RISCS

Annual Report 2021

Research Institute for Sociotechnical Cyber Security

Director's Statement

Director's Statement

Overview

As I reflect back on 2021, and the work we've done in RISCS, it seems incredible that we achieved so much in what was another extremely difficult year in which to collaborate. Even through the periods that we were not in lockdown, many workplaces remained under restrictions and many of us continued to work largely from home. Face to face events were tentatively planned and then cancelled, but there was also widespread 'Zoom' fatigue from the previous year which meant that online events no longer had the novelty of 2020. As a consequence of ongoing industrial action in the higher education sector, some academics were periodically on strike. And yet, somehow, we all carried on, continued to collaborate, and produced a lot of amazing work. Full credit goes to the seven incredible RISCS Fellows, our NCSC colleagues, and our outstanding support team who made it all happen.

Sociotechnical cybersecurity continued to grow in relevance over the year and this was evident in many of the key events of 2021. Ransomware was a dominant threat and a stark reminder of the increasing sophistication and professionalisation of cybercrime. The previously unthinkable notion of liaising with a criminal 'help desk' or engaging a ransom negotiator to regain access to organisational data became a reality for some businesses and a real prospect for consideration for others. Business leaders had fresh incentive to run through incident planning scenarios and to ensure that this new risk was incorporated into their business resilience planning. Maria Bada, RISCS Fellow for ***Cybercrime***, focused heavily on this throughout the year and provides an overview of her work and outputs later in this report. Also relevant here is Anna Cartwright's work on ***Quantification and Cyber Risk*** which continues to be at the heart of challenges around the economics and decision-making of cybersecurity.

The Log4J vulnerability came to light shortly before Christmas and severely disrupted holiday plans for cybersecurity practitioners around the world as they scrambled to ascertain if their organisations were affected. Log4J is an open-source logging library widely used in apps and services and the NCSC reported this as being potentially the most severe computer vulnerability in years. The work of Shamal Faily, RISCS Fellow for ***Secure Development Practices*** speaks directly to this. The practice of using and reusing existing libraries of code is a fundamental element of the development process and when these libraries have undetected errors in them, those errors are replicated and amplified. Understanding how best to support and incentivize security in software development is central to Shamal's work and it will continue to be pertinent.

Cybersecurity and global politics has more recently come to the fore with the very serious and disturbing situation in Ukraine. UK Foreign Secretary, Liz Truss has described this as a 'hybrid war' – that is, one that blends conventional warfare with (dis)information operations and cybersecurity. It can be difficult to differentiate between cyber incidents that are the work of private actors, state actors, or private actors acting as a proxy for state actors. This allows for plausible deniability which is not an option for conventional warfare in which there is no question as to where troops, tanks, or missiles originate. In an incredibly tense and dangerous political situation such as this one, cyber attacks can significantly add to the 'fog of war', potentially leading to an escalation of the conflict. Tim Stevens' work on the ***International Dimension*** has been so important to bring into RISCS because we are only too aware that these threats are global and need to be understood in that broader context.

The perpetuation of blurred lines between our work and home lives, and our increased dependence on digital systems, applications, and tools further highlighted the importance of thinking critically and deeply about what it means to be a secure 'digital citizen'. Working from home happened quickly and suddenly for many people and organisations and often without adequate planning and processes. Accessing secure work systems at home through VPNs was a technical solution but it did little to deal with the reality of poorly secured routers and sharing devices amongst family members. Essentially, organisations have inherited the insecurity of home networks. Online commerce, schooling, and medical appointments introduced exponentially more personally identifiable date into circulation. RISCS Fellow for ***Digital Responsibility***, Lizzie Coles-Kemp, has been at the forefront of work on human-centric approaches to cybersecurity for many years and the summary she presents in this report on where responsibility for cybersecurity can, does, and should lie, reconsiders some of the entrenched ideas that we have developed over the past few decades.

As the UK develops the new Online Safety Bill, we are conscious that what we think we need from this legislation may not be what we actually need. One of the great challenges for policymakers working in emerging digital technologies is futureproofing laws and regulations so that they deliver benefits without introducing unacceptable unanticipated consequences. And of course, that they remain relevant beyond the next cycle of innovation. It is an incredibly difficult task and one of the reasons why we have invested so much in our policy impact work. Our RISCS Fellow for ***Anticipation and Futures Literacy***, Genevieve Liveley, specialises in helping us to imagine a future world that extends beyond our past experiences and to describe the parameters or elements of that world. This work is increasingly understood as an important way to support decision making in the face of deep uncertainty and Genevieve's research has made a huge contribution.

Of course, the Online Safety Bill will have implications for citizens but it will also affect businesses. Ruth Massie, RISCS Fellow for ***Leadership and Culture*** is working to support those decision-makers in middle management who struggle to incorporate cybersecurity into their roles. These people are confronted with an oversupply of information, guidance, and recommendations – not all of which are in alignment. Producing good policy and industry advice is only effective if those people responsible for implementing it can navigate and absorb the messages and Ruth's work is generating new findings about how to best do that.

Changes in RISCS

This month marks four years exactly since I took over the role of RISCS Director from its founder, Angela Sasse. It's been an exciting, fulfilling, and deeply rewarding four years and I'm really proud of all that we've been able to achieve in RISCS over that period. I believe so strongly in the benefits of focusing on sociotechnical dimensions of cybersecurity and also of working as closely as we have – across disciplines and with our policy partners. It's therefore with very mixed feelings that I've decided to step down and focus on my own research again. You will read later in Anna G's update about some changes that are taking place across the Research Institute ecosystem. This will be an opportunity for a new Director to shape the way RISCS develops and continues to contribute to the sociotechnical cybersecurity research landscape. It feels most appropriate that the new Director be involved in that transition as early on as possible.

