISCS

The Research Institute for Sociotechnical Cyber Security (RISCS) is funded by the National Cyber Security Centre (NCSC) and hosted at the University of Bristol.

**RISCS is the UK's first academic Research Institute to focus on understanding the overall cyber security of organisations, including their constituent technologies, people, and processes.**

**RISCS takes an evidence-led and interdisciplinary approach to addressing these sociotechnical cyber security challenges.**

By providing a platform for the exchange of ideas, problems, and research solutions between academia, industry, and the policy community, RISCS promotes and supports world-leading, multidisciplinary, and scientifically robust research into sociotechnical approaches to cyber security.

# NCSC MESSAGE

This past year has been one of significant momentum for sociotechnical cyber security. For me personally, it's been a year of getting to know the RISCS team and the huge variety of topics they're covering, from adopting futures practices and creative thinking, to advising Government on Cyber Growth Strategies for the UK, all the way through to developing a conceptual and empirical basis for cyber statecraft at an international level. Against a backdrop of high-profile cyber attacks and global tensions, the research institute this year has focused on translating research into meaningful impact. I'm particularly excited to see the new RISCS Doctoral and RISCS–NCSC Impact Awards being introduced this year.

Among many achievements, several stand out as defining markers of our progress. Our researchers advanced foundational work in Principles Based Assurance, opening new pathways for successful implementation. We have begun our first implementation of the Capability Approach, with a trial commencing with Passkeys for Blind Individuals, expanding the real-world relevance of the approach. The Cyber Security Communities of support (CyCOS) Project has entered a pilot phase to investigate what works for small and medium sized companies, and to test out how peer relationships can support cyber resilience. We have also seen the completion of the Cyber Statecraft in an Age of Systemic Competition (CyCRAFT) project, which has seen a number of specialised workshops and Whitehall briefings on a vast array of topics linked to international cyber security. Additionally, through bringing in new Advisory Board members from UKRI and the Defence Science and Technology Laboratory (Dstl), we have broadened the reach and application of our research for public benefit.

None of this would have been possible without the dedication of the core RISCS team, Fellows, Advisory Board, and collaborators, and I take this opportunity to thank them for all their efforts. Their curiosity, integrity, and resilience continue to shape our institute's culture and sustain the quality of our work. I am equally proud of the internal developments we have made in NCSC this year – from how we ensure the research needs of our strategic programmes are met to preparing for the next phase of the Research Institutes.

Looking ahead, we are entering a year of opportunity. Our focus on excellence, collaboration, and societal impact will remain central to everything we do and I look forward to seeing what impact we can achieve.

I am pleased to share this annual report, which captures the breadth and depth of RISCS' achievements. A big thank you to everyone who has contributed this year.

**Pip B**
***Head of Social Sciences***
***and Internal Lead for RISCS, NCSC***

# DIRECTOR'S MESSAGE

As the fragile space between peace and war comes under increasing global pressures, military metaphors inevitably come to the fore in our conversations about cyber security. In this context it is unavoidable that we focus on security as a critical mode of frontline defence. But it is important to remember that 'security' promises us not only 'protection from …' but also 'freedom to …'. *Securus* as a Latin adjective literally means 'free from care': se- ('without') and *cura* ('care'). It implies a state of being carefree and calm, the freedom to prosper and to grow in a safe and protected environment.

The Romans famously gave us toilets and baths, wine and fast food, advertising and bureaucracy. Perhaps they also give us a way of conceptualising cyber security as a driver for peace and prosperity, even in a time of conflict.

Cyber Growth has certainly been high on the RISCS agenda this year. Two of our dynamic Advisory Board members, Ola Michalec and Simon Shiu, co-authored a major government report: 'The UK Cyber Growth Action Plan'. We were awarded new funding from UKRI and PolicyBristol to work with the Department for Science, Innovation, and Technology (DSIT) and the NCSC, exploring business engagement with the new Cyber Security Codes of Practice. We've been busy promoting our work on the Universal Barriers Framework with the business sector – including with the Department for Business and Trade (DBT).

And we've hosted a dedicated roundtable on small and medium-sized enterprise (SME) and Public Sector Approaches to Cyber Security.

It's been yet another busy year – as our Impact and Engagement Tracker for the past twelve months shows. Among the many highlights that stand out for me are two of the panels we convened at national events: one at CyberUK, discussing the value of sociotechnical approaches to cyber security, and one at the Cheltenham Science Festival, discussing 'Cyber Stories and Quantum Myths' with Luca Viganò, Adam Joinson, and Oishee Kundu. The audience particularly loved Luca's example of the story of Cinderella as a fairytale example of Multi Factor Authentication (MFA).

As you'll see from the updates that follow in this year's report, none of the important work that RISCS has delivered in 25/26 would have been possible without the vital support – and considerable talents – of its hardworking 2025 cohort of Principal and Senior Fellows: Professor Lizzie Coles-Kemp, Dr Matt Spencer, Dr Joe Burton, and Dr Marta F. Arroyabe. Our 2025 cohort of early career researchers have also made a real impact as Associate Fellows: Dr Sophie James, Dr Andrew Dwyer, Dr Oishee Kundu, Dr Bianca Slocombe, and Dr Rebecca Owens. Having spent 2025 as an Associate Fellow, Dr Sana Belguith will be staying on as a Senior Fellow for 2026.

I'm delighted that Lizzie, Joe, Marta, and Sana will be continuing their Fellowships through 2026, but our outgoing Fellows will also continue to play important roles at the heart of the RISCS community as our Alumni Fellows. In fact, some of our most valuable (and highly valued) collaborations are with our Alumni, and I want to single out former Associate Fellows Jason Dymydiuk, Partha Das Chowdhury, Maryam Mehrnezhad, and Ola Michalec for their leadership and support for various RISCS projects and activities in the last year.

Our Advisory Board and Honorary Fellows remain a constant source of practical wisdom – and I am immensely grateful for the time and expertise that they give.

Above all, I want to thank the RISCS management team – Dr Louise Evans and Dr Frances Pickworth – for their outstanding contributions over the last year.

Thank you both – and thank you all – for everything you've done and are doing to support and take care of the RISCS mission.

**Prof. Genevieve Liveley**
***RISCS Director***

RISCS

# IMPACT AND ENGAGEMENT HIGHLIGHTS TRACKER 25/26

**Apr 2025**

- **Cybernetic Culture Workshop,** *Lancaster*

**May 2025**

- **'Transforming Resilience by Rethinking the Cyber Security Ecosystem with Sociotechnical Approaches', CyberUK Panel,** *Manchester*
- **RISCS Annual Conference and Writers' Retreat,** *Bristol*

**Jun 2025**

- **'Stories of Cyber Security', Cheltenham Science Festival Panel,** *Cheltenham*

**Aug 2025**

- **CyberMi2 Research Day,** *Edinburgh*
- **Cybercrime Summer School,** *Strathclyde*

**Sep 2025**

- **Roundtable on Public Sector Approaches to SME Cyber Security,** *London*
- **Cybersecurity: A Matter of Law or a Matter of Justice?,** *Durham*

**Oct 2025**

- **Workshop on Principles-Based Assurance,** *Bristol*

**Nov 2025**

- **iNetwork Annual Conference: Universal Barriers Workshop,** *Manchester*

**Dec 2025**

- **RISCS Research Sprint: Cyber Security Codes of Practice,** *Bristol*
- **DBT presentation on Universal Barriers,** *online*

**Jan 2026**

- **Fellows' Away-Day and Workshop on AI and Cyber Security,** *Manchester*
- **Ancient Peace Studies Network inaugural workshop,** *St. Andrews*
- **Cross-Government Cyber Policy Forum,** *online*

**Feb 2026**

- **Preppers' Kit 2047 Workshop,** *Dundee*

**Mar 2026**

- **'Humanities in the Loop' AI and Cyber Security Sandpit,** *Bristol*
- **Roundtable on Cyber Security Codes of Practice with DSIT,** *London*

We see RISCS as a driver for five types of change:

**INSTRUMENTAL**
changes to plans, decisions, behaviours, practices, actions, policies

**CONCEPTUAL**
changes to knowledge, awareness, attitudes, or emotions

**CAPACITY**
changes to skills and expertise

**CULTURAL/ATTITUDINAL**
approaches to knowledge exchange, and research itself

**CONNECTIVITY**
changes to the number and quality of relationships and the quality of trust

# ADVISORY BOARD INSIGHT

In September 2025, I and fellow RISCS Advisory Board member Simon Shiu, as part of a group of researchers at the University of Bristol and Imperial College London, published a flagship report: 'The UK Cyber Growth Action Plan' (https://www.gov.uk/government/publications/cyber-growth-action-plan-2025). The work contains nine high-level recommendations and 24 targeted actions to support the development of the sector. Conclusions from the report are particularly timely given that cyber has been named one of the 'frontier industries' in the recent Industrial Strategy. In the wake of the new Government Cyber Action Plan (published January 2026), let's pause to reflect: what do we mean by 'cyber growth'?

