ANNUAL REPORT 2023/24

RISCS Research Institute for Sociotechnical Cyber Security

CONTENTS

FOREWORD

As you will see from the breadth and depth of activity outlined in this report, the new RISCS team hit the ground running during their first year.

The team has been building on the achievements and legacy of the RISCS community, whilst extending and deepening expertise and areas of interest within cyber security. For example, the RISCS Fellowship programme has been updated to address cyber security aspects of emerging priorities for the UK, such as sustainability and net zero. RISCS has also taken advantage of the new Research Institute funding model to develop strategically important projects for the Cabinet Office.

I am particularly pleased to see developing collaborations between RISCS and the other Research Institutes during the last year. Each RI was set up to develop security capability in strategically important areas; defining problem spaces and building communities of interest and talent to tackle some of the most challenging problems in cyber security. As the scale and complexity of these problems grows, their interconnected nature is becoming more apparent. Understanding and responding to these will increasingly require a collective and multidisciplinary approach. Naturally, this is something where we anticipate that RISCS and their community will be able to make a significant contribution along with partners in the other RI communities.

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.

INTRODUCTION

During the last year it has been exciting to work with the RISCS team on delivering the blueprint laid out at last year's Annual Conference.

A significant part of this has been refreshing the structure and content of the RISCS Fellowships. This meant identifying and recruiting new Fellows to engage with a range of significant themes for sociotechnical security, including sustainability, interdisciplinarity, and culture.

I'd like to welcome Dr Matt Spencer, Professor Georgios Loukas, and Professor Julie Gore to these new roles within RISCS—I'm really looking forward to their contributions in these priority areas.

I'd like to place on record our thanks to Dr Tim Stevens, Dr Maria Bada, and Dr Anna Cartwright for their fantastic work on International Relations, Cybercrime, and Quantification and Cyber Risk.

I have seen first-hand the value of this work both for NCSC and the wider cyber security community. I am especially grateful that they will continue to be part of the RISCS community as Project Fellows.

A second aspect of this blueprint has been the change to a new funding model for RISCS, along with the rest of the NCSC's research institutes. As part of this, RISCS has received funding from the Cabinet Office to deliver a series of high-profile projects, including:

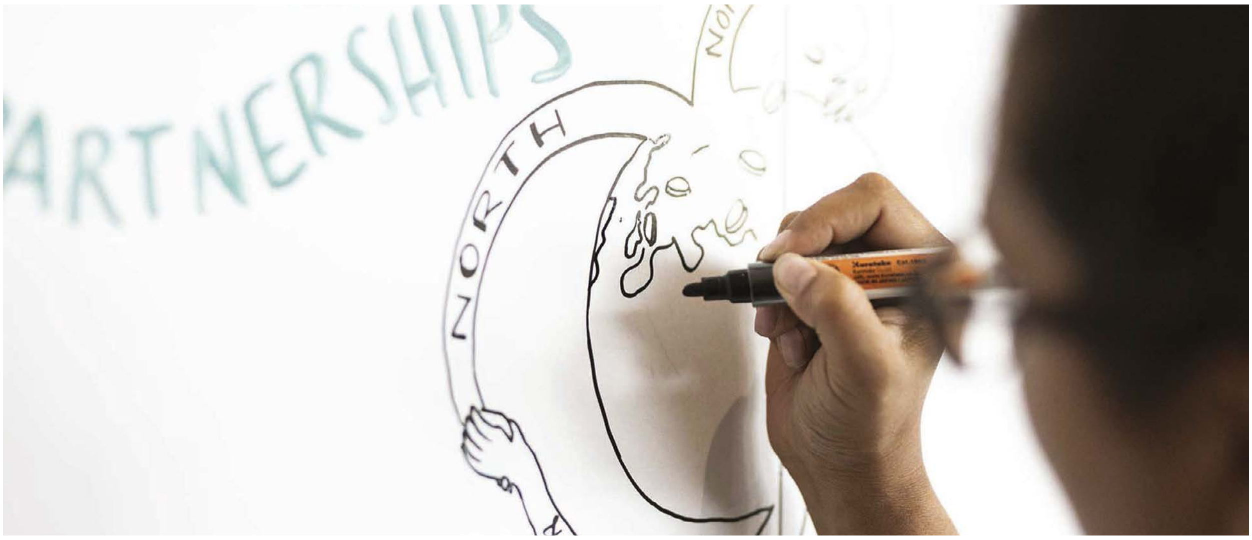
- a futures roadmap for the Government's Cyber Security Strategy to 2030;
- an evidence-based review of the current state of cyber risk quantification; and
- developing our capability to assess cyber security implementations for human factors and risks using the 'Universal Barriers Framework'.

All three of **these ambitious projects underline the growing importance of sociotechnical research in cyber security and the increasing influence of this thinking at the heart of the UK Government.**

Allied to the new funding model has been a desire for the NCSC research institutes to work collaboratively in the future. Again, **RISCS has been leading the charge on this front, running the first cross-RI workshop with RITICS in January, to explore potential joint research proposals around strategic priorities—such as Net Zero—with stakeholders from government, academia, and industry.** Please watch this space...

A final point I wanted to make is the continuing impact that RISCS-funded projects and activities are having in the wider world. This can be seen in the submission that the RISCS community provided to the AI summit organised by Downing Street in November 2023. It is also visible in the RISCS-funded research into 'Cyber Insurance and Ransomware' and 'Ransomware Harms'. Both of these projects have influenced the policy agenda at the national and international level, and both show the central contribution that sociotechnical thinking can make to some of the most challenging and complex problems that we face in making the UK the safest place to live and work online.

John W5,
Sociotechnical Research Lead,
Sociotechnical and Risk Group, NCSC



DIRECTOR'S MESSAGE

It's hard to believe that RISCS moved to its new home in Bristol only a year ago. It's been quite a year! There have been several highlights that particularly stand out for me. The RISCS 'Grand Challenge' at last year's Annual Conference, where we successfully demonstrated that the RISCS community is considerably smarter than ChatGPT. The ChelTechne AI Summit, convened in collaboration with Plexal and the Cheltenham Science Festival, which included a sumptuous 'Mad Hatter's Tea Party' and set the trend for other AI Summits (or, so we like to think). The Futures Summer School, 'When Democracy and Technology Collide', convened in partnership with SPRITE+. The RISCS/RITICS workshop on 'Net Zero, Sustainability, and Cyber Security'. And the RISCS Early Career Researcher Workshop at Royal Holloway, where it was great to see early career researchers from different universities and disciplines (including arts, humanities, and social sciences) join in conversation about the future of cyber security and the role of their research within this space.