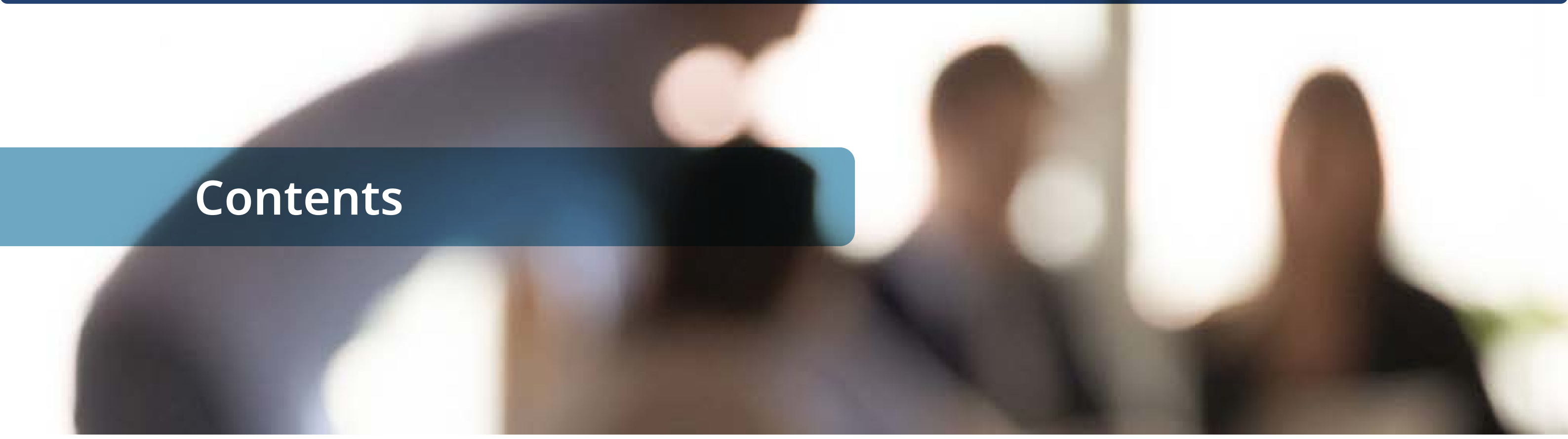
I'm delighted to be able to hand over to our Deputy Director, Tristan Caulfield, who will step into the Director role from the 1st of April this year. Tristan has been a steady leader and has great ideas about how to take RISCS forward, particularly through closer industry ties. I'll look forward to remaining an active member of the RISCS community under his leadership and vision.

As is always the case, it is the people involved that make a role like this so worthwhile and to that end, I extend my deep appreciation, admiration and thanks to a number of people. To John Madelin and Larry Hirst who have been a steady guiding force for RISCS as Chair and Deputy Chair of the Advisory Board and great friends to me – thank you both so much for all the time and commitment. Larry, you have all of our deepest appreciation for 10 years of dedicated support to RISCS. To our NCSC colleagues, Anna G, Paul W, and Helen L – it's been a complete pleasure working so closely alongside you and the rest of your great colleagues. To the RISCS Fellows; Lizzie Coles-Kemp, Ruth Massie, Tim Stevens, Anna Cartwright, Shamal Faily, Genevieve Liveley and Maria Bada – I can't thank you enough for the generosity and sheer intellectual heft that you have brought to your roles. Together, we have grown this Fellowship programme from an idea to what I now consider an absolutely central element of RISCS. This 'distributed brain', as Helen referred to it, is really the power behind the institute. There are certainly further refinements that can be made but I'm so grateful to all of you for your willingness to imagine and implement a new model for our research institute.

And finally, but by no means least, the RISCS support team – the engine room who make it all happen. I've had such great fortune to work in an incredibly happy, highly intelligent and collaborative team of people who are always willing to cover one another, provide additional support, and chip in great ideas. Flo Greatrix is responsible for the amazing policy engagement that we've been able to achieve – it simply wouldn't have been possible without her expertise and talent. Patryk Wloch and Nick Zuniga have done so much with helping to get our message out through various comms channels. And Esme Taylor, our Manager, holds all the strings together all of the time, knowing which ones to pull on a little and which ones to let the slack out on. Such deep gratitude to all of you.

So, farewell, friends. I'll be in the audience next year sitting beside you. But first, I'm off to Australia for a holiday!

Madeline



Contents

RISCS Organisational Structure

RISCS Advisory Board
Chair: John Madelin
Deputy Chair: Larry Hirst

Leadership Team
Director: Madeline Carr
Deputy Director: Tristan Caulfield
Technical Lead: Anna G
Institute Manager: Esme Taylor

RISCS Community (Open)
Policy, Academia, Industry

Leadership & Culture
Fellow: Ruth Massie
NCSC Lead: Kate R

Secure Development Practices
Fellow: Shamal Faily
NCSC Lead: Adam W1

Cybercrime
Fellow: Maria Bada
NCSC Lead: Dylan L

Digital Responsibility
Fellow: Lizzie Coles-Kemp
NCSC Lead: Lee C4

Anticipation & Futures Literacy
Fellow: Genevieve Liveley
NCSC Lead: Anna G

International Dimensions
Fellow: Tim Stevens
NCSC Lead: John N1

Quantification of Cyber Risk
Fellow: Anna Cartwright
NCSC Lead: Lee C4 & Natascha M

Policy Impact Officer
Florence Greatrix

Communications Officer
Nick Zuniga

RISCS Research Themes

Building on the five original research themes established in 2020, in 2021 RISCS has expanded its portfolio in sociotechnical cyber security by adding two more themes; the International Dimensions of Cyber Security theme and the Quantification of Cyber Risk theme. These themes consolidate and expand the scope and objectives of our work, with each research theme lead by a RISCS Fellow. The Annual Report is structured around updates from each of these Fellows, setting out their research and community building efforts over the last year across their respective fields in sociotechnical cyber security.

Theme 1: Leadership and Culture

Improving organisational cyber security is a significant challenge for the UK. How can an organisation position itself to be more secure? What can senior business leaders put in place to optimise cybersecurity behaviours amongst their workforce and what steps can they take to improve their own cyber risk decision making? Understanding how organisations can be better supported to raise their cyber security bar, and which initiatives would best help them achieve this is central to the work in this theme.

Theme 2: Cybercrime

To fully understand how we defend ourselves, we also need to understand how we might be attacked. This requires engaging with the intentions, drivers and behaviours of those who have malicious aspirations as well as those who inadvertently find themselves as “accidental insiders”. Understanding the business models of the cybercrime ecosystem, and how cybercriminals and their victims are affected by them is an important aspect of this endeavour.

Theme 3: Secure Development

Whether it is a software system, a policy, or an organisational process that is being designed and developed, we aspire to have cyber security baked in earlier in the development process with the hope that people can build better systems in the first place and avoid repeating mistakes. However, in the real world, cyber security competes against many other business priorities. We do not currently have a compelling and evidence-based return on investment narrative about why investing in cyber security early is ‘a good thing’ for business (and not just a loss prevention exercise).

Theme 4: Digital Responsibility

Digital responsibility is fundamental to digital security. Without considering security as a reciprocal arrangement where the well-being of all parties is considered, security responsibilities can feel one-sided, leading to an erosion of trust in technology and diminishing the benefits and take-up of technological approaches. A focus on Digital Responsibility helps us to build a positive and healthy relationship with digital technology and use it in a way that minimises harm and helps to increase the benefits for all.

Theme 5: Anticipation and Futures Literacy

Anticipation is broadly defined as using the future to inform action in the present. It is the core discipline that deals with how we, as humans, reason about the future. Risk management uses reasoning about the future to inform actions and decisions in the present and, in our increasing technology and data-led society, we need to consider cyber risks amongst a complex and dynamic landscape. This theme provides insights to improve cyber risk management going forward and draws upon future-oriented insights generated from the fields of Psychology, Philosophy, Narratology, Anthropology, Political Science, Mathematics, the natural sciences and many others.

