ANNUAL REPORT 2024/25

RISCS Research Institute for Sociotechnical Cyber Security

CONTENTS

FOREWORD

I have seen first-hand the value of an interdisciplinary approach for both the National Cyber Security Centre (NCSC) and the wider cyber security community. It is clear to me and to our community at large that delivering our mission requires not just deep understanding of the technologies involved, but also a profound appreciation of how technology is used in the real world, where a huge range of experts can help us understand how to have practical impact. Cyber security is sociotechnical.

As you will see from the wealth of activity outlined in this report, the RISCS team have been hard at work during their second year. I have been particularly pleased to see collaborations continue between RISCS and the other Research Institutes. Following a successful joint workshop between RISCS and RITICS (the Research Institute in Trustworthy Inter-Connected Cyber-Physical Systems) in 2024, this year RISCS joined up with VeTSS (the Research Institute on Verified Trustworthy Software Systems) to co-host a workshop exploring 'The Value of Feminism in the Theory and Practice of Computer Science and Cyber Security'. Collaborative activities like these serve to help our community see their work from a different perspective, and encourage fresh thinking.

I have also been delighted to see the continuing impact that RISCS-funded projects and activities are having at the national level. In November, RISCS Fellows were well represented at our 2024 NCSC Research Conference, with presentations on the Engineering and Physical Sciences Research Council (EPSRC)-funded project 'CyCOS: Cyber Security Communities of Support for SMEs' from Steve Furnell, Maria Bada, and Jason Nurse, as well as a session on 'Exploring Cyber Security Adoption Decision Making and Culture: Focusing on the Story Stem Method' led by Julie Gore. In December, RISCS Director, Genevieve Liveley, was invited to speak at an Industry and Parliament Dinner. And in January this year, Genevieve was joined by two of the early career researchers who contributed to the 'Universal Barriers' project to present the RISCS Framework to the Government Cyber Security Conference.

These and RISCS' wider activities highlight the central contribution that sociotechnical research can offer in tackling some of the most challenging and complex problems that we face while working together to make the UK the safest place to live and work online.

Paul Waller
Principal Technical Director – Technology Resilience, NCSC

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.

DIRECTOR'S MESSAGE

It's been another busy year for RISCS—as our Impact and Engagement Tracker for the year shows. Among the highlights that stand out for me are some of the workshops we've convened with colleagues from different NCSC teams: the roundtable discussing Market Incentives for Securing Future Technology with the NCSC Secure by Design team and colleagues from the Department for Science, Innovation, and Technology (DSIT); the workshop to stress-test our Futures Roadmap for the Government Cyber Security Strategy with delegates from the Cabinet Office, the Department of Health and Social Care, and the Department for Work and Pensions; and the Principles Based Assurance (PBA) roundtable co-hosted with HP. It was also great to see so many people from different parts of the cyber security ecosystem come together in October 2024 (just a few days ahead of the US elections) to take part in a special screening and discussion of Simon Ardizzone's documentary *Kill Chain: The Cyber War on America's Elections (HBO, 2020).* A timely (and mildly terrifying) reminder of the complexity of global cyber insecurities.

I also enjoyed taking part in an Industry in Parliament Trust Dinner at Westminster in December and discussing ideas for transforming cyber security culture in the UK so that people are empowered to be the first and the last line of defence. As the research carried out by RISCS (and others) over several years has shown us, technology-centric approaches to cyber security aren't enough on their own. Messages about good cyber hygiene, multi-factor authentication, and Cyber Essentials aren't gaining the traction needed—in part because they don't always address the bigger cultural, psychological, and behavioural influences that make people do what they do. Like the NCSC and RISCS, governments in the USA, Australia, and Netherlands are increasingly alert to the centrality of sociotechnical solutions to cyber security problems—and the latest US Federal Cybersecurity plan puts 'human-centred cybersecurity' as its top priority.

Industry and Parliament Trust dinner with Alison Griffiths MP; RISCS Director, Genevieve Liveley; and Matt Hull, Global Head of Cyber Threat Intelligence, NCC Group

2024 also brought a number of significant changes for RISCS. NCSC adopted a new model for its delivery of sociotechnical and risk expertise, moving to embed its sociotechnical specialists into priority areas across the organisation to help deliver greater impact for the wider NCSC mission. This sadly meant that, from the start of June, the dedicated specialist team that made up the Sociotechnical and Risk Group (StRG) was disbanded and John W4 and Anna G moved into new roles. The support that John and Anna gave to RISCS (along with the wider StRG team) was invaluable and, on behalf of the whole RISCS community, I want to thank both for all their hard work and dedication in championing sociotechnical research over the years—and especially for their warm and generous contributions to RISCS. *Thank you.*

There have also been internal changes within the core RISCS team. Covering for Louise, we were brilliantly supported by Yvonne Rushforth and Jenna Cox this year. Thank you both—and welcome back, Louise! Our Senior Administrator, Harriet Lloyd, moved on to another role in the University of Bristol (and we miss her greatly!). Happily, we have now appointed a new Project Coordinator, Frances Pickworth, who has previously worked with the RISCS team on events planning and report writing. Welcome back, Frances!

As you'll see from the stories that follow in this year's report, the important work that RISCS does nationally would not be possible without the ongoing contributions of its talented and hardworking Fellows. My heartfelt thanks to Professor Lizzie Coles-Kemp, Dr Matt Spencer, Professor Georgios Loukas, Professor Julie Gore, and Dr Will Slocombe for their contributions to RISCS over the last year. Our 2024 cohort of early career researchers have also made a real impact as Associate Fellows: with thanks to Dr Amel Attatfa, Dr Sophie James, Dr Partha Das Chowdry, Dr Andrew Dwyer, and Dr Becca Owens. Lizzie, Matt, Sophie, and Andrew will be continuing their Fellowships through 2025, and I am so pleased that our outgoing Fellows will continue to be part of the RISCS community as Alumni Fellows.

On behalf of the RISCS family, thank you all for everything you've done for RISCS during the last year. As seismic shifts in geopolitics, society, and technology continue to transform the sociotechnical landscape, your contributions to cyber security have never been more important.