Growth can refer to abstract metrics like GDP (Gross Domestic Product) and GVA (Gross Value Added) as well as empirical data on firm revenues, jobs, exports, skills pipelines, or even public trust. Each of these tells a different story, and none on their own captures the full picture. In calling for 'cyber growth', our aim is not to propose a single definitive metric, but to show why cyber growth needs to be understood across multiple dimensions if it is to inform policy, investment, and public debate.

Skills and workforce data form a key pillar of cyber growth measurement. Student enrolments in cyber security courses have increased, with just under 21,000 students enrolled in graduate-level cyber security courses in 2024. Employment within the cyber security sector has also grown, reaching over 67,000 full-time equivalents in 2025. These figures provide insight into labour supply and demand, but they exclude in-house cyber professionals working outside the sector itself. They also do not include generalist computer science students with cyber security expertise.

Exports offer another lens on cyber growth. UK cyber and physical security exports were valued at £11 billion in 2023, with Europe and North America as the main destinations. This figure is something to be proud of – we're the third biggest exporters of security products and services, behind only the US and China.

Finally, DSIT tracks the number of cyber security firms operating in the UK, currently estimated at just over 2,100. Because cyber security lacks its own Standard Industrial Classification code, this figure relies on combining public and proprietary datasets, which introduces uncertainty but still provides valuable insight into firm size, location, and specialisation.

Despite this breadth of data, tracking cyber growth remains challenging. A fundamental problem is the lack of a clear sectoral boundary. Without a dedicated classification code, cyber security is difficult to separate from the wider IT and digital economy. Estimates of size and growth will continue to remain imperfect, as they depend heavily on modelling choices and definitions.

Taken together, these challenges point to the need for a pluralistic approach to measuring cyber growth. Rather than relying on a single headline figure, cyber growth should be understood as a portfolio of economic, social, and institutional outcomes. Likewise, cyber policy spans multiple departments, each responsible for its own distinctive agenda.

From DSIT and the Home Office to HMRC, the NCSC, and the Department for Business and Trade, policymakers balance various competing interests. But cyber growth doesn't have to be a matter of choosing between innovating and protecting. A richer evidence base can help de-risk policy choices, identify where growth is genuinely sustainable, and improve public trust in technology-led interventions.

*This report has been adapted from a blog post that Ola wrote for RISCS earlier this year. You can read her post in full, as well as other posts by members of the RISCS community, on our website: https://riscs.org.uk/blog/.*

**Ola Michalec,**
***RISCS Advisory Board Co-Chair***

Co-chaired by Dr Jason Nurse and Dr Ola Michalec, the RISCS Advisory Board consists of members from key stakeholder groups in industry, government, and academia. The core mission of the Advisory Board is to advise on the strategic priorities of the Institute, as well as to support the activities of the RISCS research community and to maximise the impact of our work. The Institute's commitment to deep interdisciplinarity sees the 'real world' expertise of industry, business, and the wider cyber security community as foundational to its research programme. Accordingly, the Advisory Board members play a key role in advising on:

1. growing national capability and expertise in sociotechnical cyber security
2. supporting the community of researchers involved in this area
3. framing core research questions and future strategic priorities in policy for this area
4. reviewing and providing 'critical friend' feedback on research activity

# POLICY FOCUS: CYBER SECURITY CODES OF PRACTICE

The DSIT Cyber Security Codes of Practice (CoP) are designed to help UK organisations (including other government departments) optimise security provisions, providing guidelines for stakeholders on how to improve their cyber resilience in the face of increasing cyber risk. This year, we received funding from UKRI and PolicyBristol to work with DSIT and the NCSC to investigate the following research questions:

1. How can we optimise take-up of the codes by stakeholders across the ecosystem?
2. What barriers can we remove or minimise?
3. What incentives can we provide or amplify?

**Challenges (generic)**

- Voluntary codes (vs. statutory regulations) are the least influential drivers of engagement for cyber risk management – some stakeholders will hold out for statutory regulations or acts.
- Effective engagement with voluntary codes of practice is highly dependent on good governance and positive organisational culture.
- Positioning voluntary codes of practice/conduct within a broader framework (with common expectations and language) helps facilitate adoption – both the modularisation and alignment of CoP with Cyber Essentials should help drive and support adoption (further work on Principles Based Assurance (PBA) and Board Toolkits is in the pipeline).
- One size does not fit all – SMEs are poorly served by the Cyber Security CoP and Cyber Essentials.

**Challenges (specific)**

- The Cyber CoP require championing (and understanding) all through the organisational 'stack' – from the highest governance or board level through HR and Procurement, etc.
- The role of Senior Responsibility Officer (as one kind of champion) is necessary but insufficient – the whole organisation needs training and guidance.
- Navigating the different modules of the CoP portfolio is a significant barrier – a digital compass or dynamic tool (e.g., decision tree) is needed.
- Inconsistent and contradictory advice and language across different compliance requirements, e.g., the National Institute of Standards and Technology (NIST), is causing confusion – there's an urgent need for clarification, and also for a review of the Internet of Things (IoT) CoP.

**Key barriers and incentives**

- Cost/benefit analyses: organisations need reliable estimates of the costs and benefits of not complying – i.e., accessible **metrics**.
- Social proofs: organisations will use heuristics to guide their thinking on compliance (or not), observing other actors' behaviours (including that of government bodies) to guide their own – there is therefore a need for persuasive **stories** (and a 'drink your own champagne' attitude from government departments).
- Narrative credibility: there is a need for a sympathetic and joined-up policy narrative explaining why, for whom, how (etc.) the CoP are necessary – i.e., tailored **communications**.
- Resources: financial and skills-based resourcing issues will limit adoption and compliance – there is therefore a need for tailored **financial support/training**.

Our thanks to Dr Matt Spencer, Laura Barron, Andy Baldrian, Natasha Billson, Shaun Cairns, Tonejit Gad-Harry, Jennifer Daniel, Dr Dana Lungu, Alexander Kopsch, and Sharon Martin for their help.

**Sophia Walsh,**
***Doctoral Researcher, EPSRC Centre for Doctoral Training in Cyber Security, University of Bristol***

# POLICY REPORT: DIVERSITY AND CYBER SECURITY EXPERTISE


**Executive summary**

Our society is deeply and increasingly reliant on cyber security practitioners to ensure that digital services are dependable, critical infrastructure is resilient, and sensitive data is protected. Their success depends on diverse ways of thinking, skillsets, perspectives, and backgrounds. Today, the profession is being transformed, with standardised categories of specialism, new certifications, and evolving governance structures. While this process of professionalisation is driven by the need to better support practitioners and their employers, it is vital to understand any unintended consequences that may be emerging. We focus here on potential negative impacts on diversity, a topic that must be carefully addressed to ensure that cyber security remains an attractive field to work in, to support the legitimacy of professional institutions, and to enhance the efficacy of the field.

We developed methodologies for analysing the alignment of practitioners with new classifications of cyber security specialism, and for analysing the alignment of specialisms with cyber security problems. We tested these approaches using data from a small exploratory survey. We found that there is profound uncertainty about the impacts of professionalisation on diversity. This is rooted in a lack of data and a lack of theoretical analysis. This report takes a small step towards correcting this issue.


**Recommendations**

Surveys on diversity in cyber security (such as 'Decrypting Diversity', a survey formerly run by the NCSC) should be revived to ensure good quality data is available. They should be extended to gather more detailed data on respondents' expertise, for example using the CyBOK (Cybersecurity Body of Knowledge) framework. This would enable evidence to be gathered about correlations between diversity characteristics and the alignment of professionals with the UK Cyber Security Council Cyber Careers Framework specialisms. Regular surveys would enable analysis of how this alignment is changing over time.