Theme 6: International Dimensions

Cyber security is a transnational problem that requires international collaboration as well as local remedies. Initiatives and approaches to addressing cybersecurity in the UK must be considered within a global ecosystem. We focus here on issues of international order and the geopolitics of cybersecurity; the international political economy of cybersecurity; global cyber governance; cyber statecraft and diplomacy; and cyber conflict and capabilities.

Theme 7: Quantification and Cyber Risk

While some progress has been made in measuring and quantifying cyber risk, we still have a long way to go. The quantification of cyber risk is important for supporting or informing decision making processes in government, business, and amongst private citizens. But how any risk is quantified can significantly impact how we perceive it and, conversely, perceptions of some actors will influence how risk is quantified. We're working through this theme to provide critical new insight on the issue of measuring and quantifying cyber risk.

Policy Sandpit Project Report

Florence Greatrix, RISCS Policy Adviser

Over the last year we've been working with our RISCS Fellows to deliver a number of 'policy sandpits' which bring the research and policy communities together, along with representatives from industry, think tanks and law enforcement, to identify key areas for further research and collaboration around our key themes.

What is a policy sandpit?

Policy sandpits aim to build engagement with the policy community in the design of new academic research agendas. For many reasons, academic research questions often do not align well with what policy stakeholders would like to know, and even if they do, the findings may not be available at the right time for them or may be presented in an inaccessible format. Policy sandpits look to address this issue directly by developing policy-relevant research questions and setting an agenda for future research. Activities are tailored to each workshop depending on the topic in question, the desired outcome and the participants. All the workshops involve structured multi-stakeholder group discussions and minimal one-sided presentations.

Rationale

Our RISCS Fellows are thought leaders in their respective strategic themes. They are tasked with strengthening the community around their theme and identifying priorities for future research within that domain. These sandpits offered Fellows an opportunity to progress towards achieving both of these goals, with professional policy engagement expertise and support from RISCS. They were designed to provide our policy colleagues with access to a ready-made multi sector, multi-disciplinary community on key cybersecurity themes and outputs tailored to their needs.

The series also crucially offered opportunities for the next generation of cyber security researchers. PhD students and post-doctoral researchers played an active role in contributing to the policy sandpits (as organisers, participants and evaluators). This valuable engagement of early career researchers sets a path for more effective alignment of research and policy objectives in the future. We consider this an essential component to ensuring the UK's future cyber security.

Sandpits so far

Effective sandpits require more than simply bringing everyone together to achieve the desired aim. They require extensive planning to meet the unique objectives of the Fellows and our policy stakeholders, as well as effective facilitation skills on the day. As 2021 was another year filled with endless online meetings and increased pressures, sessions had to be kept relatively short and focused while still allowing everyone a chance to contribute new ideas and hear those of other colleagues.

To date we've held four sandpits:

- **Anticipation theme policy workshop** (Fellow: Prof Genevieve Liveley) – informed the work programme for Genevieve's theme this year, resulting in a wide range of follow-on activities.
- **Optimising the use of UK survey data on cyber security** (Fellow: Dr Anna Cartwright) – identified policy relevant questions for early career researchers to investigate. The findings were shared with policy colleagues and the RISCS community in a workshop that was held in March 2022.

- **Improving the UK's resilience to ransomware** (Fellow: Dr Maria Bada) – pulled together a broad community of academics, policy makers, industry representatives and law enforcement and narrowed down an area of interest for further research.
- **Future Directions in EU Cyber Security: Implications for UK Policy and Strategy** (Fellow: Dr Tim Stevens) – brought together researchers and policy stakeholders on three priority questions to identify key areas of research need.

The series in numbers

Across the four workshops, we've included 80 unique participants including:

- 24 officials from 8 Government departments and agencies (DCMS, NCSC, Home Office, Cabinet Office, FCDO, Government Office for Science, National Crime Agency, CPNI).
- 40 researchers from 21 UK and international institutions.
- 16 representatives from 13 other institutions – including industry, think tanks and law enforcement.

Summary reports

For each sandpit we have published a short report which you can find on the publications page confirming topics or questions for further research and other decisions, commitments and opportunities. We would like to thank everyone who came to a sandpit or read our follow up reports. We are excited to see further outcomes from this series as the ideas are taken forward by our Fellows, event participants and the broader RISCS community.

This project was funded by the UCL EPSRC Impact Acceleration Account and by RISCS.

Leadership and Culture Theme Report

Dr Ruth Massie, RISCS Fellow

I was honoured to be appointed RISCS Fellow for the Leadership and Culture theme this year, taking up the baton from the previous fellow, Dr Berta Pappenheim. Like my predecessor, I see cyber security as central to the long-term health and resilience of organisations. In extending her research, which looked at COVID-19 and cyber security, I have chosen to examine the breadth of cyber security advice that has been made available to organisations. There is now a plethora of advice available on cyber security practices from a huge range of sources. My research specifically attempts to understand how managers make sense of all this information.

The focus of this year's Fellowship has been on the leadership component of the Leadership and Culture theme. Within this, cyber leadership has been understood as a pan-organisation concept. The aim has been to understand what cyber security guidance is given to leadership, at all levels within an organisation, but with particular focus on that made available to middle management (sub senior leadership). This work compliments the RISCS Cyber Readiness 4 Boards (CR4B) project.

Despite, or maybe because, so much has been written about cyber leadership by so many different sources, leaders and managers at all levels of organisations are still unsure of their roles and responsibilities. Furthermore, at times the advice to leaders is contradictory or unclear. Given this, the aim of this year's Fellowship has been to better understand the current state of cyber leadership thinking, to be able to recognise where this guidance is complimentary and where it is contradictory.

Cyber security leadership advice for middle managers

This project considered the question, "What cyber security advice are sub-senior leaders within organisations exposed to?", with a sub-question of "Where does this advice compliment and/or contradict each other?". The advice selected for the research was limited to sources that are external to the leader's own organisation; this enabled us to identify other sources that a middle-manager may come across generally in the course of their role.

The core research activity was a broad literature review looking at what academia, industry and the public sector are writing about cyber leadership, with a particular focus on the recommendations made to organisational leaders. We then looked at where these viewpoints agree, disagree, have gaps and/or overlap.

Reviewing industry advice

The first step was a review of industry advice. As there is a huge range of literature available that is targeted at a variety of industries, it is simply not feasible to review all of it. Therefore, the focus was on advice provided by industry groups, such as membership organisations for example. Most often the guidance had been through some type of internal review prior to being published and it included a range of industries. This is the kind of advice that leaders may come across when fulfilling training requirements of their institutional memberships and professional registration.