I've also been delighted to see the successful funding awards achieved by so many of our Fellows. Congratulations to our former Senior Fellow, Tim Stevens, as Principal Investigator for the new EPSRC/Dstl-funded project, 'Cyber Statecraft in an Era of Systemic Competition'. And to Steve Furnell as Principal Investigator for the new EPSRC-funded project—'CyCOS: Enhancing Cyber Resilience of Small and Medium-sized Enterprises through Cyber Security Communities of Support'—on which he'll be working alongside former Senior Fellow Maria Bada, and RISCS Advisory Board Co-Chair Jason Nurse. Look out for updates on both of these major projects on the RISCS website.

I also want to thank a few people whose contributions to the RISCS mission are changing this year. Emma Moreton steps down as Co-Chair of our Advisory Board, and Adam Shostack shifts gear slightly in a move from Advisory Board member to Honorary Fellow.

Tim Stevens, Maria Bada, and Anna Cartwright become Project Fellows.

The RISCS research team has also been complemented by the energies and insights of three talented early career researchers undertaking short-term placements with us this year: Alexander Kopsch, working on 'Cyber Security and Government Policy'; Nerida Brand, working on 'International Perspectives on Cyber Security Education in Schools'; and Haya Sheffer, working on 'Contemporary Self-Tracking Techniques'.

On behalf of the RISCS family, thank you all for everything you've done for RISCS during our busy first year. I am excited to see what we can all do as we now move into our second year.

Genevieve Liveley,
RISCS Director

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
towards knowledge exchange, and research itself

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

ADVISORY BOARD INSIGHT

Teetering on the Edge: The Relationship Between Insurance and Cyber Security

In 2024 many territories and domains are now considering or enacting legal instruments with respect to cyber security, such as new regulations and laws; instruments which place obligations on legal entities, including companies and individuals, that will endure through time.

For the first time, legal entities are having to understand and resource the through-life cost of cyber safety in their products and services.

However, the role of insurance in making these legal instruments and others economically sustainable is often misunderstood.

There has been a tendency in academic circles to concentrate on 'cyber insurance' as a stand-alone product, and it has often been overlooked that much of the insurance that might be invoked in the event of a cyber incident already exists within all-risk general insurance products.

In the insurance world—following incidents such NotPetya and WannaCry, where the insured losses were estimated at $3.6bn globally—the insurance industry worldwide took steps to understand and manage the risks that they were covering, and particularly to understand unintended liabilities arising from cyber attacks. Their realisation was that a significant proportion of the $3.6bn arose from areas where the policies were 'silent, non-affirmative'.

Simply put, where no explicit cyber exclusion applies, coverage for losses caused by cyber perils might apply even when that coverage was not intended.

The potential exposure to aggregated losses at this scale and above was one of the major issues for the viability of the (re)insurance industry; so, between 2016 and 2019, the UK Prudential Regulatory Authority (PRA) conducted an investigation. The subsequent engagement involved a range of stakeholders—including insurance and reinsurance firms, (re) insurance intermediaries, consultancies, catastrophe-modelling vendors, cyber security and technology firms, and regulators—and resulted in an expression of concern about the materiality of 'silent' cyber as a risk to (re)insurance companies. It also recommended that firms needed to identify clear ways of managing silent cyber risk, setting clear appetites, defining strategies that would be owned by boards, and investing in cyber expertise.

Supervisory Statement SS4/17 set out expectations of firms regarding cyber insurance underwriting risk. It recommended that, from January 2019, all UK-regulated insurers 'should have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover.' [Cyber insurance underwriting risk - SS4/17 (bankofengland.co.uk)]

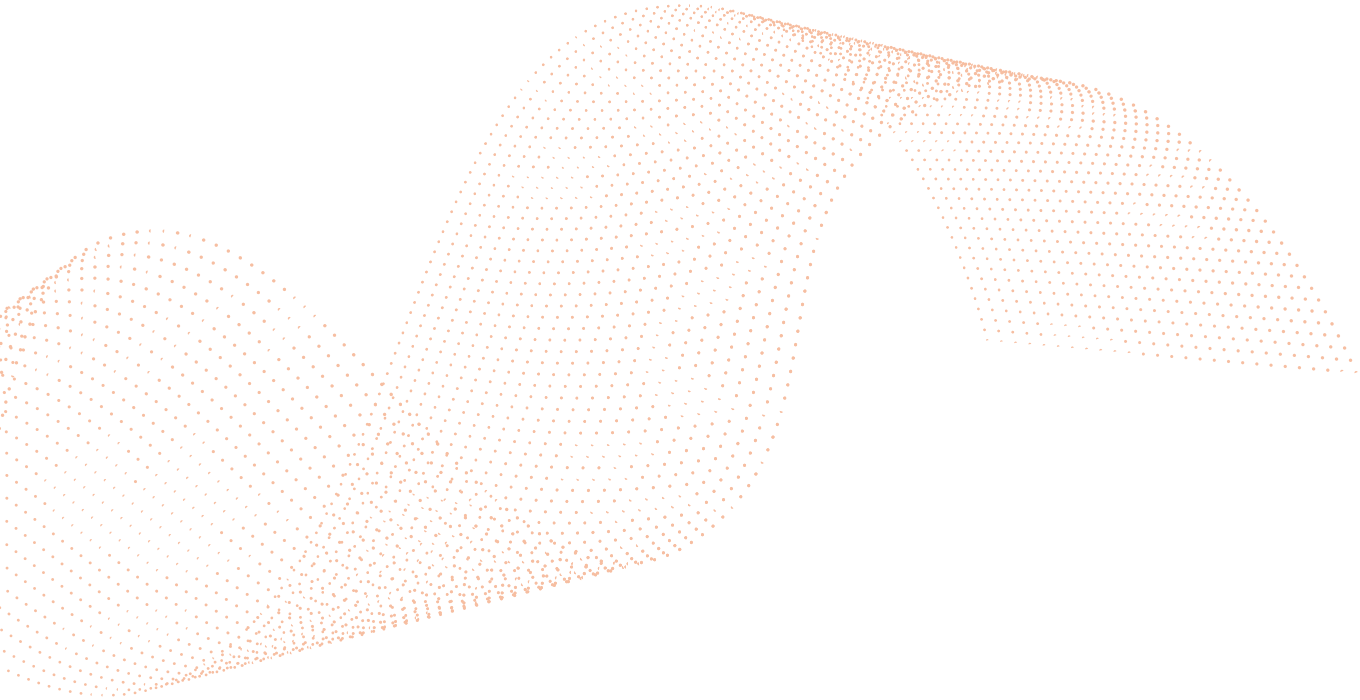
Arising from this, **a representative motor insurance policy now includes exclusions along the lines of 'mechanical, electrical or computer failures (including failures caused by computer virus or cyber attack)'** and defines 'cyber attack' as:

'Any unauthorised, malicious or criminal act or series of related unauthorised, malicious or criminal acts, regardless of time and place, or the threat or hoax thereof involving access to, processing of, use of or operation of any computer or electronic system that results in physical damage or loss of property or data.'