Prof. Genevieve Liveley,
RISCS Director

IMPACT AND ENGAGEMENT HIGHLIGHTS TRACKER 24/25

Apr 2024

- **Market Incentives for Securing Future Technology Roundtable,** *London*
- **Futures Roadmap for Government Cyber Security Strategy Workshop,** *Bristol*

May 2024

- **RISCS joint RI-exhibition stand at CyberUK 2024,** *Birmingham*
- **CyberMi2: Cybersecurity and Privacy for Minority and Minoritized People, Research Conference,** *Birmingham*
- **Cyber Statecraft in an Era of Systemic Competition (CyCRAFT) Project Workshop,** American Museum and Gardens, *Bath*

Jun 2024

- **Northern Power Group Workshop, 'Securing the Future(s): Futures Literacy in Cyber Security',** *Bristol*
- **Panel: 'Is Humanity in Danger?',** *Cheltenham Science Festival*

Sep 2024

- **Principles Based Assurance (PBA) Roundtable, co-hosted with HP,** *Bristol*

Oct 2024

- **Full-day masterclass on 'Futures Thinking and Cyber: Modelling Emerging Risks' (with NCC Group and Microsoft) at COSAC Conference,** *Dublin*
- **Special screening of Simon Ardizzone's documentary *Kill Chain: The Cyber War on America's Elections* (HBO, 2020),** *Bristol*

Dec 2024

- **Capability Workshop,** *Bristol*
- **Industry in Parliament Trust Dinner,** *Westminster*

Jan 2025

- **'Universal Barriers', Government Cyber Security Conference,** *London*

Mar 2025

- **Parliamentary Roundtable on Cyber Skills and Workforce Development,** *Westminster*
- **RISCS/VeTSS workshop 'The Value of Feminism in the Theory and Practice of Computer Science and Cyber Security',** *Bristol*

UPCOMING HIGHLIGHTS FOR 2025

Apr 2025	**Cybernetic Culture Workshop,** *Lancaster*
May 2025	**‘Transforming Resilience by Rethinking the Cyber Security Ecosystem with Sociotechnical Approaches’, CyberUK 2025 Academic Panel,** *Manchester* **RISCS Annual Conference and Writers Retreat,** *Bristol*
Jun 2025	**‘Stories of Cyber Security’, Panel,** *Cheltenham Science Festival* **CyberMi2 2025: Cybersecurity and Privacy for Minority and Minoritized People, Research Conference,** *London*
Aug 2025	**Cybercrime Summer School,** *University of Strathclyde*

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

Although the security industry is often portrayed as changing quickly, some technologies take years to bring to market and will exist in the field for even longer. So, it really pays to anticipate long-term cyber resilience requirements. My experience of engaging with different stakeholders, sharing visions and assumptions, showing new security technology ideas, and iterating on feedback has given me plenty of practice with this kind of anticipatory thinking. However, I recently had the opportunity to take a very different approach: inspired by RISCS' futures thinking research, I used creative writing to explore and enhance my knowledge of the way security information flows between stakeholders. The result is the story 'Bringing rigour to security: how hard could that be?', which you can read on the RISCS website (riscs.org.uk/resources).

A good story centres on problem-solving of some kind, and the problem I focused on was how vendors can signal and explain the merits of their security solutions. Obviously, we can make marketing claims – but, given that the security market is highly contested, why should one company's narrative be trusted above those of others? Or, more broadly, how does the market decide what good security looks like? Part of the answer lies with third-party assessments and certifications – but good assessments take considerable time and skill. So, in a rapidly changing technical environment, how do we identify good assessors and good assessments?

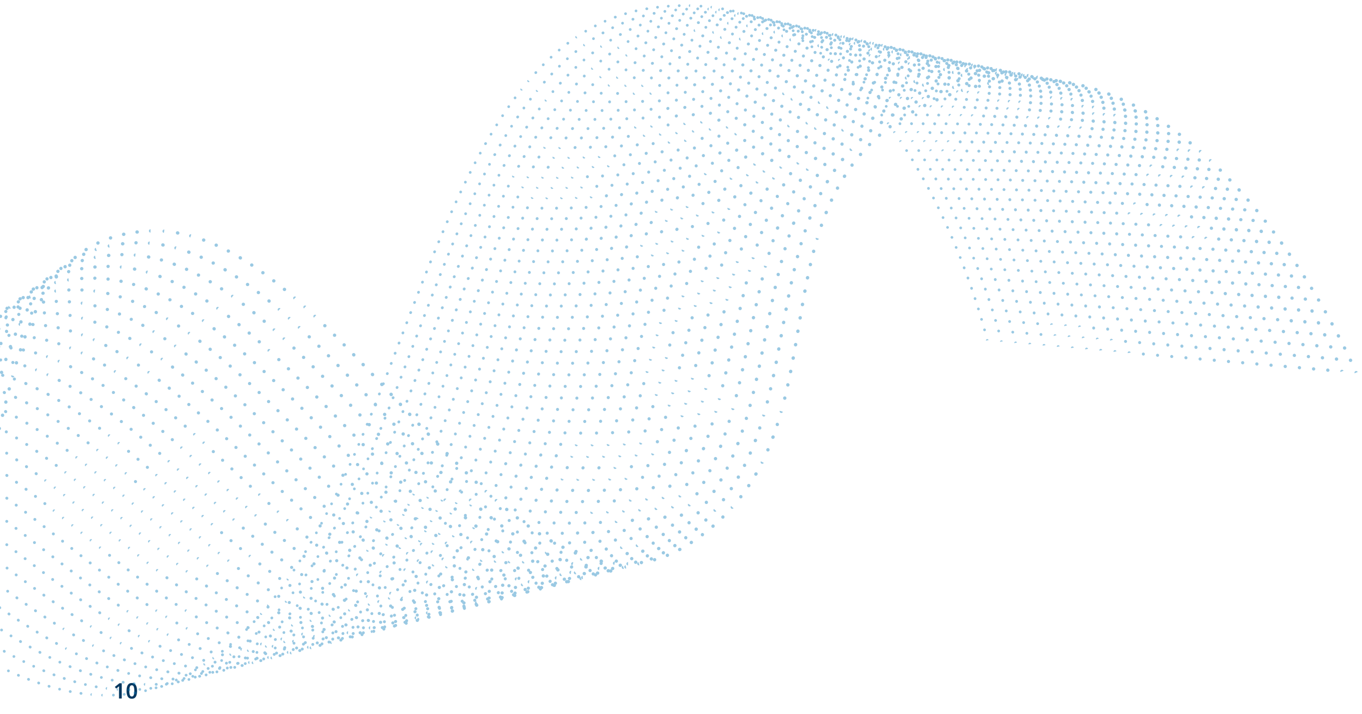
The problem of how to scale good third-party assessment is one that technical authorities are currently grappling with. The NCSC's new Principles Based Assurance (PBA) framework offers a flexible methodology that enables claims about cyber security best practice to be made and substantiated. This relatively new approach, which is being piloted and shared for feedback, provided motivation and context for the anticipation problem I wanted to explore creatively in the form of a short story.