Reviewing public sector guidance

Parallel to the industry review, the guidance given by the public sector was also widely reviewed. This included advice distributed by the UK government and Devolved

Administrations. The advice may come directly from the government or via other related public bodies, most often via a 'gov.uk' website. Again, it was felt that leaders were likely to come across such information in their daily roles.

A systematic review of cyber leadership

Finally, a systematic literature review was undertaken looking at the key journals publishing on cyber leadership but also in leadership journals where cyber is an occasional topic. This provided a wide range of academic research and related recommendations to be collated and reviewed. Whilst it was not anticipated that leaders were likely to come across this research in their general workday, often this research is used as the basis for news articles and other regularly accessible media, so it was included for reference purposes.

The literature was compiled against themes with the advice then compared and contrasted. The most common finding was that the advice is often similar when read in detail but confusing, or indeed contradictory, when read at a surface level. Simple examples involve; the use of non-dictionary words for passwords contrasting with advice to use a three random word password; changing passwords regularly versus only when compromised; or not writing passwords down but using a password manager. Whilst to those engaged in cyber these options are distinct, to those leading in other areas of organisations these mixed messages can be confusion and lead to inertia.

The next step will be to verify the findings through targeted focus groups with academic, public sector and industry representatives, with the aim being to identify clear future research questions.

Vision for the future

Looking ahead, the objective is to identify how clarity can be added to provide effective streamlined guidance for those leading within organisations, especially where cyber is not core to their job role. Whilst it is not anticipated that there will ever be a 'one size fits all' approach to cyber security, understanding where simplicity or transparency can be added will assist leaders in better protecting their organisations. We will publish a report with these findings, with the aim of highlighting the issues within individual organisations. Doing so will better enable leaders to effectively identify how to best manage cyber security guidance within their organisation.

In the long term, this research could be extended to include aspects of culture, by looking at the ways in which cyber secure cultures emerge. Again, there is a lot of existing advice and assistance available on cyber secure culture formation. But this advice can similarly be both complimentary and contradictory. By helping individual organisations to work through this advice landscape to improve clarity, we would be working to improve overall cyber security.

Research Project - Cyber Readiness for Boards (CR4B)

Lead Researcher: Professor Madeline Carr, UCL

Institutions: National Cyber Security Centre (NCSC) and Lloyd's Register Foundation

The role of boards in contributing to a broader agenda of national cyber security is well established. While board members are adept at evaluating other business risks, they often feel unsupported and ill-equipped to deal with cyber risk. This project has explored a number of factors from board perceptions and expectations of the information they need, to the struggles that CISOs encounter in trying to provide that information. We've also found that a mental health crisis amongst cybersecurity practitioners poses an 'unseen' challenge to business resilience. And we've looked closely inside the UK higher education sector to identify the unique challenges that universities face and what can be done to mitigate against them. You can learn more about this project on our website at CR4B.

Cybercrime Theme Report

Dr Maria Bada, RISCS Fellow

The aim of the RISCS fellowship on cybercrime is twofold; first, to explore the impact of cybercrime in the UK from the victims' perspective, and second, to understand the role, challenges, and capacity of the police, the judiciary, and other authorities in dealing with such crimes. Over the last year we have explored how the experience and needs of cybercrime victims differ to, or mirror, those of more traditional offline crimes. When talking about victims of cybercrime, it is important to remember that these can be not only individuals but also organisations and even nation states.

During the second phase of the fellowship, the work around understanding the impact of cybercrime on victims continued. This began with further engagement with critical stakeholders across the judiciary, police and government. With the support of NCSC, we conducted a number of interviews with a range of relevant stakeholders. These included actors at the Crown Prosecution Service, in different police departments, and also across various government departments. In these interviews, the discussions focused on the challenges in reporting and prosecuting cybercrime. Discussions highlighted that these challenges were often due to the lack of data and also the lack of clear understanding over the true number and nature of cyber-attacks. Another highlighted challenge was the current legal and geopolitical implications of cybercrime. Some initial findings of this work conducted on online victimisation have been published on our website.

Ransomware and cybercrime

In this second phase of the fellowship, I decided to hone in on ransomware. Ransomware attacks are becoming increasingly prevalent, and the techniques and delivery methods used are becoming progressively more sophisticated. Naturally, the end result of these developments is a higher cost to victims. This increased sophistication allows ransomware attacks to significantly impact networks and organizations leading to costly downtime and reputational damage.

We have also brought the community of cybercrime researchers together to help identify and consolidate the breadth of existing work which relates to ransomware, from a practical but also policy perspective. We undertook a variety of activities to try to better understand the organizational factors and decision-making processes that are aimed to prevent, detect and/or mitigate against ransomware attacks. These included:

- **Consultations –** with stakeholders from the private sector, NCSC, Home Office, law enforcement and academia to identify challenges and gaps surrounding ransomware.
- **A survey –** Between October-November 2021 we ran a survey to collect information around:
  a. the processes organisations follow to deal with ransomware incidents depending on their sector and size;
  b. ways to better prevent or respond to ransomware attacks, and who needs to do what. The findings will be published later this year.
- **A policy workshop –** In December we held a policy sandpit attended by 30 participants from industry, government, law enforcement and academia, who shared their experiences and expertise in preventing and mitigating against

ransomware. The policy sandpit provided a space to discuss ideas and identify what further research is needed to inform new policy responses and/or change how organisations prevent and respond to ransomware attacks. A write up of the workshop is available here.

- **Dissemination –** I spoke about my research with RISCS at the European Society of Criminology (EUROCRIM) E-Conference 2021, presenting the findings on Online Victimisation.

Looking to the future

Going forward we will look to identify the best methods for collecting and sharing the data needed for research on cybercrime. It will also be valuable to explore the use and impact of different research methodologies and tools. To achieve these goals, it will be necessary to continue to engage with relevant stakeholders.

We will continue to try to better understand the needs of vulnerable groups, in addition to also understanding the current practices that might lead to the victimisation of these groups online. In doing this we can help to set guidelines and policies that enhance resilience and minimise the potential harms that these groups encounter online.

Research Project - Ransomware: The Role of Cyber Insurance (RaCI)

Lead Researcher: Dr Jason Nurse, University of Kent

Institutions: Royal United Services Institute (RUSI), University of Kent, De Montfort University, Oxford Brookes University and NCSC

RaCI is a multidisciplinary research project between Royal United Service Institute (RUSI), the University of Kent, De Montfort University and Oxford Brookes University. The project is funded by the NCSC and RISCS. The project aims to understand the role of cyber insurance in handling the challenges posed by ransomware and the impact this has on how governments, law enforcement and the insurance industry set out to tackle ransomware.