The effects for car drivers of this costed accountability upon cyber and insurability are far-reaching. Firstly, whilst it is a legal requirement for the claimant to have insurance, in the event of a cyber attack the vehicle is no longer insured.

Secondly, and of greater potential consequence, the systemic risk being borne by (re)insurance for the automotive industry as a sector likely contravenes financial probity requirements. **It may well be, in the near future, that this financial exposure, driven by a global exposure to cyber attacks, will lead to the withdrawal of critical and legally required aspects of our society upon which we all rely.**

Peter Davies,
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

In our 2022/23 Annual Report, Irfan Hermani (DSIT) reported on the contribution that RISCS research was already helping to make towards meeting the goals of the UK Government's 2021 National Cyber Strategy:

> ***"What RISCS is doing will be crucial to meeting the ambitions laid out in the National Cyber Strategy. Novel and high quality research, and bringing together a broad range of unique stakeholders, will be critical in making the UK the safest place to be online, in enabling us to capitalise on the opportunities, and in solving the challenges of cyber security."***

In the last year we've continued our efforts in this area and have been working hard on three projects designed to help support the Government Cyber Security Strategy 2022-2030.

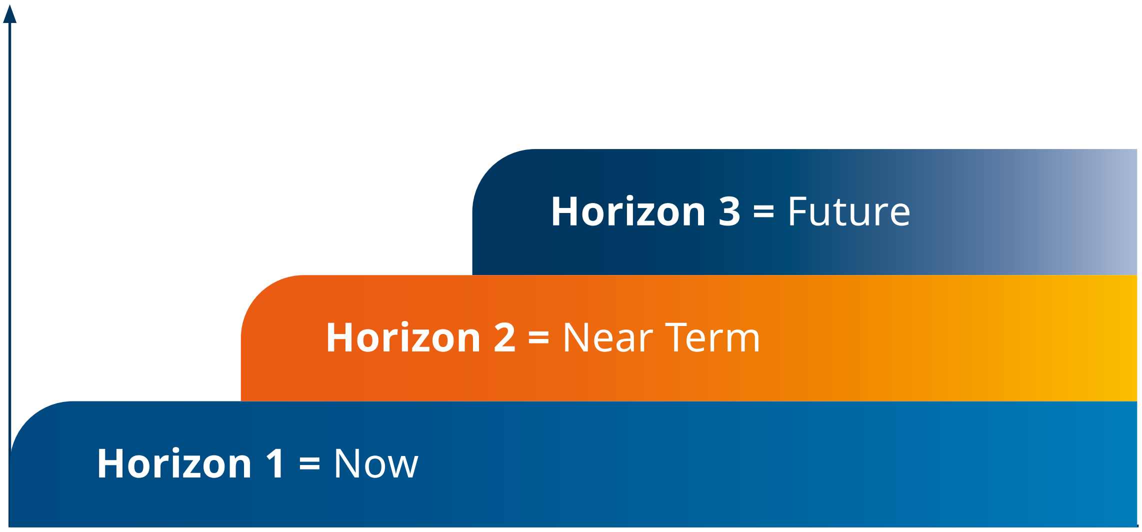
1. An evidence-based roadmap informing acceleration towards the Government's Cyber Security Strategy vision for **'All government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030'.**
2. A critical and evidence-based review of cyber risk quantification to inform the increasingly diverse set of cyber risk management challenges that the UK faces.
3. A project using the 'Universal Barriers Framework' to explore universal accessibility as a security need and to help government organisations recognise, understand, and manage the human risk factors across their cyber security operations.

These projects, together with RISCS's wider programme of research and activities, will help to support the two core and complementary strategic pillars which define the government's approach to cyber resilience in its Cyber Security Strategy:

- **building organisational cyber security; and**
- **defending as one.**

RISCS RESEARCH CHALLENGES: THREE HORIZONS

RISCS uses a traditional 'Three Horizons' model to help identify its research priorities.



Horizon 1: Challenges Now

The NCSC and other key stakeholders present RISCS with urgent research questions and rapid response projects that speak to present priorities, emerging problem spaces, developing gaps, and key topics leading on from previous research. The responsive character of these research challenges means that projects are typically led by the current cohort of RISCS Fellows. Examples of 'first horizon' research priorities for RISCS include:

- Security Culture
- Supply Chain
- Quantifying Risk
- Universal Barriers for Cyber Security
- Phishing
- Cyber Security Futures

Horizon 2: Challenges in the Near Future

The Steering Group, Advisory Board, and Fellows help to identify, refine, and mature key research topics, including problem areas where emerging technology threatens to escalate harms and risk. Fellows are supported by RISCS to develop their themes into externally funded longer-term research projects. Fellowship Themes are also reviewed annually and priority areas and tangible research questions are identified by the RISCS Steering Group and Advisory Board. Examples of 'second horizon' research priorities for RISCS include:

- Inclusive and Equitable Cyber Security
- Sustainable Cyber Security
- Quantification and Cyber Risk
- Ransomware and Cyber Insurance
- Responsible and Ethical Cyber Security
- Global Cyber Security
- Secure by Sociotechnical Design
- AI/LLM-Enabled Cyber Harms

Horizon 3: Longer-Range Challenges

The Steering Group, Advisory Board, Fellows, and wider community of interest help to horizon-scan for emerging, developing, and erupting challenges. This futures work features as a standing item at our Annual Conference, enabling the wider community of interest and expertise (from academia, policy, business, and industry) to share their foresight via contributions to an annual 'Grand Challenge'. Examples of 'third horizon' research themes from the March 2023 RISCS Grand Challenge include:

- Building Responsible and Equitable Systems
- Communicating Cyber Security and Risk
- Designing Trustworthy Services and Products
- Measuring Cyber Security
- Anticipating Future Risks, Opportunities, and Threats from AI/LLMs

RISCS PRINCIPAL AND SENIOR FELLOWSHIPS FOR 2023: THEME UPDATES

The RISCS Principal and Senior Fellowships for 2023 focused on the following themes:

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.