To get started, I thought about some of the stakeholders and people involved in making security investment decisions. To narrow the scope, I focused on an enterprise customer (as opposed to a vendor, a regulator, or a consumer) and on two characters in particular: the company's Chief Information Security Officer (CISO), and an accountant who is new to both the company and the cyber security environment. We get to see some of the problems of security investment decisions through the eyes of this newcomer. I built up a picture of these two characters as people, put them in what I think are typical situations and interactions with security-related third parties, and imagined how they'd react and introspect.

I won’t interpret my own story, but I think the result expresses more than I could have said directly about the nuances of security influence and information flows. Writing the story also helped me to develop my thoughts about the different levels and kinds of impact that industry analysts can make, compared with the technical experts who provide certification.

The story was used as a pre-read for a roundtable on PBA that I co-organised with RISCS Director Genevieve Liveley and RISCS Senior Fellow Matthew Spencer in the autumn of 2024. Hosted by HP, participants included experts and leads on PBA from the NCSC as well as academics of different disciplines working on sociotechnical approaches to cyber security. The fruitful discussion enabled by this rich mix of domain knowledge, experience, and research disciplines highlighted a number of issues that had also emerged from my short story, including how to avoid disincentivising security innovation and how to get risk owners to really pay attention to risk (rather than ensure a box is ticked). I’m looking forward to seeing how this creative approach to tackling complex cyber security issues evolves. Watch this space!

Simon Shiu,
RISCS Advisory Board Member



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: UNIVERSAL BARRIERS FRAMEWORK

The Universal Barriers Framework (UBF) illustrates that systems and designs need to consider the real-world situations in which employees practise security, including when they are tired, stressed, busy, unconfident, unmotivated, and uncompliant. Using RISCS resources brilliantly co-designed with Luke Demarest, the UBF extends traditional usability thinking, presenting cyber security risks that people might encounter in their everyday lives across 11 core intersectional categories.

In January 2025, alongside RISCS Director Genevieve Liveley, we presented the UBF at the Government Cyber Security Conference to delegates from several different government departments. This provided a great opportunity to showcase the UBF to a government audience. We provided an overview of the framework followed by a more detailed explanation of two of the 11 universal barriers: awareness and trust. Our presentation led to interesting conversations with several government departments about how they might use the UBF themselves.

This experience demonstrated the accessibility of the UBF as a tool and its usefulness in supporting and extending traditional approaches to engaging with cyber security. Identifying which barriers impact individuals and departments is a key step to managing and prioritising solutions for a more effective cyber security culture.

Jessie Hamill-Stewart,
Doctoral Researcher, EPSRC Centre for Doctoral Training in Cyber Security, University of Bristol

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

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.

RISCS conference team 2024

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 cybercrime 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 2024: THEME UPDATES

1. Digital Responsibility

This overarching theme is fundamental to the success of cyber security: unless we consider digital security as a reciprocal arrangement where the needs of all parties are supported, security responsibilities can become one-sided, leading to an erosion of trust in technology and diminishing the benefits and take-up of technological approaches. The focus on Digital Responsibility is helping the RISCS community to build a more positive and healthy relationship with digital technology and advise on ways to use it that minimise harm and help to increase the benefits for all. As we digitise and connect more of our products and services, we need to be as digitally inclusive and equitable as possible—with the goal that no member or section of society is left behind.

In 2024 my main focus has been on the development of a Digital Responsibility Framework and finalising a new book on the topic as part of a new series of policy shorts from RISCS to be published by Bristol University Press (together with Professor Mark Burdon from Queensland University of Technology). The framework articulates 3 phases of digital responsibility: *realisation, establishment and enactment.* There are several digital responsibility frameworks that focus on the actioning of digital responsibility but, in this framework, we consider digital responsibility as a *process* rather than a series of actions. I look forward to reporting next year that the book has been published!

Another highlight of this year was to record 4 online seminars on the topic of 'cyber security in society' for the Virtual Routes programme: a series of introductory seminars delivered by universities in the international Virtual Routes network that are intended to widen participation in core areas of cyber security. These seminars showcase the groundbreaking work that RISCS has done in this area and are expected to be viewed by several thousand students worldwide every year. As RISCS Principal Fellow, I am thrilled to see our work being disseminated in this way.

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

2. Cyber Security Culture

Insights from the behavioural sciences and organisational psychology have a fundamental role to play in helping us to understand how to encourage better cyber security behaviours. This RISCS Fellowship theme investigated how people behave and make decisions, both individually and in groups, and across different parts of the cyber security ecosystem. This research theme was designed to help guide the RISCS community towards new insights into the psychology of cyber security, and the behaviours upon which a positive cyber security culture is built.

This year, I pursued my Fellowship theme by investigating how people behave and make decisions across different levels within large organisations. Building on previous work with Discribe+, I completed a follow-on study utilising an innovative story stem methodology, to explore sensitively our understanding of cognition and behaviour around security adoption decision-making, focusing on aspects of cyber security culture. Findings suggest that there is a fine balance to be struck in organisations between accountability, education from the most useful voices, incentives versus punishment, and value in raising challenges for cyber security in an authentic 'no blame culture'. My presentation of the findings of this study and its innovative method for data collection was well received at the 2024 NCSC Research Conference.

Julie Gore,
Birkbeck, University of London, RISCS Senior Fellow

3. Sustainable Cyber Security

Technological research in cyber security is commonly driven by short-term priorities dictated by evolving threats, technological trends, and funding availability rather than by a long-term and sustainable outlook. For a cyber security solution to be truly sustainable, it must demonstrate more than just effective performance. It should also prioritise cost-effectiveness, energy efficiency, and seamless integration with current business operations, regulatory requirements, and economic conditions. It must take into account future developments and, crucially, ensure user acceptance (and often even active user participation). This theme was designed to help researchers set targets for innovations that work both now and over the long run by prioritising cost efficiency, multidisciplinary collaboration, and the involvement of the human.