By combining an extensive literature review with stakeholder interviews and workshops, the project will seek to gain critical insights into the cyber insurance industry. This will involve engagements with a diverse global community, including insurance professionals, law enforcement, civil servants, cyber security and incident response experts, data breach lawyers and businesses.

RaCI's research findings will be pivotal in helping decision makers to navigate cyber risk management approaches. The finding will also help them better understand ransomware challenges in the context of cyber insurance, while also providing clear and actionable recommendations that can be adopted by governments and practitioners alike.

Secure Development Practices Theme Report

Dr Shamal Faily, RISCS Fellow

Research activities

In 2021, we began to explore practices that can help address knowledge asymmetry problems in cyber security, to foster a better understanding of different actors' needs and expectations. We have developed an approach such that, with modest tweaks to modelling notations, we can both model and tentatively validate specifications to expose knowledge asymmetries when the models are discussed collaboratively. This approach was designed to evaluate the effectiveness of different design practices at exposing knowledge asymmetries.

We are currently exploring techniques for evaluating these approaches. We have chosen the design of access control as a general problem space, because this is known to be a difficult problem.

We have been developing a specification exemplar to form the basis of lab-based studies, one that is simple enough for different participants to comprehend quickly, but with sufficient nuance that knowledge asymmetries can be identified to determine how good the techniques are at addressing them. The exemplar under development is derived from the Tokeneer Token ID System. As an example of a system that is 'correct-by-construction', Tokeneer provides a baseline so that models created using different techniques can be evaluated against it.

Community activities

In 2020, we created a map of Secure Development Practice capability in the UK higher education sector. This year, we updated this map and are reviewing sustainable approaches for maintaining it beyond the end of the fellowship.

We ran a community workshop on Secure Development Practices education in December 2021 which was well-attended by educators both in higher education and industry. Several interesting challenges emerged in the workshop. For example, how should we teach developers to rate the security 'health' of their code? How, in a packed undergraduate or post-graduate curriculum, do we teach security to developers without sacrificing other quality concerns like usability, performance, and maintainability? Finally, how should educators assess the 'readiness level' of some piece of security development practice research they wish to incorporate into the curriculum - particularly if their background is in software engineering or cybersecurity, but not both?

Open problems and opportunities

Informing the software developer

In recent years, developers have become more aware of the relationship between security and their software. It may be less obvious to them how what they develop might be exploited, but there is a growing acknowledgement that the software stack they rely on is exploitable. This acknowledgement is, however, a source of tension. Irrespective of their power to address security problems, it remains the case that -- as the ultimate experts on how their code works – it may be left to software developers, not security professionals, to find workable solutions. This burden of responsibility may have long term implications, particularly if they are blamed or accept blame should these problems be exploited in the future. At our recent Security Education workshop, it was proposed that secure development education should not be purely technical. It should also include topics such as strategies for promoting mental resilience and wellbeing, and information on the form occupational hazards in software development might take.

Methodological challenges

Secure Development Practices remains a methodologically challenging area. We are starting to see more qualitative research on developers' security and privacy needs and expectations. However, this research often does little more than re-iterate long standing collaboration problems between product and security stakeholders. This means that while research is being undertaken, it commonly fails to accurately target the correct problems. It seems unlikely these obstacles will be successfully navigated without innovative practice and software tools that address the tensions between building an innovative product and a resilient one.

Such practice needs to be grounded in research from convincing, ecologically valid lab studies, or commercial practice via action research. Our current work is attempting to make progress with the former. Empirical evidence from practice is still ultimately necessary to elevate the technology readiness level of the research to the point that it can be effectively used and shared by educators and practitioners. That evidence will remain elusive until we can address two methodological hygiene factors; first, the perception of decision makers that innovation to secure design practices is too risky, and second, the perception that any collaboration with researchers to collect data about such practices is invasive and unlikely to lead to a return on the time invested in it.

Tooling and principles as an opportunity

Lightweight techniques, such as threat modelling, are becoming vehicles for embedding secure development practices that research practitioners and educators can adopt with comparative ease. With DevOps now becoming a dominant paradigm, with its drive to 'shift security left', these techniques and tools are leading to the acceptance that secure development practice is more than just coding. Coupled with a growing interest in cyber resilience, non-security stakeholders are now beginning to seriously consider what it means to demonstrably secure products earlier, rather than later in a product's life.

NCSC's work in Principles Based Assurance (PBA) appears to build on the opportunities afforded by improvements to design techniques and tools. With its emphasis on evidencing of design for usability and continuous assurance, the search for clarity on how these principles should be applied could be the vehicle for researchers and practitioners to work together to overcome the highlighted methodological hygiene factors.

Digital Responsibility Theme Report

Professor Lizzie Coles-Kemp, RISCS Fellow

The fellowship in Digital Responsibility examines what digital responsibility might mean and its relevance to security. The aim of the fellowship is to develop a research agenda that furthers our understanding of digital responsibility. In developing the research agenda, the fellowship captures the current state of the art in guiding principles of digital responsibility, builds a research community dedicated to studying the relationships between digital responsibility and information security, and develops practical implementation guidance for both practitioner and policymaker.

Below is the story of the fellowship as told by Lizzie Coles-Kemp (Fellow) and Nick Robinson (Assistant Research Fellow) who are both in the Information Security Group at Royal Holloway, University of London.

The story so far

In the first phase of this fellowship, we undertook a series of scoping activities to identify what digital responsibility is and what the main barriers to achieving it are. This included a four-week reading group programme and townhall-style workshop, which focused on the practice of digital responsibility. From these initial activities, we found that digital responsibility is still difficult to define and that it means many things to different people (e.g., a technology or service that is secure by design, accessible and inclusive, or a governance/risk framework that identifies where responsibilities lie in relation to technology use). Nevertheless, we found that digital responsibility intersects with many facets of digital technology:

- Technology design and the deployment of technology;
- The frameworks and processes used to implement digital technology;
- The relationships that we have with and through digital technology; and,
- The networks of power that are necessary for the realisation of benefits through technological access.

These intersections relate to a number of research areas that are of interest to cyber and information security:

- Responsible research and innovation (RRI)
- Responsibilisation and the individualisation of risk
- Responsibility, care and technological design
- Responsibility and technological security (e.g., AI)

Similar to other RISCS research themes, our work was severely impacted by the COVID-19 pandemic as face-to-face research was curtailed and we all shifted to online forms of communication. However, COVID-19 also surfaced the importance of digital responsibility to online safety and security. As life moved online during the pandemic, significant parts of society needed a range of support to be able to do this. Most of this support was informal, provided by friends, family, community and third sector organisations. Our work in Phase 1 indicated that digital responsibility was part of these helping relationships. In Phase 2, we chose to explore this insight in more depth.