The UK Cyber Security Council should commence work on new candidate specialisms to address the current lack of coverage of security human factors and security awareness. The latter could be based on the European Cybersecurity Skills Framework's 'Cybersecurity educator' role.

Future iterations of CyBOK should be informed by research into expertise diversity, to ensure that the value of the humanities and social sciences within cyber security is better reflected. Humanities and social science researchers working in the field of cyber security should engage more closely with the CyBOK community to support this.

The UK Cyber Security Council Cyber Career Framework's cross-referencing of specialisms with CyBOK knowledge areas should be refined and validated through qualitative studies of cyber security problem scenarios.

Spencer, M., Cámara-Menoyo, C., and Monteath, T. (2025). Diversity and Cyber Security Expertise: Policy report. University of Warwick.

https://warwickcim.github.io/cyberexpertisediversity_survey/

https://doi.org/10.5281/zenodo.17659435

**Matt Spencer,**
***University of Warwick,***
***RISCS Senior Fellow***

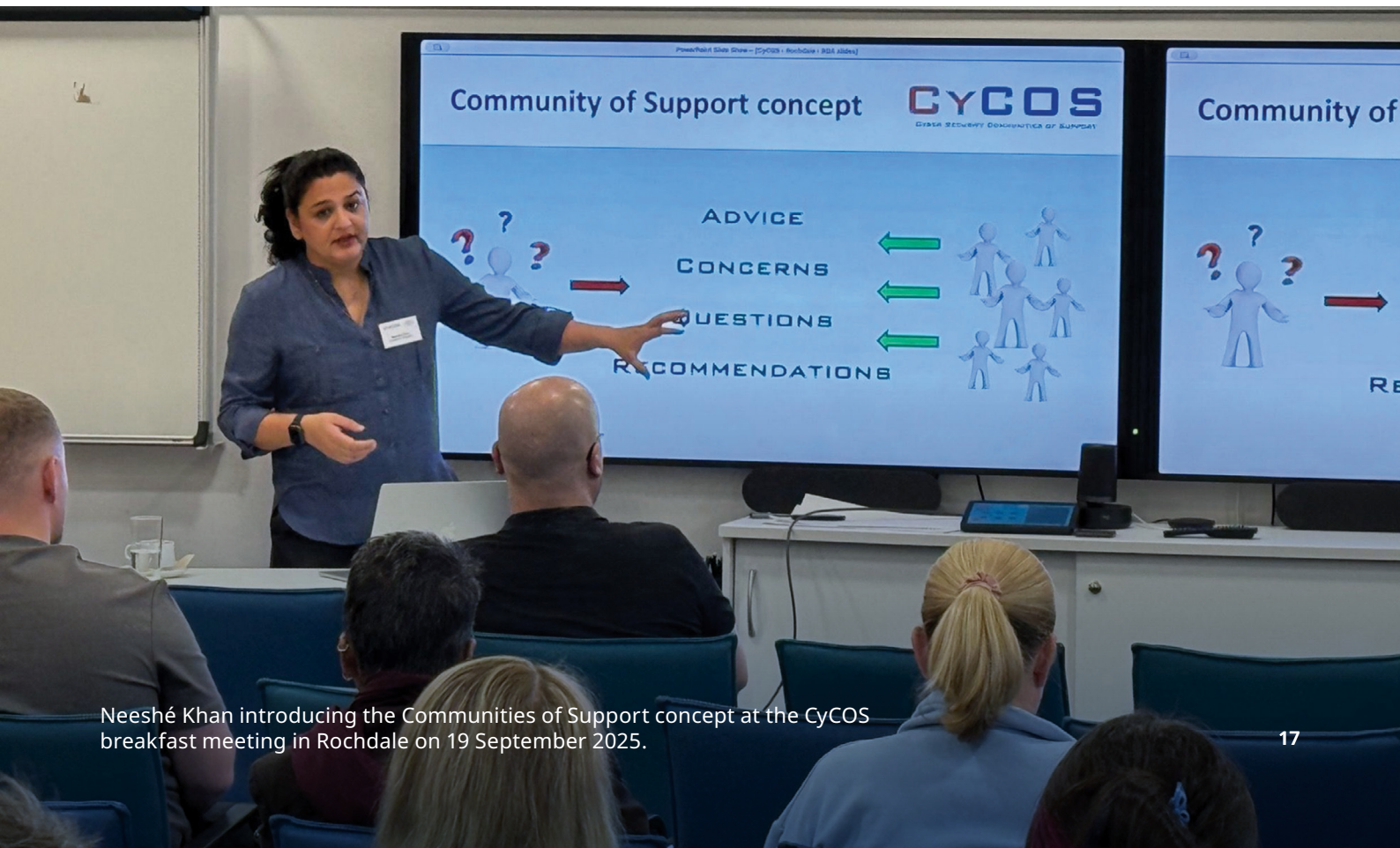
# RISCS RESEARCH ‘PROBLEM PAGE’

In an environment where sources of research funding are increasingly under pressure, it is ever more essential to demonstrate that our research aligns with important national challenges. The following set of questions highlights the problems that the RISCS community have identified as among the most urgent for sociotechnical researchers to help address. Each of these direct challenges has been proposed by key RISCS stakeholders.

***If cyber security doesn’t work for people, it doesn’t work.*** Sociotechnical problems and solutions cut across all areas of cyber security, but there are four key themes around which these problems and solutions cluster:

1. Barriers and Incentives (including Economics)
2. Future Risks and Resilience (including AI)
3. Cultures and Communications (including International Relations)
4. Usability and Trust (including Insider Threat)

Robust research into these areas is likely to underpin and complement the best work produced in any part of the cyber security ecosystem, including work on secure by design, cyber-physical systems, verification, and secure software and hardware.




Neeshé Khan introducing the Communities of Support concept at the CyCOS breakfast meeting in Rochdale on 19 September 2025.

The RISCS problem set is regularly updated and shaped through consultation with RISCS Principal, Senior, and Associate Fellows; the RISCS Advisory Board; industry and business delegates at the RISCS Annual Conferences; DSIT; the NCSC; and the EPSRC. It includes some of the generic cross-cutting themes above but links these to the priority challenges directly proposed by key RISCS stakeholders.

| | |
|---|---|
| **1** | What are the barriers and incentives to adoption of multi-factor authentication in the FTSE 100? **Barriers and Incentives** |
| **2** | What are the barriers and incentives for small businesses and start-ups to adoption of basic cyber security practices and accreditations, such as the NCSC's 10 Steps to Cyber Security and Cyber Essentials? **Barriers and Incentives** |
| **3** | How do we incentivise better security for cyber-physical systems? **Barriers and Incentives** |
| **4** | How will game-changing technologies (automation, LLMs, AI, quantum, etc.) change the ways in which cyber security products and services are designed and delivered for people and businesses? **Future Risks and Resilience** |
| **5** | What are the risks (and where is the resilience) as consumer apps become password-less? **Future Risks and Resilience** |
| **6** | How can we communicate cyber security and cyber risk and resilience to different audiences? **Cultures and Communications** |
| **7** | What are the normative and cultural traits, behaviours, and attitudes among different professional groups that aid or block cyber security implementation? **Cultures and Communications** |
| **8** | How do we foster robust, replicable, and evidence-led approaches to supporting sociotechnical cyber security and safety research across all parts of the research lifecycle? **Cultures and Communications** |
| **9** | How can we use data (and what data do we need) to map the scale, reach, and impact of cyber crime harms upon vulnerable groups? **Usability and Trust** |
| **10** | How can we deploy human-centred design and human behavioural studies to enhance cyber resilience, safety, and security? **Usability and Trust** |

# RISCS PRINCIPAL AND SENIOR FELLOWSHIPS FOR 2025: REPORTS

### Digital Responsibility

I am delighted to say that five years of RISCS work in digital responsibility have come together in the first publication in RISCS' Bristol University Press 'Shorts' series. *Understanding Digital Responsibilities* was written by myself and colleague Mark Burdon and sets out our thinking to date on this topic. The book is written for policy makers, academics, and practitioners grappling with questions of responsibility in digital contexts. Whether you are writing a policy that addresses a societal issue through digital means or a practitioner designing and implementing a digital system, this book has something to offer.