This year, I was involved in a range of cyber security initiatives where sustainability can be achieved through interdisciplinary collaboration. I represented RISCS at the Resilience beyond Observed Capabilities (RBOC) Network+ Internet of Things (IoT), Resilience and Security Forum, helping shape the debate on how IoT applications combined with AI challenge cyber security. I was also part of an EPSRC-funded project with the Universities of Greenwich, UCL, Queen Mary, Reading, and Bristol – summarised in a publication entitled 'Doing cybersecurity at home: a human-centred approach for mitigating attacks in AI-enabled home devices', which showed that non-expert citizens can be trained to recognise attacks on AI and protect themselves against them. This is now followed by a new EU-funded project (GANNDALF) and a new PhD project focusing on involving the citizen in reporting security and privacy incidents related to large language models (LLMs).

George Loukas,
University of Greenwich, RISCS Senior Fellow

4. Futures Literacy

This theme was focused around equipping the cyber security community with strategies to understand and communicate about risk and resilience. Some cyber risks we may be confident we can identify as we look to implement strategies for blocking or mitigating them; others are less clearly defined and require more consideration and analysis. Technical challenges also dovetail with complex social shifts and currents, and being aware of future trajectories and possible scenarios remains vital to understanding both risk and resilience. So, whether it is assessing the risks to data security, considering the potential impacts of emerging technology on future industry, or designing trusted automated products, it is critical that cyber security is informed by rigorous futures thinking. By supporting the RISCS community to become more 'futures literate', this theme was designed to assist in more effective decision-making as we prepare for a range of possible futures.

This year, I have continued to work on identifying potential future challenges in cyber security. This has included follow-up work from the 2023 RISCS/SPRITE+ Summer Camp, 'When Technology and Democracy Collide', dealing specifically with the issue of 'Dissent' that emerged from the Summer Camp discussions. I've been exploring some of the issues involved in facilitating legitimate dissent whilst guarding against manipulation by hostile actors in the cyber ecosystem.

Such broad thinking about cyber security – the need to consider holistically both the accuracy of data and the legitimacy of social aspects of technological change – has also featured in my contributions to socialising the RISCS Government Cyber Security Strategy Roadmap 2040 futures scenarios. My contribution to this project has involved working with other futurists to consider the whole-systems challenges that implementation of the strategy might face, both now and in the future. My research in this area suggests that the paradigm of centralisation versus distribution will have a marked effect on network and data security across a range of domains.

This year I also gave a keynote at the RISCS/DISCRIBE+ Digital Security by Design Symposium on *Narrating Futures*, in which I drew parallels between historiography and how the past is narrativised, suggested possible approaches to considering narratives of futures, and discussed the ways in which narratives can be deliberately co-opted to support particular perspectives in cyber security.

Will Slocombe,
University of Liverpool, RISCS Senior Fellow

5. Interdisciplinarity in Cyber Security

Cyber security involves—and needs—a rich variety of interdisciplinary perspectives: computing, systems theory, economics, design, communication, psychology, organisation theory, and more. The value of interdisciplinarity has become increasingly recognised in academia. However, processes of professionalisation—important forces driving the standardisation of qualifications, statuses, and roles—tend to reinforce the most mainstream forms of expertise and make it harder to recognise the value of bringing together diverse ways of thinking in professional practice. This RISCS Fellowship focuses on building our understanding of interdisciplinarity in cyber security, with particular attention to concepts and methods from the humanities and social sciences (such as communication, culture, narrative, social organisation, and behaviour).

In 2024, I published a RISCS policy report: *Assurance by Principle: Preparing for the Next Generation of Product Security Assurance.* In September 2024, I and my team followed this up with an excellent RISCS roundtable looking at the implementation of the NCSC's new PBA approach. The roundtable discussed several of the themes in the report and started conversations with other researchers and practitioners about further research needed to support policy in this area.

I have also focused on the development of a new survey for RISCS, the 'Cyber Expertise Diversity Survey', with design and engagement with stakeholders taking place in the spring and summer, and the survey running in the autumn. The survey is an exploratory exercise examining how processes of professionalisation of cyber security may shape the diversity of the cyber security practitioner community. Data analysis and write-up will take place in 2025, along with further engagement with the community to refine and communicate the findings.

I also published two open access papers on topics relevant to RISCS. The first (Spencer, M., & Pizio, D. 2024. 'The de-perimeterisation of information security: The Jericho Forum, Zero Trust, and Narrativity', *Social Studies of Science,* 54:5, 655-677) looks at the history of de-perimeterisation from a cultural/narrative viewpoint. The second (Spencer, M., Coles-Kemp, L., & Hansen, R. R. 2024. 'Navigating the Landscape of Security Modelling: The MORS Grid', *Journal of Cybersecurity,* 10:1) is a study of security modelling undertaken in collaboration with RISCS Principal Fellow, Lizzie Coles-Kemp.

Matt Spencer,
University of Warwick, RISCS Senior Fellow

RISCS PRINCIPAL AND SENIOR FELLOWSHIPS FOR 2025

Two of the RISCS Principal and Senior Fellowships from 2024 have been refreshed and continue into 2025, and three new Fellows have joined the team. In addition to Lizzie Coles-Kemp (Digital Responsibility) and Matt Spencer (Interdisciplinarity in Cyber Security), the Senior Fellows team now includes Marta F. Arroyabe (Cyber Security and SMEs), Joe Burton (Futures Literacy), and Thomas Groß (Reliable Sociotechnical Cyber Security).

To find out more about our Senior Fellows, take a look at their bios on the RISCS website.

Our Principal and Senior Fellowships for 2025 are now focused on the following five themes:

1. Cyber security and SMEs

Cyber security is a growing challenge for Small and Medium Enterprises (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 new RISCS Fellowship theme 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 important not just for their individual resilience but also for the security of entire digital ecosystems, given the role of SMEs 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 F. Arroyabe,
University of Essex, RISCS Senior Fellow

2. **Futures Literacy**

This RISCS fellowship will be focused on the 'Future of Insecurity', including 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. Joe's research in this area seeks to advance methodological, pedagogical practice in futures through data-immersive simulations, foresight scenarios, and wargaming. He will also be working on a new book project, *Artificial Intelligence and Global Security: A History of the Future*, which aims to explore how the future of AI was perceived and understood in national security communities during the Cold War and early post-Cold War environments.