This year, having established the research agenda for this theme, Lizzie worked on a pilot project to explore how responsibilities are realised, established, and actioned in the case of assisted access (where voluntary and third-sector organisations support individuals to securely access online services). She worked on a pilot study in the North East of England and took the learning outcomes from that study to work with NCSC in two workshops to explore how responsibilities related to digital assistance were actioned through the adoption of digital technology policy, regulatory compliance, and technological practice. The workshop design included UX techniques such as the use of personas, user journeys, and storyboarding. The results of the workshop foregrounded the importance of relationships and relational support in establishing and actioning digital responsibilities related to secure service access and data protection. In particular, the workshops revealed how the security of these relationships is based on a negotiated set of responsibilities between all parties involved. As a follow-on to these workshops, NCSC is in the process of developing approaches to 'cyber security for all' that include digital responsibility as a central concept, and Lizzie is supporting RISCS in its 'Universal Barriers' project.

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

2. Cybercrime

Understanding how people behave—both individually and in groups, and across different parts of the cyber security ecosystem—is a priority for the cyber security research community. This includes understanding people whose intentions are non-malicious and who simply want to do a good job, and those who inadvertently find themselves acting as 'accidental insiders', as well as the intentions, drivers, and behaviours of those who have more malicious aspirations. This research theme has helped to guide the RISCS community towards new insights into understanding both the perpetrator and the victim, exploring topics such as insider threat, online harms, and support for victims of cybercrime.

In September 2023, Maria participated in the Annual Conference of the European Society of Criminology (EUROCRIM) where she presented a RISCS report on 'Improving the UK's resilience to ransomware' and shared research conducted during her 2021/22 RISCS Fellowship. Maria is also one of the team of collaborators now working on the EPSRC-funded project 'Enhancing Cyber Resilience of Small and Medium-sized Enterprises through Cyber Security Communities of Support (CyCOS)', and has become a RISCS Project Fellow.

Maria Bada,
Queen Mary University of London, RISCS Senior Fellow

3. Futures Literacy

In a world characterised by high levels of volatility, uncertainty, complexity, and ambiguity, it is more important than ever that we equip ourselves with robust strategies to help the cyber security community to understand and communicate about risk and resilience. Whether it's assessing the risk of moving proprietary data to the cloud, considering the potential impacts of emerging technology on current and future industry, or designing trusted automated products, it's critical that cyber security is informed by rigorous futures thinking. 'Futures literacy' is the practical capability that enables us to do this kind of thinking well, and to use strategic foresight to take informed action in the present. By supporting the RISCS community to become 'futures literate', this theme is helping us all to make more effective decisions as we assess risk and prepare for a range of possible futures.

This year, Will has engaged with various communities about setting the scene and addressing future challenges for cyber security. He represented RISCS at the inaugural 'ChelTechne' summit at which representatives from academia, industry, and government considered, broadly, the future of AI. He was actively involved in the SPRITE+/RISCS Summer School, setting the research agenda with a highly interdisciplinary group of participants. Both of these events highlighted not only the technical but also the sociotechnical issues around cyber security, as well as broader concerns around cyber security and democratic process. He is currently part of an initiative considering the innovation ecosystem in the North West, which is focused on ensuring business innovation and entrepreneurship factors in appropriate security awareness. He is also exploring the possibilities of capacity-building in interdisciplinary approaches to cyber security in the academy, and leading the 'Futures' thread of the RISCS 'Futures Roadmap for the Government's Cyber Security Strategy 2030' project.

Will Slocombe,
University of Liverpool, RISCS Senior Fellow

4. International Relations

Most of the cyber security challenges we face, as well as the opportunities to address those challenges, have important international dimensions. States compete for power and influence in cyberspace through diverse economic, military, and intelligence means. They seek advantage through direct strategic competition and by exploiting the opportunities of international diplomacy and trade. Companies are integrated into complex transnational supply chains and a global cyber security market that thrives on innovation but struggles to keep pace with dynamic and agile cyber threats. Considerations about how to balance national priorities with a complex international cyber security landscape, while still keeping human beings at the centre of decision-making, is a major challenge on which this theme has focused.

The past year has been one of transition for the theme, as RISCS research priorities have been realigned with a new set of emerging and future cyber security challenges. The International Relations RISCS theme has been represented nationally and internationally in discussions about cyber security, with cyber resilience and offensive cyber operations in particular emerging as key considerations for academic and policy communities. In 2023, Tim published a new book—entitled What is Cybersecurity For? (Bristol University Press)—and work on NATO and strategic cyber competition; he also co-edited a forthcoming Research Handbook on Cyberwarfare (Edward Elgar), among other research outputs. Tim was successful in securing a major funding award for the new EPSRC/Dstl project—'Cyber Statecraft in an Era of Systemic Competition'—which he now leads as Principal Investigator. This year, he joins the new cohort of RISCS Project Fellows.