At the heart of the book is a framework of digital responsibility developed from the thinking that took shape during my RISCS fellowship. The framework brings together digital responsibility as a component of a system or policy, and digital responsibility as a dynamic interactive component of policy negotiation and digital systems implementation. The framework is designed to help policy makers, security practitioners, and researchers break down questions of digital responsibility and develop practical steps to ensure that digital responsibilities are treated as a living, dynamic interaction woven into day-to-day use of digital systems.

We recognise that the topic of digital responsibilities can seem a little abstract, so we worked with illustrator Chris Day at Little Creature to bring the topic to life and to show some of the many ways in which digital responsibility touches our day-to-day lives. The book shows how responsibilities are reflected not only through our actions and the assignment of blame when responsibilities are missed, but also through our day-to-day interactions and in our hopes and aspirations for the future.

**Lizzie Coles-Kemp,**
***Royal Holloway, University of London, RISCS Principal Fellow***

### Futures and Emerging Technologies

It was a pleasure to contribute to the RISCS community this past year. Highlights included involvement in the RISCS PBA workshop, where I was able to deliver remarks about how human factors continue to be conceived too narrowly in cyber security, how adversary human factors and behaviour need to be factored into PBA processes in a more comprehensive way, and how new ways to model the behaviour of threat actors should/could be embedded within assurance processes and iterated over time. Another highlight was a workshop on AI Security that I co-hosted in Manchester alongside RISCS Fellow Sana Belguith (Bristol), and Tooska Dargahi (Manchester Metropolitan University), with the support of RISCS. I delivered a back casting session on the future emergence of Artificial Super Intelligence, which encouraged attendees to think about technical and sociopolitical trajectories in this area. It was illuminating to see how the future scenario, which was itself AI

generated, revealed and reflected our own biases and the biases embedded in AI systems. Two major publications last year highlighted the importance of Cyber Diplomacy (the *Palgrave Handbook on Cyber Diplomacy*) and *AI and Serious Online Crime* (a research report for CETaS and the Alan Turing Institute). RISCS continues to be an incredibly supportive, creative, and vitally important community driving research and engagement on sociotechnical cyber security and technological futures.

**Joe Burton,**
***Lancaster University, RISCS Senior Fellow***

### Cyber Security and Resilience in SMEs

In 2025, my RISCS-related research focused on the sociotechnical and economic dimensions of cyber security adoption and governance, particularly in SMEs. I organised a RISCS workshop in September on market and incentive structures shaping SME cyber security, and contributed to other RISCS events throughout the year. I also delivered a presentation at a RISCS PBA workshop, examining PBA as an economic system and highlighting implications for incentives, accountability, and exclusion. During the year, I submitted several research papers on cyber security adoption, organisational capabilities, and SME cyber resilience, which are currently under review. One of our papers was cited in the Cyber UK Growth Action Plan.

Alongside academic research, I was actively engaged in applied and impact-oriented work aligned with RISCS' mission. I participated in CyberUK 2025 as an exhibitor, showcasing an AI-enabled cyber security self-assessment and maturity tool designed to support small organisations, CyberSecurityAId. I also led and delivered cyber security consultancies for SMEs through the Innovate UK-funded Cyber Innovate to Elevate programme with Freeport East. This work involved multi-week audits, gap analysis, benchmarking against relevant assurance frameworks, and the development of tailored cyber security roadmaps to support organisational improvement and the resilience of small businesses.

I continued to contribute to policy-facing and advisory activities relevant to RISCS. I served as an academic mentor within HMRC's Open Innovation Policy Fellowship, focusing on risks associated with the use of AI in the public sector. I also continued my roles as a member of the Bank of England's Central Bank Digital Currency Academic Advisory Group and of the Advisory Board of the Eastern Cyber Resilience Centre, advising on digital transformation, cyber security, and SME-related challenges. In parallel, I secured and developed new funding for work on SME cyber security, critical infrastructure, and the sustainability of cyber security (including links to the circular economy), with several projects planned to commence in 2026.

**Marta Fernandez De Arroyabe Arranz,**
***University of Essex, RISCS Senior Fellow***

### Interdisciplinarity in Cyber Security

I was delighted to continue with my RISCS senior fellowship in 2025, as an opportunity to think through interdisciplinarity in sociotechnical cyber security across practice, research, and policy.

In collaboration with Carlos Cámara-Menoyo and Timothy Monteath I wrote up the policy report from our exploratory survey study of expertise diversity within the cyber security profession. This work examined the value of diverse expertise in cyber security practice, and looked at the ways in which diversity of expertise could be threatened or enhanced by increasing standardisation of professional roles.

I published a Special Issue on critical interdisciplinary cyber security for the journal *Information, Communication and Society*. In my introductory article, I look at interdisciplinarity in light of the growing interest within critical security studies in reflexive conceptions of 'critique'. Building on these ideas, I argue that being interdisciplinary in cyber security research today is not just a matter of combining tools and ideas from different disciplines. It also requires careful positioning of scholarship in relation to the interests within policy and practitioner communities.

Building on my previous RISCS report 'Assurance by Principle', I developed further policy research into PBA. Responding to questions raised by NCSC about potential barriers to PBA adoption, I developed a new report examining the different kinds of sociotechnical causal mechanisms that policymakers will need to consider when planning the introduction of PBA to a new sector. This report also drew on fantastic contributions from attendees at a RISCS PBA workshop held in October 2025. You can find this report (and links to other publications) on the RISCS website.

**Matt Spencer,**
***University of Warwick, RISCS Senior Fellow***

# RISCS PRINCIPAL AND SENIOR FELLOWSHIPS FOR 2025

Three of the RISCS Principal and Senior Fellowships from 2025 have been refreshed and continue into 2026, and two new Senior Fellows have joined the team. In addition to Lizzie Coles-Kemp (Digital Responsibility), Joe Burton (Futures and Emerging Technologies), and Marta F. Arroyabe (Cyber Security and Resilience in SMEs), the Senior Fellows team now includes former Associate Fellow Sana Belguith (AI and Space) and Daniel Thomas (Cyber Crime).

To find out more about our Senior Fellows, take a look at their bios on the RISCS website: https://riscs.org.uk/fellows/senior-fellows/.

Our Principal and Senior Fellowships for 2026 are now focused on the following five themes:

**AI and Space**

As I transition into the role of RISCS Senior Fellow, my focus for the coming year will move from project initiation toward the integration and synthesis of the research themes established during my fellowship. Building on the foundations of the SCULI (Securing Convergent Ultra-Large Scale Infrastructures) and Space Invaders projects, my primary goal is to bridge the gap between technical breakthroughs – such as our recent AI safety assessments – and practical, sociotechnical guidance for the UK's critical infrastructure. I intend to focus on:

- Consolidating cross-sector insights: translating the multidisciplinary findings from our Manchester workshop and international panels into a coherent set of security principles for the space and defence sectors.
- Strengthening community ties: using my position on the Space West advisory board and my links with the NCSC to ensure that our research remains aligned with national security priorities and industry needs.
- Sustainable knowledge transfer: ensuring that the high-level security challenges identified in my work on post-quantum cryptography and AI resilience are communicated effectively to policymakers, helping to move from 'awareness' to 'actionable frameworks'.

**Sana Belguith,**
***University of Bristol, RISCS Senior Fellow***

### Futures and Emerging Technologies

I am delighted to be continuing in my role as Senior Fellow in 2026. The focus of my continued RISCS fellowship is 'Futures and Emerging Technologies', which includes the aim of understanding how the deployment of emerging technologies such as AI may induce risk and uncertainty in national security communities, how the deployment of AI in cyberspace for both defence and offence creates instability and/or unintended consequences, and how AI might induce mass cognitive/psychological effects in populations through emerging forms of deceptive content. My work on technological futures continues across teaching and research. I have ongoing research projects on Human-AI teaming and the Strategic Cultures of Threat Actors in Cyber Security, and I continue to embed creative futures methods in my teaching, including through the use of student short stories based on the 'useful fiction' approach. Plans in the pipeline include the further development of a book project on The History of AI Futures and large research grant applications on (a) Technological Disorder, and the (b) the threat from Artificial Super Intelligence.