Joe Burton,
Lancaster University, RISCS Senior Fellow

3. **Reliable Sociotechnical Cyber Security**

This new RISCS Fellowship theme investigates how we can reinforce practitioners' confidence in and adoption of the outcomes of sociotechnical cyber security research. Its aims are to improve the reliability of the recommendations made, to support the adoption of robust solutions, and to advance robust and evidence-based research overall. Based on research to evaluate the scientific methods of the field and to ascertain the strength of evidence achieved, the Fellowship will establish lessons learned and broader guidance regarding outcomes that hold water. In terms of core research, the Fellowship will focus on the intersection between the problem clusters 'Barriers and Incentives' and 'Usability and Trust', including issues such as supporting the adoption of privacy-enhancing technologies and understanding the latent factors impacting their perceived trustworthiness and usefulness.

Thomas Groß,
Newcastle University, RISCS Senior Fellow

4. 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 the effectiveness of security controls 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 our 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

5. Interdisciplinarity in Cyber Security

Cyber security involves—and needs—a rich variety of interdisciplinary perspectives: computing, systems theory, economics, design, communication, psychology, organisation theory, and more. The value of interdisciplinarity has become increasingly recognised in academia. However, processes of professionalisation—important forces driving the standardisation of qualifications, statuses, and roles—tend to reinforce the most mainstream forms of expertise and make it harder to recognise the value of bringing together diverse ways of thinking in professional practice. This RISCS Fellowship will focus on building our understanding of interdisciplinarity in cyber security, with particular attention to concepts and methods from the humanities and social sciences (such as communication, culture, narrative, social organisation, and behaviour).

Matt Spencer,
University of Warwick, RISCS Senior Fellow

RISCS EARLY CAREER ASSOCIATE FELLOWSHIPS FOR 2024

In April 2024 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 2024 focused on the following research themes:

- Amel Attatfa - Cyber Diplomacy and Geopolitics
- Partha Das Chowdhury - Capability and Usability
- Andrew Dwyer - Digital Decisions, (Geo)Political Economies
- Sophie James - Netnography
- Rebecca Owens - Digital Citizenship

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

Cyber Diplomacy and Geopolitics

Over the past year, my research has centred on cyber diplomatic actions within international relations in cyberspace, forming the core of my PhD in cyber security. A key contribution of my work is the development of a novel model of cyber diplomacy, highlighting the critical need for multi-stakeholder cooperation. This model advances knowledge by applying Actor-Network and Securitisation theories in innovative ways, with practical applications for real-world scenarios.

As part of my engagement with RISCS, I attended the RISCS Awayday, where I met and networked with fellow members, exchanged ideas, and contributed to the RISCS Problem Book by participating in discussions and offering input. I also co-authored Chapter 14, 'Cyber Diplomacy in the Field of Critical Infrastructure Protection', for the forthcoming Handbook on Cyber Diplomacy, examining cyber threats to critical infrastructure and diplomatic mitigation strategies. I am also currently leading a research paper on cyber diplomacy, further expanding this field.

Looking ahead, my Fellowship will continue to explore the evolving landscape of cyber diplomacy, particularly in relation to emerging technologies and geopolitical shifts, with a focus on how cyber diplomacy and AI may intersect to enhance global cyber security and international cooperation.

Amel Attatfa,
Abertay University, RISCS Associate Fellow

Capability and Usability

In December 2024, I organised a workshop on a Capability Approach to Digital Privacy and Security at which practitioners and leading academics from various UK universities gave short keynotes exploring the extent to which a capability approach can inform inclusive security engineering. We are now in the process of putting the deliberations together in the form of a special issue.

While a capability approach can point to the information necessary for inclusive security, there remains a gap in terms of how such an approach should work in practice. This year I collaborated with Karen Renaud and published a paper in the IEEE special issue on inclusive security and privacy (2024): P. Das Chowdhury and K. Renaud, 'Advocating a Policy Push Toward Inclusive and Secure "Digital-First" Societies,' in *IEEE Security & Privacy*, vol. 22, no. 5, pp. 23-31, Sept.-Oct. 2024.

Motivated by the USS data breaches affecting UK academics, I also collaborated with Karen Renaud and Awais Rashid on an extensive study that included 131 data breach victims. We proposed a paradigm called 'ethical responsibilisation', formulated by drawing from the realisation-based paradigm of justice. The paper was published at the prestigious ACM New Security Paradigms Workshop.

I participated in various policy deliberations during the past year. At Ofcom's roundtable on emerging technologies, I emphasised that an assessment of opportunities for disadvantaged groups is key to an inclusive 'digital-first' society. I was also part of REPHRAIN's (National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online) policy contributions.

I presented at the Cybernetics Culture Workshop at Lancaster University, which was organised by RISCS Associate Fellow Sophie James, and at the Rossfest Symposium at the University of Cambridge. The latter was organised in memory of Professor Ross Anderson, one of the signatories of the aforementioned manifesto on the use of a capability approach to protect against online harms. I also presented at the NCSC's annual Academic Centres of Excellence in Cyber Security Research (ACE-CSR) Conference 2025, held at Lancaster University in January.

I am currently collaborating with RISCS Associate Fellow Rebecca Owens to formulate a proposal for a workshop on cyber security and the law. The focus of the workshop will be to evaluate alternative legal frameworks for addressing aggregate harm, bringing together practitioners from cyber security and law. Our goal is to put together the deliberations in the form of an academic research output.

Partha Das Chowdhury,
University of Bristol, RISCS Associate Fellow

Digital Decisions, (Geo)Political Economies

The past year has involved examining the role of what I term as 'everyday information geopolitics' that (re)shape sociotechnical dimensions of cyber security across various scales. This has focused on three 'scenes' to understand information geopolitics at work: in examining the concept of cyber power, investigating recursive ecologies (exploring how recursion is reshaping decision in automated systems), and how cyber security becomes manifest in communities through everyday practice. My work has sought to deepen how geopolitics transcends the conventional view on the 'international' – for example, at international discussions on cyber intrusion tools (including the France and UK-led Pall Mall Process) – to shape, and be shaped by, the political economies of technology convergence, and how geopolitical activities shape communities' responses to fraud.