Tim Stevens,
King's College London, RISCS Senior Fellow

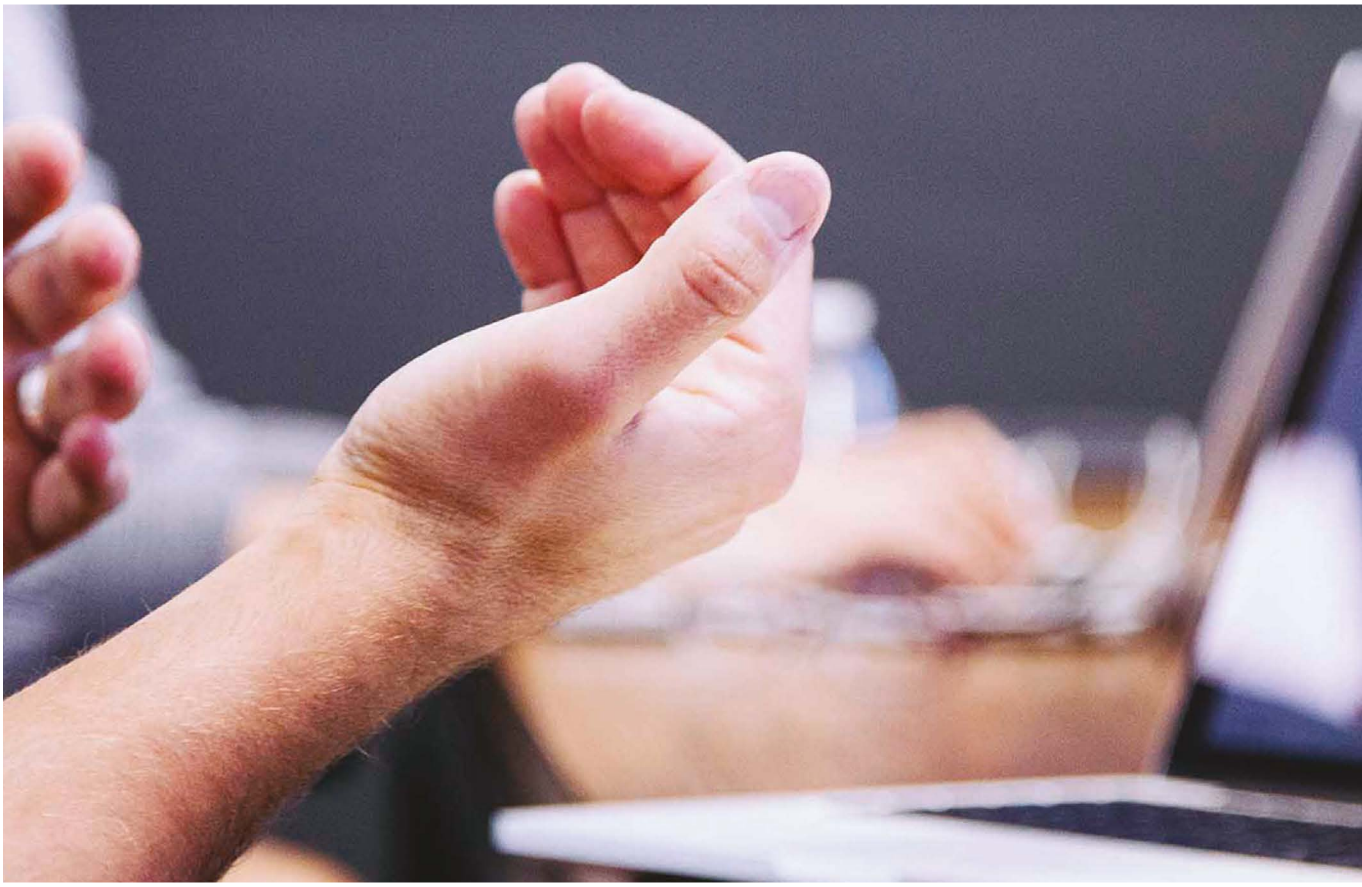
5. Quantification and Cyber Risk

The body of knowledge around cyber risk quantification has been growing in recent years as people seek methods to introduce more repeatability and objectivity to their risk management processes and to frame cyber risk in terms that stakeholders care about. Yet there are barriers to the wider adoption of quantification in cyber security: misconceptions about what cyber risk quantification is; lack of accessible tools and resources; lack of knowledge of good practice and how best to integrate quantification into a wider risk-management process; and the risk of poor implementation of quantification driving perverse behaviours.

This has been a busy year for Anna and the Quantification theme. In May 2023 she ran a workshop on 'Ransom, extortion and cybercrime' in collaboration with RISCS and the

Institute of Applied Economics and Social Value at De Montfort University. This workshop focused on the evolving business model of ransom and extortion, exploring whether insight from hostage-taking and kidnapping might inform the strategy against ransomware. In November 2023, she organised an event exploring 'Cybersecurity in small businesses: impact, incentives and supply chains' with Oxford Brookes University, RISCS, and the Security Awareness Special Interest Group (SASIG), a leadership forum for the industry with over 8,000 members. The workshop brought together business (Data Rockstar, Risk Evolve, East Midlands Cyber Cluster), policy (NCSC), law enforcement (South East ROCU, Police CyberAlarm), and academic expertise to provide actionable recommendations on how to promote behaviour change on cyber security in micro and small businesses. Workshop topics (on evaluating impact, supply chains, and incentives) were shaped through conversations with the relevant NCSC teams. Anna is now leading the 'Cyber Risk Quantification' project for RISCS/NCSC and joins the new cohort of RISCS Project Fellows.

Anna Cartwright,
Oxford Brookes University, RISCS Senior Fellow



RISCS PRINCIPAL AND SENIOR FELLOWSHIPS FOR 2024

Two of the RISCS Principal and Senior Fellowships from 2023 have been refreshed and will continue into 2024, and three new Fellowships have been introduced in response to emerging strategic priorities.

Our Principal and Senior Fellowships for 2024 are now focused on the following five themes:

1. 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. With a research agenda established, 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 we plan 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. We are 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, 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 new RISCS Fellowship theme investigates how people behave and make decisions, both individually and in groups, and across different parts of the cyber security ecosystem. In particular, it will work with an innovative story stem methodology to sensitively explore our understanding of cognition and behaviour around security adoption decision-making. This research theme will help to 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.

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

3. Futures Literacy

This theme aims to help equip 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 will assist more effective decision-making as we prepare for a range of possible futures.

Will Slocombe,
University of Liverpool, RISCS Senior Fellow

4. 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 technical cyber security solution to be sustainable, it needs to exhibit not only performance effectiveness but also cost efficiency, energy efficiency, and compatibility with the existing business processes, regulatory environment, and economic factors, along with consideration of the future landscape, and—of course—user acceptance. In fact, sustainable cyber security solutions likely need people not only to accept them but also to participate actively. This theme will 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.

George Loukas,
University of Greenwich, 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 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). The principal activity will be the development of a survey that will help us to learn more about how different kinds of (inter)disciplinary expertise are perceived and valued within the profession.