Safe and secure digital access

In February 2021 we held workshops with local community groups in the North East of England on issues associated with forms of digital assistance, in the context of access to everyday digital services. Taking place over Zoom, we asked participants to provide stories of assisted digital access from their everyday experiences as support workers within their local communities (capturing them on the digital storyboarding platform Padlet). From these workshops, we found that communities have relied more and more on informal forms of assistance when receiving help accessing a digital service - often sourcing this assistance from kin and friendship networks, or from local third sector organisations. This emphasised how the notion of responsibility is often distributed between different people and groups, when they either give or receive help accessing digitally-mediated services. With circumstances exacerbated by the pandemic, our workshops also revealed that whilst such assistance is essential for many, services are not designed with that assistance in mind.

To explore how we might include access assistance in the design of access to services, in May 2021 we ran two policy workshops with participants from the NCSC, in order to gain insight into some of the key policy, regulatory and technological challenges that exist around different forms of assisted access. Building on previous community engagement workshops, our aim was to introduce participants to different stories and examples of assisted digital access. We asked participants to reflect on the lived experiences and challenges faced by the individual(s) in each story and to develop a set of problem statements that identify some of the most relevant issues and policy gaps relating to assisted forms of access (whether formal/informal or digital/non-digital). For NCSC, the workshop offered a unique perspective on the wider implications of how NCSC currently deploys cyber security in practice, both positive and negative, for the lives of people previously missing from cyber security narratives and decision making. The workshop also highlighted the responsibilities that such bodies have towards the digital security of marginalised and underserved communities - although, these responsibilities are still not clearly understood by relevant stakeholders.

On the horizon

Entering its final phase, we are committed to a number of exciting engagements as part of the fellowship that seeks to draw together (and further expand) our growing research agenda on digital responsibility. First, we are continuing to host the Critical Security Reading Group (CSRG) at Royal Holloway, University of London, which has allowed for continual reflection and discussion on topics related to digital responsibility and security. Second, we are consolidating our findings in a number of research outputs that are currently undergoing peer review. As part of these outputs, we are preparing a collaborative review piece on assisted digital access, hopefully for publication on the NCSC blog in 2022. Finally, we are currently working on a review that attempts to map the different responsibilities that arise from the various iterations of the UK government’s Online Safety Bill. This review has involved tracing the trajectory of the Bill from White Paper to the recently published Draft Bill, asking where certain responsibilities are being ascribed by various stakeholders and where some of the clear gaps and tensions exist. All of this work will be curated together with a report summarising a research agenda and call to action, to further the study of digital responsibility and its relationship to information and cyber security.

Anticipation and Futures Literacy Theme Report

Professor Genevieve Liveley, RISCS Fellow and Dr. Anna G NCSC Lead

The aim of the RISCS Anticipation and Futures Literacy Fellowship is to improve our understanding of the relationship between futures thinking and cyber security. Futures thinking is an essential component of cyber security. Resilient cyber security frameworks demand the capacity to anticipate the probability of future threats, in both their nature and potential impact, in order to successfully develop mitigation and defence strategies. In 2021 we worked to further develop expertise in this exciting research area, to map best practice, and to build both capacity and community among those interested and involved in strategic futures and cyber security.

What is anticipation?

Anticipation, as an academic discipline deals with analysis of how we, as humans, reason about the future. It is broadly defined as using expectations about the future to inform actions in the present.

What is futures literacy and why is it relevant for cyber security?

Futures Literacy is the skillset that guides anticipatory thinking and action. UNESCO calls it an "essential competency for the 21st century". It is "the skill that allows people to better understand the role of the future in what they see and do. Being futures literate empowers the imagination, enhances our ability to prepare, recover and invent as changes occur."

For further details see: https://en.unesco.org/futuresliteracy/about.

Applying futures literacy and anticipation

One example of using futures literacy and anticipation to empower the imagination is the creation of fictional future narrative scenarios, such as futures news media stories. In spring 2021, together with academic colleagues from the FLiNT (Futures Literacy through Narrative) consortium and CyRes, we created a storybook of fictional narratives inspired by real news stories and informed by case studies of cyber security in the automotive industry. A selection of these stories is available to read on our website.

Futures stories like these, can help to focus minds on the importance of future preparedness when managing the risks and obligations for which boards and others are legally responsible. Such stories help boards to identify learning points to inform action now, spot potential weaknesses in existing policies and plans, explore new ways to mitigate risks and harms, and – crucially – to build not only resilience but forward-thinking 'prosilience'.

A year of activities

We have had another busy year socialising our theme and building up the community of cyber security futures practitioners and experts across government, industry, business, and academia. We gave presentations on the theme to DCMS, took part in a fireside chat with Siân John at the April 2021 Microsoft Security and Compliance Summit, convened a panel and podcast for CyberUk, and joined Ann Johnson as guest for her cybersecurity podcast, "Afternoon Cyber Tea". We have also presented a number of academic papers at various conferences and seminars, including the AESIN Virtual Security Conference in July, the IEEE International Symposium on Technology and Society (ISTAS) in October, and the IALC Futures Analysis and Strategic Foresight conference in November. These presentations have helped to raise awareness of anticipation and futures literacy as useful tools for those working, researching, and making policy across the wider cyber security ecosystem.

Policy workshop

In July we ran an online policy workshop with 20 participants from government, academia, and the wider cyber security community to discuss how futures literacy could benefit cyber security policy, and where it might be relevant to both academic and policy communities. During the workshop we spent time looking at examples of good practice, as well as highlighting some of the barriers and challenges that stand in the way. It was great to see so many people from across the cyber security ecosystem excited about the benefits and possibilities of futures literacy.

Looking forward

We plan to present some highlights from the project at the international 'Anticipation' conference taking place in Arizona in November 2022, as part of a specially curated session on 'Securing the Future(s): Creative Futuring for UK Defence and Security'. And we anticipate that "Anticipation and Futures Literacy" in cyber security will continue to grow from strength to strength in the future.

Research Project – Stories of Cyber Security (SOCS)

Lead Researcher: Professor Genevieve Liveley, University of Bristol

Institutions: University of Bristol and NCSC

This project examines the potential for stories and storytelling to inform and support more effective communication of cyber security good practice and policy. The first phase of the project mapped what the 'storyworld' of this narrative ecosystem looks like –identifying problem areas where narrative dynamics are weak and failing to engage key stakeholders. It adopted a systems thinking approach to the narrative analysis of a portfolio of stakeholder stories that interact across the ecosystem of cyber security. The second phase of the project analyses the dynamics of these varied interactions and suggests practical recommendations for employing different narrative strategies in cyber security communications. For example, one of the project's key discoveries is that the NCSC's narrative role in this ecosystem is best understood as that of the 'donor' or 'helper' – a classic mentoring or caring character whose prime function is often to help 'heroes' defeat 'villains'. The free provision of tools and services, and work supporting people to take charge of their own cyber security, align well with this 'donor' or 'helper' characterization. As do metaphors and narrative tropes emphasizing the role of the NCSC in mentoring, advising, and supporting others. The project has also found that the NCSC's core mission and strategic narrative is that of the 'quest' – which emphasises teamwork, profits, optimism, and future possibilities. A full report detailing these findings will be published later this spring.