This has led to each strand presenting differing forms of engagement:

Cyber Power: This has included four main outputs: 1) A small research project funded by the Department for Science, Innovation and Technology (DSIT) exploring how technology convergence shapes the future(s) of cyber security; 2) I gave two talks on cyber power: First in May 2024 for the EPSRC/Dstl and RISCS project, Cyber Statecraft in an Era of Systemic Competition, on critical readings of cyber power; and second in September 2024, for the Foreign, Commonwealth and Development Office (FCDO) on UK academic perspectives on cyber power; 3) I continue to lead the Offensive Cyber Working Group (OCWG) that is developing thinking on a COP (Concepts, Organisation, and Practice) framework; and 4) I gave evidence to the UK Parliament's Joint Committee on the National Security Strategy (JCNSS) in March 2025 on 'Offensive Cyber.'

Recursive Ecologies: I have continued to engage with how automated systems – including a range of AI technologies – are reshaping sociotechnical relations. This includes a chapter published in the book 'Digital Ecologies: Mediating more-than-human worlds' examining how to consider computation through an ecological frame and deepening thinking on the concept of recursivity to understand geopolitics and a commissioned report with Dr Roxana Radu (University of Oxford) on 'Enabling Secure Democratic Ecosystems through AI.'

Everyday practice: I continued my work as Co-I on the EPSRC Equitable Privacy project, led by the University of Bristol. This work has sought to understand how equitable forms of security and privacy occur in community studybeds. This has led to the acceptance of a CHI (Conference on Human Factors in Computing Systems) paper – 'Friend or Foe? Navigating and Reconfiguring "Snipers' Alley"' – to be presented in May 2025. This paper explores how communities experience and respond to fraud through actors' security systems and 'dark patterns.'

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

Netnography

One of the highlights of the year was conceptualising and securing funding for the Cybernetic Culture Workshop: Consumption, Security & Society in the Digital Age which will take place in April 2025 at Lancaster University. This innovative one-day event will provide a platform for critical, interdisciplinary discussions on how digital consumption can have implications for security practices, and vice versa. By inviting contributions from a broad range of fields spanning cyber security, consumer behaviour, digital culture, and social harm, the workshop aims to explore the complex socio-cultural dynamics of digital spaces. With over 18 speakers from world-leading UK institutions (e.g. Bath University, University of Bristol, University of Exeter, University of Strathclyde, Bournemouth University, Leicester University, and others) the event promises to be an exciting and productive gathering of expert researchers fostering collaboration and new insights at the intersection of technology, society, and security. An ISBN has been granted by Lancaster University's Library for the published proceedings of the conference so that these will be made publicly available in print and online.

Since completing my PhD, I have also been advancing my research with an online ethnography for an upcoming paper on the dark and uncanny 'corners' of the web and how these have attracted touristic attention. This study critically examines the socio-cultural dynamics that shape online spaces and produce cyber forms of dark tourism which may have implications for consumer well-being and security practices. The work highlights the need for an interdisciplinary perspective in understanding these complex environments. The work is currently in the writing-up phase and seeks to shed light on how cultural and psychological factors drive digital behaviour and impact cyber security. An abstract has been submitted to the Academy of Marketing Conference 2025 and the fuller manuscript is intended for submission to a world-leading academic journal.

Additionally, I was honoured to present at the FACTOR (Forensic Linguistics, Cybersecurity, and Technology Research) Lecture Series, where I explored the intersection of online communities, memetic culture, and security. Lastly, I co-organised and co-led Lancaster University's participation in the Lancashire Cyber Education Week 2025, contributing to an initiative that engaged young people within the growing cyber sector. It was inspiring to see the students so absorbed and excited, learning in such a dynamic way; through the activities I co-designed, they didn't just observe the work of cyber professionals, academics, and practitioners – they became a part of it.

Sophie James,
Lancaster University, RISCS Associate Fellow

Digital Citizenship

As a RISCS Associate Fellow, I have been able to advance critical research on cyber security and privacy, fostering interdisciplinary collaborations to develop policy-driven solutions that address complex online harms. The RISCS network has provided an invaluable platform for knowledge exchange, facilitating the development of innovative, multidisciplinary research initiatives in collaboration with leading experts, including RISCS Associate Fellow Dr. Partha Das Chowdhury.

My engagement with RISCS has included presenting research at the RISCS-sponsored CyberMi2 Research Day, where I contributed to key discussions on strengthening digital security and privacy resilience. Beyond this, my work continues to explore the evolving landscape of complex online harms and to develop strategies that empower citizens in the digital sphere. A notable example is the Economic and Social Research Council Festival of Social Science event I organised at Newcastle City Library, where I employed interactive arcade machines to educate citizens on their informational rights.

Rebecca Owens,
Newcastle University, RISCS Associate Fellow

Participants at CyberMi2: Cybersecurity and Privacy for Minority and Minoritized People, Research Conference, Birmingham

CybeMi2 Research Day 2024
AGENCY RESEARCH
RISCS Research Institute for Sociotechnical Cyber Security
2nd CyberMi2 Research Day, 2024
Cybersecurity and Privacy for Minority and Minoritized People
https://sites.google.com/view/maryammjd/cybermi2-2024
Friday, 24 May 2024, The Exchange, University of Birmingham, UK

RISCS EARLY CAREER ASSOCIATE FELLOWSHIPS FOR 2025

In January 2025 we appointed three new early career researchers to enhance our team of RISCS Associate Fellows. Sophie James and Andrew Dwyer from the 2024 cohort continue their Fellowships and are joined by Sana Belguith (University of Bristol), Oishee Kundu (University of Bath), and Bianca Slocombe (Coventry University).

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

- Sana Belguith – AI, Space and Cyber Security
- Andrew Dwyer – Digital Decisions, (Geo)Political Economies
- Sophie James – Netnography
- Oishee Kundu – Markets and Technology Futures
- Bianca Slocombe – Psychology and Cyber Security

You can find out more about our new and continuing Associate Fellows on the RISCS website.

RISCS PHD STUDENT PLACEMENTS FOR 2024/25

UX Design as a Hooking Tool in Baby Tracker Apps

My research was part of a placement with RISCS, which provided me with the opportunity to explore UX Design as a Hooking Tool in Baby Tracker Apps. It investigates how user experience (UX) design in baby-tracking apps (BTA) is intentionally crafted to influence user behaviour, often serving the business interests of app developers. Drawing insights from industry guidebooks, I analyse how app designers utilise psychological principles to ‘hook’ users, fostering habitual engagement that encourages frequent interactions with the app. While such methods are common across digital platforms, their application in parenting apps raises ethical concerns, as new parents seeking support may be particularly vulnerable to these persuasive techniques.