Matt Spencer,
University of Warwick, RISCS Senior Fellow

RISCS EARLY CAREER ASSOCIATE FELLOWSHIPS FOR 2023/24

In April 2023 we appointed 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 for 2023/24 focus on the following research themes:

- Communicating cyber security, and intersections between cyber security and creative methods – Ola Michalec, University of Bristol
- Security and privacy engineering topics in the complex risks and harms concerning minority and minoritised users – Maryam Mehrnezhad, Royal Holloway
- Video games, virtual reality (VR), and artificial intelligence (AI) – Dr Richard Cole, University of Bristol
- Online and virtual reality harms – Alicia Cork, University of Bath
- AI metrics and risk in smart cities, control systems, surveillance, and weaponry – Jason Dymydiuk, University of Wolverhampton

The following updates offer a snapshot of the varied activities that this incredible team have been working on:

Communicating Cyber Security and Intersections between Cyber Security and Creative Methods

As RISCS Associate Fellow, I've been presented with plenty of fantastic opportunities to engage with the research network. Starting in March 2023, I wrote a blog for the RISCS website outlining my hopes for the Institute and for the broader cyber security community. In July 2023, I collaborated with colleagues in cyber security, as well as with RISCS Director Genevieve Liveley, on submitting a proposal for a UKRI funding call: 'What is theoretical computer science? An ethnography of merit'. Unfortunately, the proposal didn't receive funding, but we're not giving up! Our short paper has been accepted at a conference, 'Undone Computer Science', which will be held in February 2024 in Nantes. In September 2023, I was invited to present at a workshop and exhibition held by Dr Maryam Mehrnezhad (also an Associate Fellow of RISCS). This session was a valuable feedback opportunity and effectively a 'test run' of an exhibition I organised at the V&A Museum a few weeks later, which was also on the topic of security and arts but in the context of energy.

I am currently working with the team of RISCS Fellows on a project concerned with the future of cyber security in the UK Government. This will be an opportunity to highlight relevant research conducted with other colleagues on e.g. cyber security imaginaries (with Ben Shreeve and Awais Rashid), the cyber security of supply chains (with Colin Topping, Awais Rashid, Barney Craggs, and Andrew Dwyer), and the Cyber Assessment Framework. I'm also hoping to learn more about novel approaches to cyber security 'futuring', especially from anthropology and arts.

Following the Undone Computer Science conference, I will work with the bidding team to re-shape the proposal for another funding call. We're hoping that hosting a workshop under the RISCS banner will help with scoping and securing the right collaborators.

I'm grateful for being part of this network. So far, it has been a wonderful learning experience. I look forward to future events, collaborations, and projects.

Ola Michalec,
RISCS Associate Fellow

Security and Privacy Engineering Topics in the Complex Risks and Harms Concerning Minority and Minoritised Users

It has been a pleasure to carry out cyber security and privacy (SP) research, alongside knowledge exchange and networking activities as a RISCS fellow. During this time, RISCS has supported the opening of the CyFer Art Exhibition '23 (associated with the EPSRC PETRAS CyFer project) and the organisation of the first CyberMi2 Research Day (focusing on SP for marginalised users) at Royal Holloway, University of London (RHUL). With RISCS's support, I am delighted to be organising the second CyberMi2 Research Day in 2024. More specifically, as part of my RISCS Fellowship role, I held a RISCS-CyFer Research Day: an interdisciplinary networking event with a series of talks and round-table discussions about the complex risks and harms of modern technologies (including misinformation on social media, PETs for pets, and bodily SP: the case of menopause), and the key role of knowledge exchange with diverse audiences. The networking opportunities provided by RISCS have enabled me to have out-of-the-box conversations about various SP topics with other experts across disciplines and stakeholders beyond the academic sector, which has contributed to my future research vision—especially on topics relating to gender and SP.

Maryam Mehrnezhad,
RISCS Associate Fellow

Video Games, Virtual Reality (VR), and Artificial Intelligence (AI)

This past year has involved exploring the relationship between cyber security and video games, both as content and method. While security systems abound in video games, particularly within the sci-fi genre, there are not many games about cyber security. Those that do exist tend to gamify complex systems, rather than focusing on the human element of cyber security. Scholarship has called for games that focus more on cyber safety, on human interactions with complex systems, and on broadening representation within the field of cyber security.

In response to this call, and as co-Director of the Bristol Digital Game Lab, I organised a 'concept game jam' in November 2023 on the theme of 'Exposing Algorithmic Bias'.

With algorithms becoming more and more important in scaling decision making, the aim was to use the game jam to think through how existing biases can be embedded, augmented, or even generated anew. We were particularly interested in the amplification of risk through the application of machine learning and AI. The game jam attracted 65 colleagues from across the University and City of Bristol. We had artists, computer scientists, policy experts, and creative writers—the perfect mix for a multidisciplinary exploration. As the game jam was only four hours long, we were more interested in how the mechanisms of gaming and play can expose these processes than in creating publishable games. However, we ended the evening with six games/prototypes that explored a range of questions, from the inner workings of algorithmic bias to the very human side of hiring algorithms. The games, along with a video of the event, will be published shortly on the Bristol Digital Game Lab website.

The game jam was a productive method in exploring a range of interrelated themes and questions, and I hope to be able to run further events of this nature focusing on other aspects of sociotechnical cyber security, particularly those related to human interaction.

Richard Cole,
RISCS Associate Fellow

Online and Virtual Reality Harms

This has been a busy and productive year, and highlights include:

- Taking part in a panel at the British Psychological Society's Cyberpsychology Section Annual Conference 2023, titled: 'Psychology's Contribution to Cybersecurity: Reflections, Interventions, and Opportunities'.
- Publishing a paper at CSCW on transdisciplinary mapping of online harms. The paper won an award for Best Method.
- Getting accepted to lead a workshop at CHI24 called 'Shaping The Future: Developing Principles for Policy Recommendations for Responsible Innovation in Virtual Worlds'.
- Becoming a finalist for the Peter Troughton Research Staff Prize at University of Bath.
- Contributing to the Joint IEEE-Council of Europe report on the Metaverse and its impact on human rights, the rule of law, and democracy.
- Contributing to the REPHRAIN Metaverse and Web 3.0 whitepaper.
- Being invited to talk to Ofcom about online harm transparency metrics.

Alicia Cork,
RISCS Associate Fellow

AI Metrics and Risk in Smart Cities, Control Systems, Surveillance, and Weaponry

The RISCS Associate Fellowship has offered me the opportunity to enhance my position in sociotechnical cyber security through related work both within my own university institution and outside it. In June 2023, my post-doctoral work was disseminated as part of a wider REPHRAIN funded project—'Supporting Small and Medium-Sized Enterprises in Using Privacy Enhancing Technologies'—undertaken alongside RISCS Fellows Maria Bada, Steve Furnell, and Jason Nurse. I have also been conducting research into national and international disinformation and misinformation campaigns, with an eye to the significant number of elections taking place around the globe in 2024. I am interested principally in the lessons we can learn from history and how they might be applied alongside technology capabilities for lifelong education programmes aiming to equip security agencies, election candidates, and voters to deal with this threat. As part of this research I have attended two workshops on 'AI-Enabled Election Disinformation'. In February 2024 I represented RISCS at 'CyberConnect: Where IT Meets Everyone' (part of the Leicestershire Innovation Festival) where I spoke as part of a roundtable event introducing businesses in the region to the sociotechnical aspects of cyber security. I am also currently part of the team working on the RISCS Futures Roadmap for Government Cyber Security Strategy 2030.