**Joe Burton,**
***Lancaster University, RISCS Senior Fellow***

### Digital Responsibility

The RISCS Fellowship in Digital Responsibility examines what the term 'digital responsibility' means and its relevance to security. Its goal is to enhance the relationships between responsibility and the design, deployment, and use of security controls so that their effectiveness is improved for all. The Fellowship was launched in 2020 and its initial purpose was to develop a research agenda that furthered our understanding of digital responsibility. In 2023 a second phase for the Fellowship began, and attention was turned to the operationalisation of digital responsibility and how we can make this often-abstract concept into something practical that can be embedded in day-to-day cyber security practice. Over the next 12 months Lizzie plans to publish the outputs from the first phase of the digital responsibility Fellowship and to set out a framework for thinking through where and how to enable digital responsibilities. She is also committed to the development of an engagement toolkit to support discussions related to the realisation, establishment, and actioning of digital responsibilities.

**Lizzie Coles-Kemp,**
***Royal Holloway, University of London, RISCS Principal Fellow***

**Business**

Cyber security is a growing challenge for SMEs, which are critical to the economy yet often lack the resources, expertise, and strategic frameworks to manage cyber risks effectively. As SMEs embrace digital transformation, they face evolving threats that can disrupt operations, compromise sensitive data, and impact wider supply chains. Many SMEs struggle to implement cyber security measures that are both effective and feasible within their resource constraints. This RISCS Fellowship will focus on understanding how SMEs perceive and respond to cyber risks, identifying the barriers they face in adopting security measures, and exploring how policy, regulation, and industry initiatives can better support them. A key activity will be the development of a research-driven framework to improve SMEs' access to practical, scalable cyber security solutions. Ensuring that SMEs are equipped to manage cyber security effectively is not just important for their individual resilience, but for the security of entire digital ecosystems, given their role in supply chains and interconnected networks. By supporting the RISCS community to develop more SME-focused approaches to cyber security, this theme will contribute to more inclusive and effective security strategies, strengthening the overall resilience of the economy in an increasingly digital world.

**Marta Fernandez De Arroyabe Arranz,**
***University of Essex, RISCS Senior Fellow***

**Cyber Crime**

Cyber crime has a significant impact on society. It is an under-reported crime type, where victims often blame themselves. This Senior Fellowship will focus on improving understanding of cyber crime and disseminating that understanding. The approach to improving understanding will often involve collecting quantitative data on security properties of systems, or cyber crime within them, and combining analysis of that data with analysis of qualitative information from interviews or scraped text from people causing or trying to prevent crime within these systems. One current project involves interviewing researchers who have experienced legal risks to understand what that looks like across the UK and US. Daniel hopes his technical background and transdisciplinary approach will be helpful to the RISCS community. The key activity he will organise during his fellowship is the 9th Strathclyde International Perspectives on Cybercrime Summer School, which will be held 24th-28th August 2026 at the University of Strathclyde.

**Daniel Thomas,**
***University of Strathclyde, RISCS Senior Fellow***

# RISCS EARLY CAREER ASSOCIATE FELLOWSHIPS FOR 2025: REPORTS

In April 2025 we appointed a new cohort of five outstanding early career researchers as RISCS Associate Fellows. These are all 'rising stars' in the sociotechnical space, whose interdisciplinary skills and expertise make them the perfect people to help RISCS explore and shape the future of cyber security.

Our Associate Fellowships cohort of 2025 focused on the following research themes:

- Oishee Kundu (Cardiff University) - Markets and Technology Futures
- Bianca Slocombe (Coventry University) - Psychology and Cyber Security
- Andrew Dwyer (Royal Holloway, University of London) - Digital Decisions, (Geo)Political Economies
- Sophie James (Lancaster University) - Netnography
- Sana Belguith (University of Bristol) - AI, Space, and Cyber Security

The following updates offer a snapshot of the varied activities that the Associate Fellows have been working on.

**Markets and Technology Futures**

Is security a criterion when buying digital technology? The question merits investigation at both an individual and an organisational level, the latter involving an examination of procurement procedures and purchasing frameworks. In public procurement, there has been a shift from being price-drive to value-driven, and values can range from the social (fair employment, inclusivity) to the environmental. Research and practice have demonstrated the role of the demand side, particularly government procurement, in promoting innovation, social value, and sustainable development. But what about security and resilience? Although Cyber Essentials certification is a requirement for suppliers bidding for certain types of contracts, it is not universal, and it may have limited links to the product or service being supplied.

As a RISCS Associate Fellow, I contributed to the PBA workshop, presenting perspectives from public procurement about choosing products based on a complex mix of price and values. More broadly, I have enjoyed the opportunity to share my knowledge and expertise with NCSC. While it is encouraging to note the NCSC's acknowledgement that markets don't work perfectly without intervention, what is less explored is how public procurement can shape the market towards more secure digital futures.

My academic background lies in innovation management, and for over 50 years now, innovation scholars have been emphasising the role that buyers or the 'demand side' play in technology development. Technology development is an interactive and iterative process, intricately linked to social systems, buyer preferences, and norms and values. However,

this considerable body of innovation scholarship has not been able to dispel the belief that technological breakthroughs come from a cornucopia of research investment and 'if you build it, they will come'.

I have always been keen to unpack the beliefs and narratives that shape how we think about digital security and technology futures. Thanks to the fellowship, I was able to take this idea to the Cheltenham Science Festival 2025 and was part of a panel discussion on 'Cyber Stories and Quantum Myths' with Genevieve Liveley, Luca Viganò, and Adam Joinson. We discussed how stories – from simple fairytales and fables to grand epics - can help to convey cyber security concepts and make sense of the opportunities and challenges of the digital world. We also discussed the need to be cautious about the stories we tell, as they can perpetuate existing biases. Nevertheless, stories forge connections across cultures, and finding technical concepts described through stories can perhaps lower the barriers to engagement with questions about technology markets and technology futures. Promoting a more participatory approach to digital security would also be a triumph of the 'demand side' and perhaps accelerate the process of creating desirable technological futures.

**Oishee Kundu,**
***Cardiff University, RISCS Associate Fellow***

**Psychology and Cyber Security**

My research examines how sociotechnical factors shape decision-making across multiple security themes. My RISCS fellowship has provided a strong platform from which to embed this perspective across numerous funded projects for different government departments and organisations.

This work has included updating frameworks for analysing terrorist targeting behaviours by integrating considerations of digital behaviours and assessing the potential role of technical support tools in supporting parts of this process. I have contributed to improving insider risk assessment by exploring how technical actions intersect with psychological and organisational factors, and by assessing the potential for AI to support rigorous, evidence-based approaches to identifying and mitigating insider threats. I have delivered scenario exercises as part of a project on foreign interference and state threats, weaving in cyber components to capture data on how participants make decisions. This work has highlighted challenging questions around issues of risks and responsibilities that demand sociotechnical analysis. I have also investigated how sacred values shape international negotiations, raising questions about how such values may shift or manifest differently in cyber-mediated contexts.

Through engagement with the RISCS community and participation in key events, I have been able to exchange ideas and situate this work within a rich interdisciplinary environment. I have also been invited to contribute to wider sector conversations. This includes presenting to technical leads from major international companies at the Overseas Security Advisory Council UK (OSAC) and presenting at the Homeland Security in Applied Research Technology

& Science (HEARTS) Symposium in Singapore. This is a forum that convenes academia, industry, and Home Team practitioners. These engagements have broadened the reach of my research, strengthened cross-sector relationships, and revealed promising opportunities for future collaboration.

**Bianca Slocombe,**
***Coventry University, RISCS Associate Fellow***

**Digital Decisions, (Geo)Political Economies**

It has been a pleasure to be an Associate Fellow at RISCS for a second year, where the whole team has continued to support my work concerning my interest in the role that automation (including AI) and digital technologies are playing across security and privacy at various geopolitical scales, whether in communities in Northern England, national policy discussions, or international attention to cyber operations and cyber intrusion technologies. My focus this year has been on two principal axes.

Cyber strategy and policy: This year, I was awarded funding for a project examining how cyber policy considers the 'whole of society' and its contribution to a state's cyber power. This is a comparative study between Australia and the UK, conducted with my UNSW Canberra collaborator, Dr Sally Burt, with UK funding granted by the SPRITE+ network. I benefited from funding from RISCS to travel to Paris to the second Pall Mall Conference on countering the proliferation of cyber intrusion capability. I have continued to engage with events on cyber operations to help build better exchange of perspectives between academia and government.

Everyday practice: The focus for this aspect of my work this year has been on two funded projects:

1. An EPSRC-funded project, Equitable Privacy, where I have been working on developing new abstractions to link community-centred studybeds to those of software development, and which will lead to forthcoming publications. This project also produced a paper I presented at the premier human-computer interaction conference (CHI – 'Friend or Foe? Navigating and Re-configuring "Snipers' Alley"'), which explored how people experience digital security.
2. As PI on an AHRC-funded project, Fake in the Community, where I have been working with communities to build resilience against 'cheap fakes' to build a prototype toolkit to foster grounded community-building and conversation.