International Dimensions Theme Report

Dr Tim Stevens, RISCS Fellow

Few of the challenges of cyber security map easily to national borders and jurisdictions. Whilst national cyber security is a key policy area for governments, it is hard to develop it absent of the consideration of the multiple transnational dependencies and challenges cyber security presents. Indeed, all of the other RISCS research themes contain within them, implicitly or explicitly, international aspects that underpin and shape much of their nature and character. Effective cyber security recognises its international dimensions, as outlined in the recent UK National Cyber Strategy, for instance, and seeks to adapt and plan accordingly.

To enhance our understanding of this situation, in March 2021 RISCS inaugurated a new research theme on the 'International Dimensions of Cyber Security', which I am honoured to now lead. The broad aim of the fellowship is to identify, map and develop the community of UK researchers exploring the international dimensions of cybersecurity and to encourage multistakeholder collaborations that address particular policy challenges with international dimensions.

Building the community

Many academic researchers in the UK work on international cyber security issues, yet most work in relative isolation and are not well served by professional bodies and networks. This is changing slowly, including through new initiatives like the Offensive Cyber Working Group (OCWG) and the British International Studies Association International Security and Emerging Technologies Working Group (ISET). I believe that RISCS can play a unique role in encouraging the growth, visibility and sustainability of this research community, while at the same time putting it in conversation with key members of government and industry.

We have conducted an initial mapping exercise of academic researchers and research groups in the UK. This identified 100+ researchers at over three dozen universities, whose work focuses to a large extent on international cyber security. Their work bridges diverse disciplines, from law to economics, geography and criminology, and across political science, economics and international relations. We were also encouraged by a growing cohort of talented doctoral researchers, something which is essential to the longer-term sustainability of any research community.

We have held two workshops with members of this community, alongside colleagues from government and industry. COVID-19 has suspended any plans for face-to-face events, but we hope to develop this component of the fellowship more over the next reporting period. Please contact me if you would like to contribute to our work in any way, or have ideas that we can build upon to achieve our community focused goals.

Bringing the international in

At the beginning of the fellowship, RISCS and the National Cyber Security Centre (NCSC) hosted a one-day workshop, 'Bringing the International In' (February 2021). An expert panel, consisting of representatives of NCSC, Department for Digital, Culture, Media and Sport (DCMS), Foreign, Commonwealth and Development Office (FCDO), and King's College London, gave their thoughts on international cyber security research and policy priorities. Stakeholders from academia, industry and government then broke into small groups to discuss how the UK cyber security research community could direct its future multi-disciplinary efforts to address them.

The workshop identified five main research areas and a set of general principles. The research areas were understandably broad and we encourage their deeper exploration. They serve currently to inform further thinking on how to structure national research priorities. The five themes are: International Order and Geopolitics; International Political Economy; Global Governance; Statecraft and Diplomacy; Cyber Conflict and Capabilities.

The general principles included: recognition of the need for multi- and inter-disciplinary research; the pairing of ‘pure’ research with ‘applied’ research relevant to a diverse stakeholder community; analytical frameworks that incorporate multiple levels of analysis and the importance of civil society, industry, international organisations and individuals, as well as states.

Future directions in EU cyber security

In January 2022, we held a second workshop, ‘Future Directions in EU Cyber Security: Implications for UK Policy Strategy’. Developed in partnership with our NCSC colleagues, this primarily academic/government event explored ongoing and future developments in EU cyber security and their implications for UK cyber security policy, strategy, decision-making and research. It responded directly to the post-Brexit situation, in which the UK is no longer part of the European Union, yet remains connected to it in multiple policy fields relevant to cyber security.

The workshop was structured in three themes, each run by an academic chair and RISCS facilitator: Law and Regulation (Professor Lorna Woods, University of Essex); Technological Sovereignty (Dr Andrew Liaropoulos, University of Piraeus); European Partnerships (Dr Helena Farrand Carrapico, Northumbria University). We will be reporting soon on these discussions and how we might work with stakeholders to address policy challenges through academic research and collaboration.

Looking ahead

We will publish a report on the recent workshop on EU cyber security and develop concrete research proposals that address the needs of UK policymakers. We have plans for a second strand of work with the NCSC, looking at how to measure and assess the international impact of UK cyber security policy and strategy.

In combination with this we will continue to socialise the aims and themes of the fellowship with the research community and look into how we can best develop and serve researchers in academia, industry and government. Thus far, the reaction from the community has been solely positive and I welcome input from colleagues as the theme progresses.

Quantification and Cyber Risk Theme Report

Dr Anna Cartwright, RISCS Fellow

Knowledge around cyber risk quantification has been growing in recent years as analysts try to frame cyber risk in terms that stakeholders can understand and care about. We still, though, have a long way to go. Contemporary discourse relies far too much on anecdotes and numbers seemingly 'plucked out of the sky', about the size of the cyber-security risk. This argument is not new, but fortunately the knowledge gap is gradually starting to be bridged. There are still however barriers to the wider adoption of quantification in cyber security. For example, organizations may underestimate cyber risk, but lack the appropriate tools or knowledge to integrate quantification into a wider risk management process, or they may poorly implement appropriate policy.

The quantification and cyber risk theme explores the following questions:

- How can we integrate quantification into a wider risk management process?
- How do we overcome the challenges and enable the cyber security community to use quantification to optimum effect?
- Where can quantification be used to accurately assess cyber risk and enable effective cyber security decision-making?
- Can quantification play a role in bridging the gap between cyber risk and other areas of risk, such as safety?

The Fellowship currently involves two complementary strands: (1) optimising the use of UK government survey data on cyber security and (2) cyber-risk management in small and medium enterprises (SMEs).

Optimising the use of UK government survey data on cyber security

There is a wealth of UK government data on cyber security, most notably the Cyber Security Breaches Survey, Commercial Victimization Survey and Action Fraud data, as well as other surveys that touch on cyber, such as the Longitudinal Small Business Survey. The data sets from these surveys are available for research purposes from the UK Data Service. Currently, however, the data is under-utilized as a resource for studying cyber-security. In this stand of the fellowship, we are enabling and encouraging research that utilizes these data sets.