Jason Dymydiuk,
RISCS Associate Fellow

PHD STUDENT PLACEMENT: RISCS PROJECT UPDATE

Undertaking a six-month placement with RISCS provided me with an invaluable opportunity to develop a research project aimed at equipping vulnerable users of digital technologies, particularly children and adolescents, to negotiate evolving cyber risks. As children are positioned both as increasingly vulnerable users and as digital natives, my research involved navigating conflicting discourses of protection and empowerment, while acknowledging the interconnectedness between risks and opportunities. My research identified critical knowledge and research gaps in the literature, aiming to inform national priorities in both research and policy and to create positive social impact.

Throughout my collaboration with RISCS, I thoroughly enjoyed being a member of a dynamic research community with access to experts who approach issues of cyber security in increasingly creative and innovative ways. Underlying RISCS's human-centred approach to cyber security challenges is a culture of inclusivity and interdisciplinarity, which values the unique perspectives and methodologies offered across various disciplines. As a researcher in the arts and humanities, I am deeply grateful to RISCS for recognising the value of incorporating expertise from diverse fields of study for addressing the multifaceted challenges of today's cyber security landscape.

The placement also proved rewarding on a personal level and significantly transformed my understanding of the online risks and opportunities facing today's youth. Most importantly, it has enriched my appreciation of the social and cultural implications of digital technologies, while also igniting a passion for addressing these challenges. Working with RISCS has inspired me to explore new avenues for applying my research skills to real-world challenges in the future. I am immensely grateful to Genevieve Liveley, the RISCS community, and the South, West & Wales Doctoral Training Partnership for their unflagging support throughout this placement.

Nerida Brand,
Doctoral Researcher,
South West and Wales Doctoral
Training Partnership (SWWDTP)

RANSOMWARE: THE ROLE OF CYBER INSURANCE (RACI) AND RANSOMWARE HARMS AND THE VICTIM EXPERIENCE (RHAVE) PROJECTS – RISCS PROJECT UPDATE

Ransomware is now a significant national security threat to the UK and to countries across the world. It continues to impact on the operation and delivery of key public and private services, undermining the economic resilience of the country at a pivotal time.

The University of Kent, the Royal United Services Institute (RUSI), De Montfort University, and Oxford Brookes University recently completed a significant programme of research on ransomware aimed at understanding the threat and providing recommendations targeted at the UK Government and the security and insurance industries.

Ransomware: The Role of Cyber Insurance (RaCI) Project, Key Findings:

- The main drivers behind the continued success of ransomware include: the challenges around securing businesses; the low costs and risks for cybercriminals in the ransomware ecosystem; and the fact that cybercriminals continue to find innovative ways to extort victims.
- Contrary to common belief, we found no compelling evidence that victims with cyber insurance are much more likely to pay ransoms than those without.
- The insurance industry plays a key role in ransomware response. It is therefore uniquely placed to do more to instil discipline in both insureds and the ransomware response ecosystem in relation to ransom payments to reduce cybercriminals' profits.
- **Our research does not advocate for an outright ban on ransom payments or for stopping insurers from providing coverage for them. Instead, it makes the case for interventions that would improve market-wide ransom discipline so that fewer victims pay ransoms, or pay lower demands.**

Ransomware Harms and the Victim Experience (RHaVE) Project, Key Findings:

- Ransomware attacks cause a wide range of harms, including physical, financial, reputational, psychological, and social harms.
- We set out a framework involving first-order, second-order, and third-order harms to better assess the impact of ransomware attacks.
- The harms from ransomware go beyond financial and reputational costs for organisations. Interviews with victims and incident responders revealed that ransomware creates significant physical and psychological harms for individuals and groups.

- **Our research found that downstream harms to individuals from ransomware are more severe when attacks encrypt IT infrastructure, rather than steal and leak data.**
- The harm and cumulative effects caused by ransomware attacks have implications for wider society and national security, including supply chain disruption, a loss of trust in law enforcement, reduced faith in public services, and the normalisation of cybercrime.

RaCI

- The RaCI research received significant media coverage, including from The Record, AP, and Financial Times.
- The research team also conducted a number of high-level briefings on the findings, culminating in a briefing to the Counter Ransomware Initiative summit in Washington D.C. in 2023.
- Some of the recommendations from the RaCI RUSI report are currently being implemented by the NCSC and The Home Office.

RHaVE

- Members of the research team produced two opinion pieces, one for RUSI and one for Computer Weekly.
- The research team delivered two public events, both of which were attended by senior NCSC and industry decision-makers.
- Jamie MacColl gave oral evidence to a parliamentary inquiry on ransomware. The inquiry’s report also extensively referenced the findings from the research.

Jason Nurse, *University of Kent* and
Jamie MacColl, *RUSI*

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.

> SMEs account for the vast majority of UK businesses and generate three fifths of employment, but are also significant in experiencing cyber security incidents, with a third of small businesses and over a quarter of micro businesses having suffered breaches or attacks in the last year.

While related guidance and support is available from a range of sources, SMEs can find themselves overwhelmed with information and unable to interpret the advice. CyCOS aims to better understand SMEs' needs and the experiences of those that they turn to for support, and to use these insights as a foundation for a new approach: forming Cyber Security Communities of Support.

The research is supported by a range of relevant partners, including the Home Office, IASME, ISC2, the Chartered Institute for Information Security, the Centre for the New Midlands, and three of the UK's regional Cyber Resilience Centres (Eastern, East Midlands, and London).

The project began in September 2023 and is now completing the background investigation phase. This has confirmed that many SMEs recognise that they have a requirement for cyber security, but are less than confident that they are appropriately protected. Assessment of online advice and guidance reveals an abundance of material for the SME audience. However, this varies significantly in terms of the coverage, completeness, and clarity of the advice being offered. That much of the guidance highlights *what* needs to be done, but does not offer a clear sense of *how* to do it, also poses a challenge. SMEs may consequently find themselves more aware of (and more concerned about) cyber risk, but no closer to being protected from it.