**Andrew Dwyer,**
***Royal Holloway, University of London, RISCS Associate Fellow***

## Netnography

During 2025/26 I contributed to a range of cyber security education, outreach, and interdisciplinary engagement activities linked to Security Lancaster and the wider regional cyber ecosystem. As Academic Lead for the Lancashire Cyber Festival Education Week 2026, I designed and delivered Cyber Quest, a gamified campus-wide cyber challenge that brought over 100 college and sixth-form students to Lancaster University to explore pathways into cyber careers through hands-on activities such as phishing detection, code-breaking, and digital forensics challenges. I also shared reflections on the design of Cyber Quest through the Lancaster University Cyber Security Education blog, highlighting the value of immersive and interdisciplinary approaches to cyber literacy.

Alongside this outreach work, I have integrated cyber security, digital risk, and misinformation into undergraduate teaching by embedding these themes within a core Social Media Marketing module, introducing students to issues such as platform vulnerabilities, misinformation, influencer accountability, and social media crisis management from a marketing and consumer perspective.

I am currently organising the upcoming Cybernetic Culture Workshop 2026, an interdisciplinary event kindly funded by RISCS and hosted at Lancaster Castle, bringing together researchers across marketing, cyber security, and the humanities to explore emerging cultural dimensions of digital risk and cyber culture under the theme of 'digital underworlds'.

Finally, I have been developing my research profile around the cultural dimensions of cyber risk, examining how online 'dark' digital environments challenge perceptions of reality, including phenomena such as 'the Backrooms', the historical origins of supernatural industries in Victorian Britain, and the growing dependency of consumer subjects on AI companion technologies. This emergent research agenda is currently being developed through a series of manuscripts, with papers presently under second and third round review at world-leading journals.

**Sophie James,**
***Lancaster University, RISCS Associate Fellow***

**AI, Space, and Cyber Security**

The past year of this fellowship has been a period of rapid expansion, moving from foundational research to contributing to and leading national and international conversations on the security of our most critical convergent infrastructures. I have focused on the intersection of cyber security, emerging technologies, and sociotechnical approaches.

The fellowship has enabled me to secure significant funding and lead pioneering projects that address the 'perfect storm' of emerging threats related to AI, quantum, and space.

- The space frontier: Building on the momentum of the fellowship, I am now the Project Lead for 'Space Invaders: Enhancing the resilience of space systems' (£100k), focusing on space system resilience, and the ASSAI: Assessing Space Security in the Presence of AI project (£70k) in collaboration with the Alan Turing Institute and Dstl.
- Scale and convergence: I co-lead the SCULI Programme Grant (£6.8m), a five-year programme to secure ultra-large scale infrastructures. This ensures that the sociotechnical insights championed by RISCS are embedded into the very fabric of future UK infrastructure.
- The quantum transition: Through a British Council-funded project, I have spearheaded the roadmap for migrating critical systems to post-quantum cryptography (PQC), ensuring global infrastructure remains secure in the 'Quantum Era'.

A highlight of my technical contribution this year was the rapid security assessment of DeepSeek. Within 24 hours of its release, my team successfully bypassed its safety guardrails. This breakthrough provided immediate, actionable intelligence to the UK security community, resulting in:

- Feature coverage by the University of Bristol.
- Inclusion in the NCSC CTO's weekly highlights, directly informing national awareness of LLM vulnerabilities.


Co-organisers Joe Burton, Sana Belguith, and Tooska Dargahi at the Workshop on AI and Cyber Security in Manchester, January 2026

I have also delivered a number of keynotes, talks and panels to national and international audiences:

- Policy and governance: I represented the community at the United Nations Institute for Disarmament Research (UNIDIR) Outer Space Security Conference in Geneva and currently serve on the Steering Board of the Space West Cluster.
- International influence: I have advocated for collaborative defense against cyber threats to space assets, from the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Conference in Colorado, US – where I spoke on the urgent need for a cyber-skilled space workforce – to the Global MilSatCom in London.
- Thought leadership: I have delivered keynotes at the RITICS Fest, the Surrey Cyber Security Cluster, and the RISCS PBA workshop, consistently bridging the gap between academic rigor and operational security needs.
- National convening: I co-organised a landmark workshop in Manchester on Sociotechnical Approaches to AI Security, where I curated and led a panel that focused on the intersection of AI, defence, and space while considering national and international policies.

**Sana Belguith,**
***University of Bristol, RISCS Associate Fellow***

# RISCS EARLY CAREER ASSOCIATE FELLOWSHIPS FOR 2026

In January 2026 a new cohort of five early career researchers joined the team as RISCS Associate Fellows.

Our Associate Fellowships cohort of 2026 will focus on the following research themes:

- Jiahong Chen (Sheffield University) – Law
- Nandita Pattnaik (Kingston University, London) – Families and Homes
- Lena Podoletz (Lancaster University) – Criminology
- William Seymour (King's College London) – Security, Privacy, and Ethics
- Sarah Turner (University College London) – Ransomware and Internet of Things (IoT)

You can find out more about our new Associate Fellows on the RISCS website: https://riscs.org.uk/fellows/associate-fellows/.

Look out for updates on their research and activities on our website and social media accounts.





# RISCS PHD STUDENT PLACEMENTS FOR 2025/26

**The Valuation of Secure Software**

RISCS and the University of Warwick are jointly supporting a Warwick Collaborative Fellowship, which will enable a research student to undertake a PhD exploring the valuation of secure software, working with Matt Spencer at the University of Warwick's Centre for Interdisciplinary Methodologies.

The security of digital infrastructure impacts contemporary society in many ways, from privacy to safety, from economy to the availability of vital services. Actors of many kinds, whether consumers of software, developers, vendors, or policymakers, have an interest in demonstrating and assessing the security of software products. This project builds on sociological research into cyber security (Spencer 2024, Spencer and Pizio 2024) arguing that this challenge of evaluation and communication cannot be seen as a purely 'technical' challenge. Drawing on work on valuation (Helgesson and Muniesa 2013), market narratives (Beckert 2013), and narrative theory of organisation (Cooren 2000), the student will explore how value is accounted for in software marketing, procurement, and policy; how practitioners 'make sense' of security as a kind of quality of software; and how narratives about security shape the constitution of digital infrastructures.

**Research questions:**

- How is the value of secure software made visible in market practices?
- How can sociological approaches to valuation contribute to our understanding of secure software?
- What are the implications of this perspective for cyber security policy?

The student will work closely with RISCS throughout the project, and our impact activities will include a RISCS policy workshop on valuing software.

**Matt Spencer,**
***University of Warwick, RISCS Senior Fellow***

# RESPONDING TO BBC *PANORAMA'S* 'FIGHTING CYBER CRIMINALS'

During her summer internship with RISCS, doctoral student Lucy Davies (University of Bristol) drew upon the expertise of the wider RISCS community to put together a critical response to the BBC Panorama documentary 'Fighting Cyber Criminals'. Lucy summarised her findings in a blog post in which she explored the impact of the programme on public understanding and engagement with cyber security.

**Key takeaways:**

- The documentary deserves credit for making cyber crime accessible in a constrained format and for offering rare access to NCSC operations.
- The documentary portrays hackers as omnipotent and cyber security as the domain of elite 'spies'; such mythologising may discourage the general public and SMEs from taking practical cyber security actions themselves.
- The framing of ransomware as purely financially motivated represents an oversimplification and ignores other rationales (e.g., activism, espionage, disruption).
- The psychological burden on cyber security professionals is glamorised rather than realistically portrayed, missing an opportunity to raise awareness of burnout and human-centred issues at the heart of incident responses.
- While seemingly targeted towards a primary audience of business owners and members of the general public, the documentary offers little in the way of clear, empowering advice – potentially leaving viewers confused and disengaged.
- Experts highlight the need for inclusive language and demystification to support national cyber resilience.

**Proposed actions:**

- Produce a follow-up episode or companion content focused on practical cyber security advice tailored to specific audiences (e.g., SMEs, parents, older adults).
- Showcase cyber security educators and everyday security practices to help normalise and humanise digital safety.
- Reframe cyber security in media communications to reduce fear-based storytelling and foster a sense of agency and relevance among key audiences.
- Encourage policymakers and media outlets to collaborate on public-facing cyber literacy initiatives using responsible and accessible language.