By examining two industry guidebooks and their influence on three widely used BTAs, I identified UX strategies grounded in behavioural psychology, including habit formation models, variable rewards, and heuristics-based decision-making. These techniques—framing effects, scarcity tactics, and aesthetic usability—subtly drive users toward increased engagement and data input, sometimes leading to dependency-like behaviours. While these tools can enhance usability, they also underscore the fine line between assisting users and manipulating them.

This research emphasises the importance of increased awareness and regulatory dialogue to ensure that UX-driven engagement prioritises user well-being over commercial interests. It highlights the necessity of balancing innovation with ethical responsibility, especially in technologies aimed at vulnerable user groups.

I sincerely thank Prof. Genevieve Liveley for her invaluable guidance, Dr. Maryam Mehrnezhad for her support, and the RISCS community for their remarkable work in researching such an essential area to make the internet a safer place. My appreciation extends to the SWWDTP UKRI AHRC Fund for their financial support, as well as to the young parents whose experiences have deepened my understanding of this issue.

Haya Sheffer,
Doctoral Researcher, University of Reading and Cardiff University,
South West and Wales Doctoral Training Partnership (SWWDTP)

The changing landscape of international relations and an increasingly fragmented internet

In the Summer of 2024, I worked with RISCS for two weeks, on two projects: (1) conducting a series of interviews on the subject of ethical regimes in cyber security; and (2) participating in the 2024 workshop on Cyber Statecraft in an Era of Systemic Competition. Reflecting on the former, I am pleased with the amount of ground we were able to cover in terms of situating ethical concerns in the triple helix, and had some success theorising about the presence of a shared ethical order of value underpinning national security concerns in academic, government, and industrial spaces.

Reflecting on the latter part of the placement, it was fascinating to get a snapshot of a field so dramatically in motion. Since May 2024, the UK's place in the world has become ever more precarious, and interest in effective cyber statecraft has altered and intensified as a result, but the implications for the multistakeholder approach remain muddy and complex.

In addition to being a great opportunity to get involved with a very active research community, both of these experiences did a lot to refocus my own research, which has turned towards the question of how states use the academy as a tool for building cyber capacity by securing valuable patents, knowledge, and coveted niches within the global supply chain. The small but growing body of associated literature at the intersection of cyber security and knowledge security points to a new theatre for international conflict, and one with drastic and potentially alarming implications for academics and internationalisation. All told, it was a great pleasure to work with RISCS, and I am very glad to have played some small part in filling out the map of how states navigate cyberspace.

Kester Brookland,
Doctoral Researcher, EPSRC Centre for Doctoral Training in Cyber Security, University of Bristol

CYCOS: ENHANCING CYBER RESILIENCE OF SMALL AND MEDIUM-SIZED ENTERPRISES (SMES) THROUGH CYBER SECURITY COMMUNITIES OF SUPPORT – RISCS PROJECT UPDATE

Led by Prof. Steven Furnell (University of Nottingham), in collaboration with Dr Maria Bada (Queen Mary University of London) and Dr Jason Nurse (University of Kent), the 30-month CyCOS project seeks to investigate and enhance the cyber security support provided to SMEs.

The project is now entering the final year of activity, with the work to date having successfully engaged with both the SME community and various cyber security providers and advisory sources that provide existing support to this audience. This has included the establishment of further collaborative relationships, with both the Federation of Small Businesses and the National Cyber Security Centre now having been added to the project and its advisory board.

In the most recent period, the team has been working to capture experiences from SMEs and advisors in order to better understand their support journeys – examining questions such as what prompts support to be sought, and what happens as a result. The project is ultimately working towards piloting of the Community of Support approach, and current work is underway to lay the foundations for this, designing the operational principles and providing interested SMEs with related upskilling via ISC2 Certified Cybersecurity training and certification.

Dissemination and awareness-raising activities have continued throughout the year, with 15 invited talks and panel contributions at a variety of events both in the UK and beyond. Examples included talks at UK Cyber Week, the Frankfurt Tech Show, and the ISG Business Summit, and panel contributions at the International Cyber Expo and the Global Cyber Security Capacity Centre Annual Conference. We have also contributed to online events, including SME-focused online panels in the teissTalk and Infosecurity Magazine webinar series, and a presentation in the ISC2 webinar series. In terms of academic outputs, a paper from the early work from the project was presented at the Human Aspects of Information Security and Assurance (HAISA) 2024 conference, and two further papers are currently in review. The HAISA paper will also be further developed as an invited journal paper.

We have also hosted our own engagement event as part of our planned dissemination activities, with the East Midlands Cyber Security Communities of Support Conference having been held in October 2024. This saw attendance from various local SMEs and cyber providers, and input from various CyCOS partner organisations including CIISec, the Cyber Resilience Centre for the East Midlands, IASME, and ISC2.

Steve Furnell,
University of Nottingham

CYCRAFT: CYBER STATECRAFT IN AN ERA OF SYSTEMIC COMPETITION – RISCS PROJECT UPDATE

Funded by EPSRC and Dstl with RISCS support, the project, ‘Cyber Statecraft in an Era of Systemic Competition’ (CyCRAFT) began at the end of 2023 and is now in its second and final year. It responds to UK government efforts to develop a 21st-century approach to foreign policy, diplomacy, and governance in and through cyberspace – a suite of efforts we characterise as ‘cyber statecraft’. Led by King’s College London in collaboration with researchers from the University of Bath and the Royal United Services Institute (RUSI), it has continued its work to understand the challenges governments face in developing 21st-century approaches to cyber statecraft. Specifically, the project aims to develop concepts and frameworks for understanding and promoting the UK’s international engagement in cyberspace for the next decade and beyond.

Project members have been working to theorise and explain the central concept of ‘cyber statecraft’, understand how the UK and other middle powers conduct their cyber statecraft activities, evaluate ‘cyber power’ quantitatively, and explore the role of the private sector in cyber statecraft. They have given conference papers, drafted academic articles for peer review, published reports (such as for the Carnegie Endowment for International Peace), and written op-eds and commentaries for various media outlets. Video commentaries by our researchers have been viewed over 10,000 times.