The next phase of the project aims to investigate and understand these experiences in more depth by developing case studies of SMEs' support journeys. The overall evidence base will then provide the foundation for designing and piloting the 'Communities of Support' and determining whether these can offer an additional route for SMEs to engage with their own protection.

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 new project, ‘Cyber Statecraft in an Era of Systemic Competition’ (CyCRAFT), began at the end of 2023. 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 and involving researchers at Bath University and the Royal United Services Institute (RUSI), **this project will examine the nature and character of cyber statecraft and develop concepts and frameworks for understanding and promoting the UK’s international engagement in cyberspace for the next decade and beyond.**

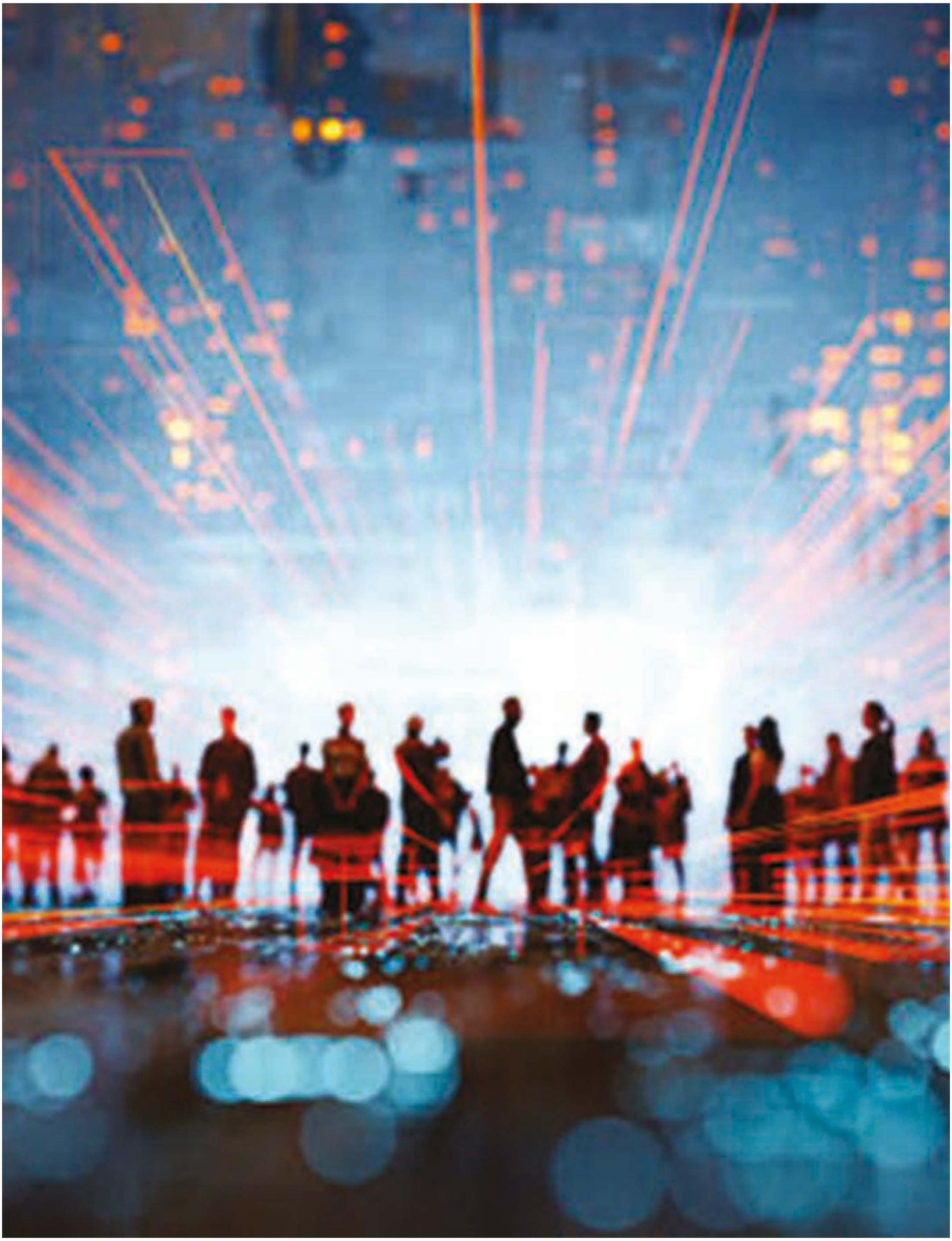
The CyCRAFT project comprises three work packages, each of which relates to key themes of UK international strategy, and which will be further enhanced by a cross-cutting engagement plan:

- Theory, Practice, and Evaluation of Cyber Statecraft (Bath)
- Middle-ground Cyber Competition and Statecraft (KCL)
- the Role of the Private Sector in Cyber Statecraft (RUSI)

Work to date has prioritised staff recruitment and the preparatory phases of the two-year project.

Activities for 2024 include: data-gathering workshops in the UK to map government cyber statecraft activities; stakeholder roundtables in middle-ground countries (Brazil, India, and South Africa); conceptual and theoretical research on cyber statecraft; development of a new framework for measuring and evaluating cyber power; conference presentations; and a new series of public and community engagement projects led by RUSI.

Tim Stevens,
King’s College London



MANAGER'S AND SENIOR ADMINISTRATOR'S MESSAGE

In May 2023 Harriet joined the RISCS team as Senior Administrator, and has been working alongside Louise to support Genevieve, the Fellows, the Advisory Board, and the many other stakeholders in delivering the RISCS vision.

A crucial (and enjoyable!) part of our team's role involves supporting the RISCS Fellows, helping to forge industry-university partnerships, and gathering expert input on the shaping of new research programmes and funding calls. Our Senior Fellows are in place for 2024 and are already actively engaged in research in one or more of the areas identified as a priority for NCSC. This spring, we will be holding an open competition to find a new cohort of early career Associate Fellows, and we will also be reopening our very popular Affiliate Fellow programme in the coming year. We're excited to see where this new cohort of RISCS collaborators take the Institute, and what we can subsequently offer our RISCS community.

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

Louise Evans, *RISCS Manager* and
Harriet Lloyd, *RISCS Senior Administrator*

RISCS

Research Institute for
Sociotechnical Cyber Security