You can read Lucy's blog post in full on the RISCS website: https://riscs.org.uk/blog/

**Lucy Davies,**
***Postgraduate Researcher and RISCS Doctoral Intern, Cyber Security (Cyber Secure Everywhere) CDT, University of Bristol***

# RISCS UKRI PROJECT UPDATES

## CyCOS: Enhancing Cyber Resilience of Small and Medium-sized Enterprises (SMEs) through Cyber Security Communities of Support

Led by Prof. Steven Furnell (University of Nottingham), in collaboration with Dr Maria Bada (Queen Mary University of London) and Dr Jason R. C. Nurse (University of Kent), CyCOS has been investigating and enhancing the cyber security support available to SMEs.

The project is now in its final year, and the key aspect of the last year has been the formation of the Communities of Support and the commencement of pilot activities. At the time of writing we have two Communities, one based around micro-SMEs and one composed of small and medium businesses. Each began with around eight SME members, alongside an allocation of accompanying cyber experts to provide advisory input. Community activities are underpinned by a Support Broker platform, providing each group with an area for discussion and raising questions. Additionally, the team is running online meet-up activities (at approximately three-week intervals) to establish and build Community engagement. These are based around topics suggested by the SMEs, and delivered by the CyCOS team and project partners. The main project period has been extended until the end of September to allow the communities to be maintained and to extend the findings from the pilots.

Alongside this, we will be trialling the establishment of SME-led Communities, with host SMEs being positioned as 'Support Beacons' and attracting others to join a Community that they facilitate. The CyCOS team is recruiting the SMEs and designing a Beacon 'toolkit' that can be used to guide and support their activities. Beacon-led Communities will then be incorporated into the activities being arranged for the existing pilots.

Dissemination activity has been significant, with highlights including a keynote panel at Infosecurity Europe in London, and exhibiting and speaking at the SME XPO event thereafter. CyCOS has also been represented in panel sessions at teissLondon, the Global Cyber Summit, and CIISec LIVE, and delivered talks at various events including EUROCRIM 2025 (Athens), the 4th Annual University of North Texas Cybersecurity Symposium (Dallas), and the ERC State of Small Business Britain Conference (London). We have also run a breakfast meeting for the Rochdale Development Agency and provided input to the RITICS Economics of Cyber Security workshop in Oxford. Academic outputs have included papers published in *Computers & Security* and the CRITIS 2025 international conference, and a related article in the BCS ITNOW magazine.

Full details and links to resources can be found at www.cycos.org.

**Steven Furnell,**
***University of Nottingham***

# CyCRAFT: Cyber Statecraft in an Era of Systemic Competition

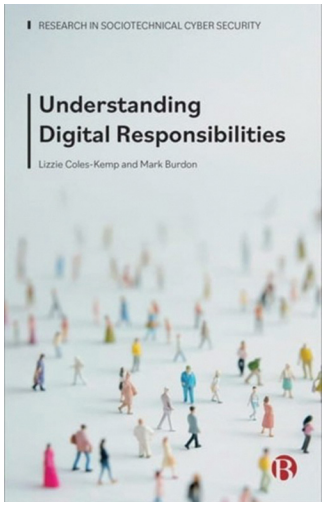
Funded by EPSRC and Dstl with RISCS support, the two-year project, 'Cyber Statecraft in an Era of Systemic Competition' (CyCRAFT), is drawing to a close. Led by King's College London, in collaboration with the University of Bath and the Royal United Services Institute (RUSI), the project explores the utility and character of 'cyber statecraft' as a way of understanding and analysing state behaviours in and through global cyberspace. Cyber statecraft encompasses not just the everyday activities of defensive cyber security but also the workings of cyber diplomacy in international fora and the use of digital tools for military and intelligence operations. Our contention is that cyber statecraft provides a lens through which to view state actions in cyberspace that are often viewed as separate but which in reality are often interconnected and complementary. This holistic perspective allows us to identify and evaluate states' development and use of cyber power and to understand how they seek to achieve national strategic objectives through cyber statecraft.

This project has been characterised throughout by a high level of stakeholder engagement. We held ten public events, several dedicated specialist workshops – including colleagues from Brazil, India, and South Africa – and have latterly hosted 'Whitehall Briefings' to inform policy-making across UK Government. Project members have also contributed to government workshops feeding into the next iteration of the National Cyber Strategy and given oral evidence to Parliament. Our outreach programme has also included a series of video commentaries on YouTube, specialist reports for RUSI and the Carnegie Endowment for International Peace, and academic conference papers. Several articles are in review with academic journals and will be published in due course. This includes work on conceptualising cyber statecraft through 'repertoires' of state behaviour; econometric, discourse, and conceptual analyses of cyber power; a comparative study of middle powers' cyber statecraft; and articles on private-sector firms as key contributors to cyber statecraft.

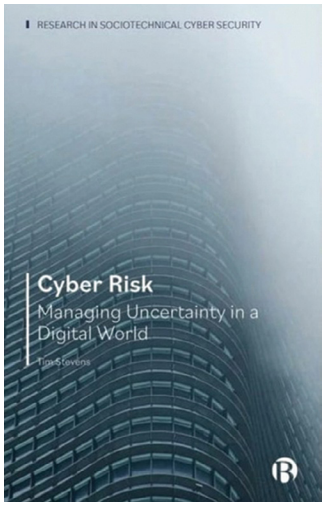
**Tim Stevens,**
***King's College London***

# BRISTOL UNIVERSITY PRESS 'SHORTS'

This year, in collaboration with RISCS, Bristol University Press (BUP) has launched a series of book 'Shorts' on the broad theme of Sociotechnical Cyber Security. This series, edited by Genevieve Liveley (RISCS Director) and Lizzie Coles-Kemp (RISCS Principal Fellow), aims to provide a unique platform for interdisciplinary work that examines the intersection of cyber security technologies and societies. The first book in the series has now been published, with a second forthcoming.




*Understanding Digital Responsibilities* by RISCS Principal Fellow Lizzie Coles-Kemp and Mark Burdon (open access) addresses the question: 'How can we make the digital world safer, more responsible, and accountable?' BUP says: 'This innovative book offers an original framework for understanding digital responsibility, blending insights from law, technology, and policy. Through a series of case studies showcasing work from early career researchers, it highlights the diverse groups, values, and governance challenges shaping digital environments across jurisdictions. From crafting effective policies to designing ethical digital products, this book equips policy makers, practitioners, and academics with the tools to minimise harm and enhance accountability and responsibility in the digital age. This is a vital resource for navigating the complexities of digital responsibility in a pluralistic, globalised world.' This book is now available under Open Access from the BUP website.




*Cyber Risk: Managing Uncertainty in a Digital World* by RISCS Project Fellow Tim Stevens asks: 'What does it mean to live in a world where our most essential systems are digital – and vulnerable?' BUP says: 'This book takes readers beyond the technical aspects of cyber security to explore how the management of digital risk shapes politics, policy, and everyday life. Drawing on case studies from corporate boardrooms to international affairs, it reveals the social and political logics driving the fast-growing cyber risk industry. From insurance markets to resilience planning, the book unpacks how these practices order people, places, and possibilities – and why understanding them is vital for navigating the promises and perils of our digital future.' This book is currently in preparation and will also be published under Open Access.

Proposals for books of between 30,000 and 50,000 words are encouraged from a variety of disciplines. If you would like to discuss submitting a proposal, please email the series editors:

- **Genevieve Liveley: g.liveley@bristol.ac.uk**
- **Lizzie Coles-Kemp: Lizzie.Coles-Kemp@rhul.ac.uk**

More information about this series is available on the Bristol University Press website: https://bristoluniversitypress.co.uk/research-in-sociotechnical-cyber-security.


Steven Furnell offers insights from the CyCOS project as a panellist at Infosecurity Europe 2025.

# MANAGER'S AND PROJECT COORDINATOR'S MESSAGE

Louise and Frances have spent another busy year supporting Genevieve, the Fellows, the Advisory Board, and our ever-growing community in delivering the RISCS mission. Events sponsored or organised by RISCS this year have frequently taken us from Bristol to London and Manchester, and involved us supporting activities in Strathclyde, St Andrews, Durham, Dundee, and Lancaster.