The project has benefited immensely from wide stakeholder engagement. In the UK, we have held workshops with government, industry and civil society to discuss the present and future of UK cyber statecraft. Project personnel have hosted experts from India, Brazil and South Africa. Our dedicated public events programme has showcased national and international expertise, with nearly 2,000 attendees.

For the remainder of the project, we will continue with our public engagement activities, complete our evaluation model for cyber power, push academic articles to publication, and begin feeding back our findings to UK government and others.

Tim Stevens,
King’s College London

The CRC Model
Working with businesses
Working with University talent
Supporting SMEs
Security alerts Guidance, & Services

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT
WWW.CYCOS.ORG
University of Nottingham
Queen Mary University of London
University of Kent
Engineering and Physical Sciences Research Council
RISCS

CyCOS conference and exhibition, October 2024, University of Nottingham

Please assess the following elements and assign relevance based on whether they form the definition of cyber power (NA = not part of cyber power definition):

Participants at a CyCRAFT workshop exploring UK cyber power, Bath

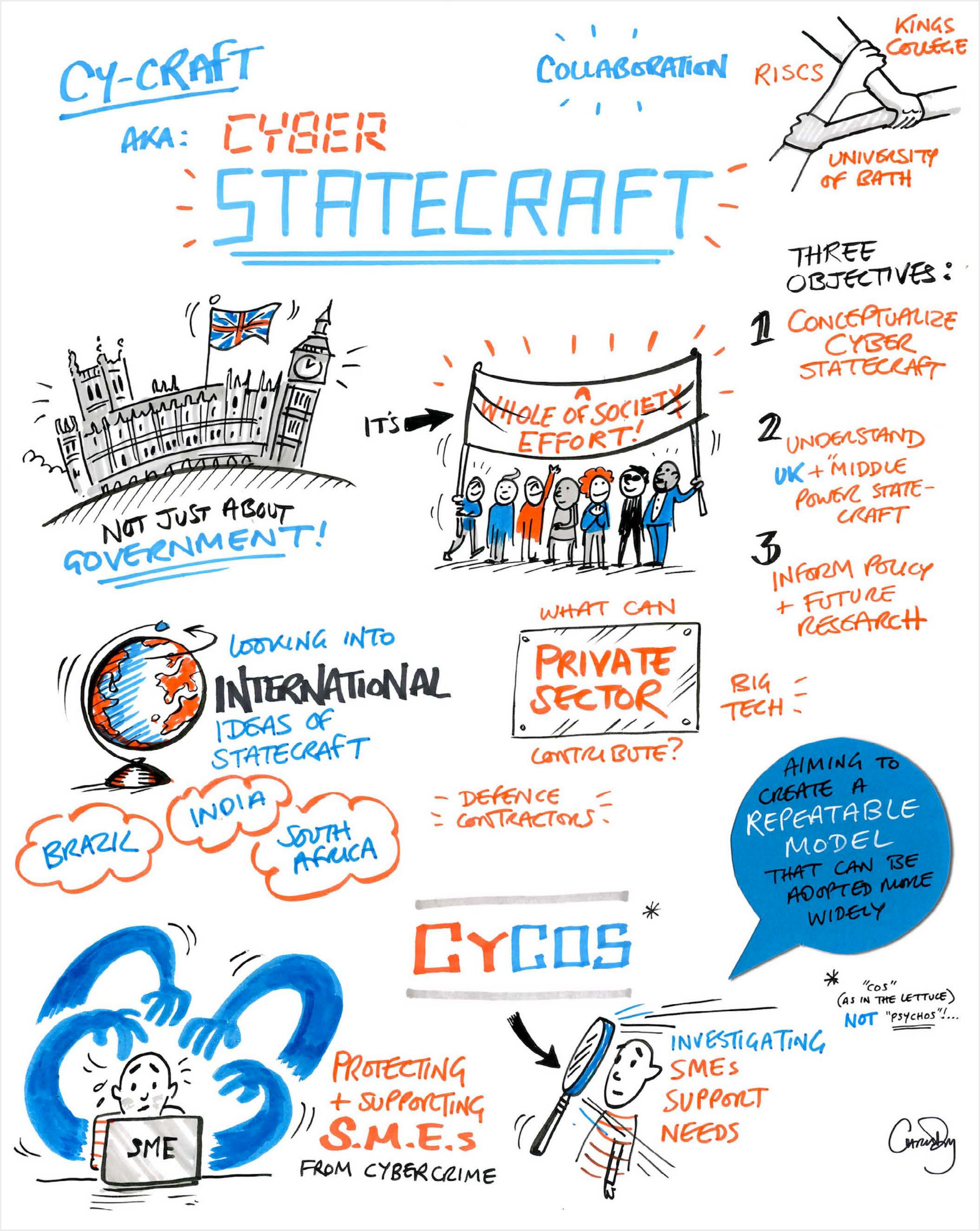

CY-CRAFT
AKA: CYBER STATECRAFT
COLLABORATION
RISCS
KINGS COLLEGE
UNIVERSITY OF BATH
THREE OBJECTIVES:
1 CONCEPTUALIZE CYBER STATECRAFT
2 UNDERSTAND UK + "MIDDLE POWER" STATE-CRAFT
3 INFORM POLICY + FUTURE RESEARCH
NOT JUST ABOUT GOVERNMENT!
IT'S
WHOLE OF A SOCIETY EFFORT!
LOOKING INTO INTERNATIONAL IDEAS OF STATECRAFT
BRAZIL
INDIA
SOUTH AFRICA
WHAT CAN PRIVATE SECTOR CONTRIBUTE?
BIG TECH
DEFENCE CONTRACTORS
AIMING TO CREATE A REPEATABLE MODEL THAT CAN BE ADOPTED MORE WIDELY
CYCOS*
* "COS" (AS IN THE LETTUCE) NOT "PSYCHOS"!...
SME
PROTECTING + SUPPORTING S.M.E.s FROM CYBERCRIME
INVESTIGATING SMEs SUPPORT NEEDS
ChrisDay

Illustration by Chris Day, Little Creature Ltd

MANAGER'S AND PROJECT COORDINATOR'S MESSAGE

In October 2024 Harriet, our brilliant Senior Administrator, moved on to a new role at the University of Bristol. Happily, Frances joined the team as our new Project Coordinator in February 2025 and is now working alongside Louise to support Genevieve, the Fellows, the Advisory Board, and our ever-growing community in delivering the RISCS mission.

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*

RISCS

Research Institute for
Sociotechnical Cyber Security