In July 2021 we held a policy workshop on "Optimising the use of UK government survey data on cyber security". The workshop was organised by RISCS Policy Officer Florence Greatrix and UCL Public Policy Manager Jenny Bird. We welcomed representatives from the National Cyber Security Centre, Department for Digital Culture, Media and Sport, law enforcement, the private sector, and academia. We adopted a knowledge exchange framework, to address the following questions: (a) What data on cyber-security in SMEs is freely available for academic research? (b) What are the priority policy questions we should try to analyse with that data? (c) How can we most effectively analyse the data?

At the workshop we identified a set of priority policy questions that could be investigated with existing survey data. Further details on the workshop are available in the RISCS workshop note.

Following on from the workshop we launched the RISCS Prize Competition: Optimizing the use of UK government survey data on cyber security, based on the outcomes of the policy workshop. The competition encouraged novel data analysis and cyber security research by PhD students and early career researchers. Specifically, we were looking for submissions (in the form of an academic paper) that studied one or more of the policy questions detailed above using existing survey data.

The winners of the prize competition were Steven Kemp, David Buil-Gil, Fernando Miró-Llinares and Nicholas Lord with the paper "When do businesses report cybercrime? Findings from a UK study". We were also pleased to award second place to Lukas Walter and Daniel Woods, for the paper "Reviewing the Likelihood of Cyber Incident".

Earlier in March 2022 we held a second engagement workshop to gather feedback on the outcomes of the competition and set a plan for future collaboration and analysis. Looking to the future of this strand, we intend to have an annual competition and workshop to continue the knowledge exchange among government, practitioners and academics on data collection, sharing of data and analysis.

Cyber-risk management in SMEs

SMEs are widely considered to still be relatively lax when it comes to cyber-security. While there is no simple solution to this cyber-security capability gap, in a recent Home Office funded project, we identified that local micro IT companies could form part of the solution. Micro IT companies are often embedded in their community and therefore provide an ideal way of cascading information through local business communities. These IT providers may, however, lack sufficient knowledge and support to be capable of guiding their clients through effective cyber security and risk management practises. Moreover, IT companies often operate in largely unregulated markets, meaning that some IT companies may actively disseminate poor advice and practise.

In December 2021 and January 2022, we held a series of focus groups and interviews with local IT companies and relevant stakeholders. These focus groups were organized by our research assistant Dr. Esther Edun. The discussion in the focus groups was structured around the following questions:

- Where do you currently access information/advice on cyber-security?
- What are the main barriers for small businesses in adopting cyber-security best practice?
- What support from government could facilitate the adoption of best practice?

Based on the outcomes of the focus groups we are developing an academic paper and a targeted policy summary. This summary will explore the opportunities and challenges of cascading cyber security information, while also highlighting best risk management practices through local IT companies.

Vision for the future

The overarching questions we will attempt to address in this theme going forward are:

- How can we effectively obtain accurate and reliable data so that we can quantify cyber risk across different organizations?
- How can we enable sharing and facilitate accurate analysis of that data?
- How can the data we obtain be best utilized to improve cyber risk management practices in organizations?

The current strand of work on “optimising the use of UK government survey data on cyber security” effectively works towards helping us answer the first two of the questions set out above. While the second strand, ‘Cyber-risk management in small and medium enterprises (SMEs)’, is designed to guide us towards answering the third question.

In the long term, the primary ambition is to join these strands of work together and actively trial interventions. These interventions would be aimed at improving the linkages between data on cyber security and risk management behaviour in organisations.

Research Project – Security Economics of the Supply Chain for Connected Places

Lead Researcher: Dr Manos Panaousis, University of Greenwich

Institutions: NCSC Critical National Infrastructure (CNI) Research Team and University of Greenwich

This research project involving researchers from the University of Greenwich is looking at how we can better understand the economic drivers involved in Connected Places supply chains. The first phase has involved looking at some existing smart cities and reviewing the makeup of their supply chains and the nature of the companies involved. Drawing on the NCSC Cyber Security Principles for Connected Places, as well as CIISec resources and ETSI controls where applicable, the project aims to design a model case of a typical connected place. In this instance the project looked at a smart traffic light system, and its supply chain to understand how the different cyber security principles can be practically applied to this case. The project also hopes to propose an economic feasibility assessment framework, to analyse the NCSC Cyber Security principles for Connected Places. This will involve identifying expenditures involved in delivering these capabilities and activities required to implement the CP principles, along with examining the damages they prevent. We hope this research will develop a better understanding of how best to incentivise players in this ecosystem and articulate the risk involved in a lack of adherence to the recommended principles.

Closing Message

Anna G, NCSC Technical Lead for RISCS

In April 2021 I had the privilege of joining the RISCS leadership team as NCSC's Technical Lead for RISCS. As a member of the Sociotechnical Security Group (StSG) in the NCSC, I've experienced first-hand the role and impact of RISCS. The opportunity to work more closely with the team and community has been hugely exciting for me and I continue to be awed by the breadth of fascinating research and multi-disciplinary expertise which RISCS fosters and supports.

This year has seen us build on the successful first year of our Fellowship programme, continuing to invest in our five established research themes as well as introducing two new themes. We recognise the importance of supporting our experts to do the deep thinking in critical problem spaces and bring together a diverse community to collaborate on innovative approaches. Together, our seven research themes demonstrate the broad landscape of sociotechnical security across which our experts and the wider RISCS community seek to add value. To ensure the fantastic work of the community pulls through to impact in the right places, we've also deepened our engagement with policy-makers and sought out opportunities to listen to industry and key voices in cyber security.

The end of this year sadly brings us to a time of change as Madeline has decided it is the right time for her to step down as Director. I would like to take this opportunity to offer our thanks and appreciation to Madeline for the tremendous energy and insight she's brought to RISCS. In her four years as Director, the community has grown and developed, and importantly Madeline has brought in innovations that provide a foundation for RISCS to continue to be an asset to the UK and a critical part of our cyber security research community. While Madeline will certainly be missed, I hope that she will continue to be an important part of the community and future of RISCS. I would also like to welcome Tristan Caulfield, who will step into the role of Director for the coming period. I look forward to working more closely with Tristan and value the perspective he will bring to the work of RISCS.

We're also coming into a period of transition for RISCS as a research institute as the current funding cycle, jointly funded by NCSC and EPSRC, is coming to an end in summer 2022. This provides a natural point for us to reflect on the impact of all four of our research institutes and an opportunity to look to the future. In collaboration with EPSRC, NCSC is developing a long term model for the research institutes. Current events are a stark reminder of the complex and critical role cyber now plays in our day to day lives and on the world stage and why the work of RISCS and all our research institutes matters. We will share with the community what this next phase is going to look like as soon as we're able to – inevitably it's taking some time to cross the i's and dot the t's behind the scenes – but we remain committed to the communities, expertise and leadership that the research institutes provide and look forward to supporting RISCS into the future.