A crucial part of the team's role involves helping the RISCS Fellows undertake and promote their work, coordinating our events, helping to forge industry–university partnerships, and gathering expert input on the shaping of new research programmes and funding calls.

We will keep you up to date on all the activities and findings of the RISCS team, including our Fellows, through our website and social media accounts, and you can also keep in touch with us via email: contact-riscs@bristol.ac.uk

**Louise Evans, *RISCS Manager* and**
**Frances Pickworth, *RISCS Project Coordinator***

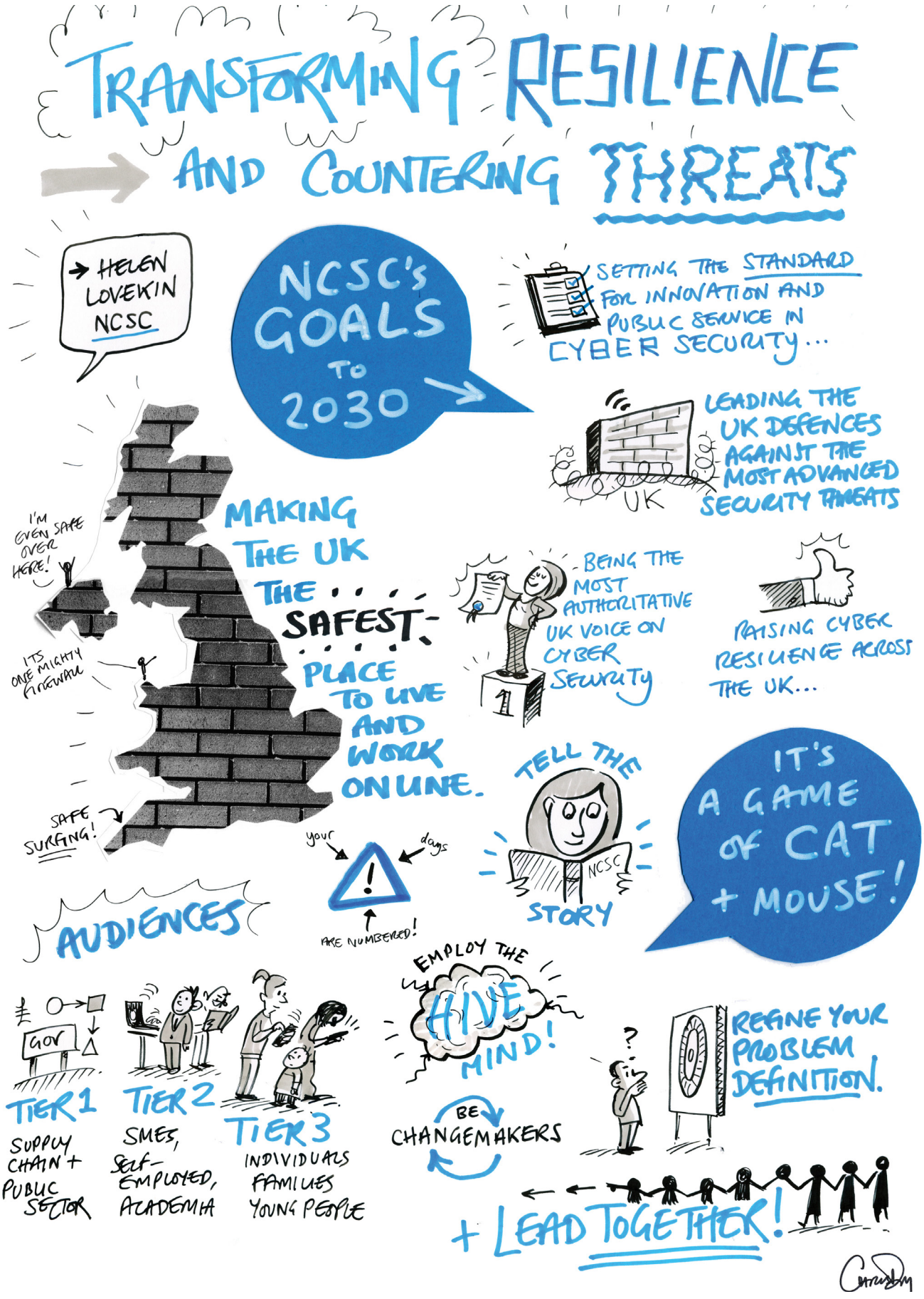
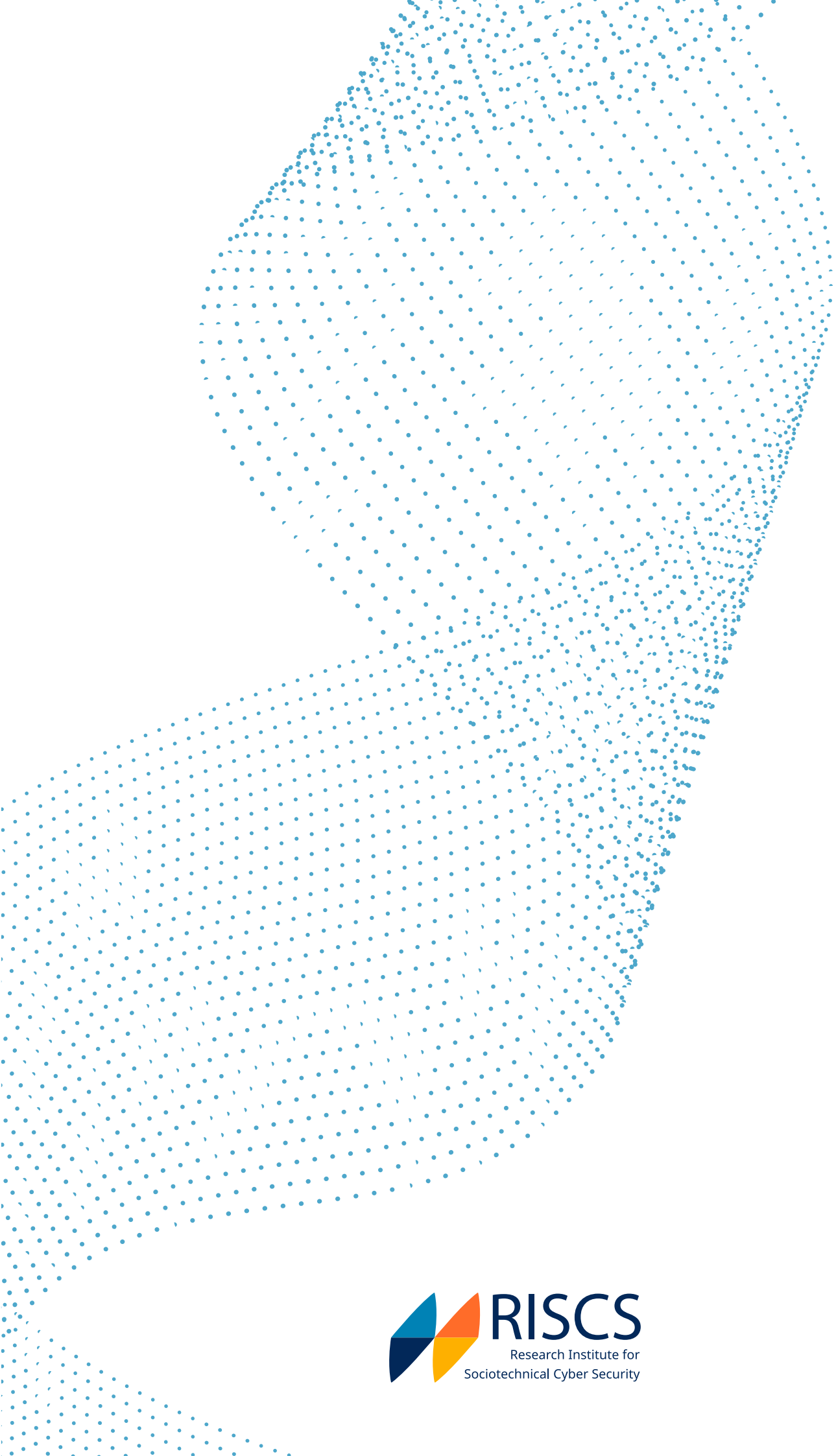



Illustration of the 2025 RISCS Annual Conference
by Chris Day, Little Creature Ltd



RISCS
Research Institute for
Sociotechnical Cyber Security