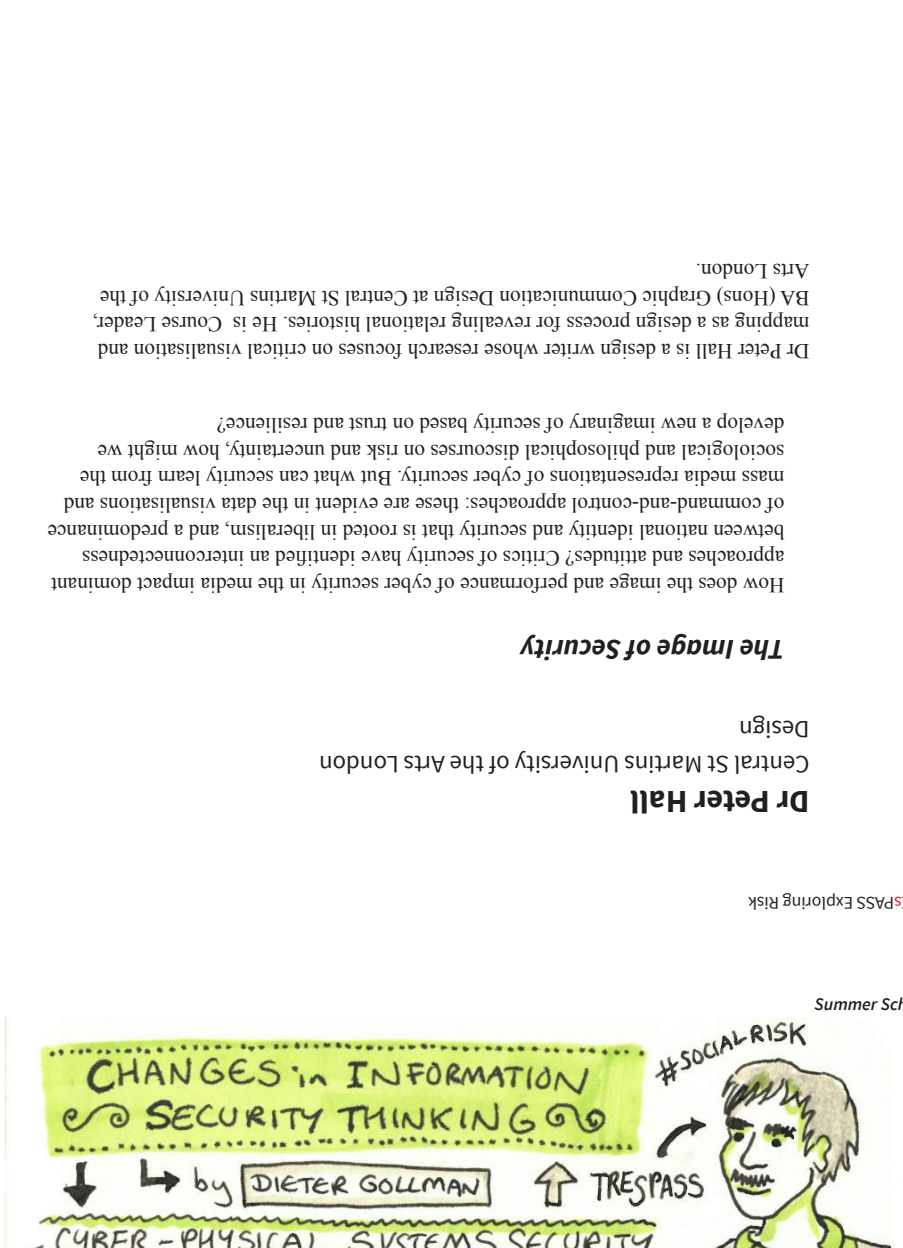


Summer School

TRESPASS
prevent
prioritise
predict

Dr Peter Hall
Central St Martins University of the Arts London
Design

The Image of Security

How does the image and performance of cyber security in the media impact dominant approaches and attitudes? Critics of security have identified an interconnectedness between national identity and security that is rooted in liberalism, and a predominance of command-and-control approaches: these are evident in the data visualisations and mass media representations of cyber security. But what can security learn from the sociological and philosophical discourses on risk and uncertainty, how might we develop a new imaginary of security based on trust and resilience?

Dr Peter Hall is a design writer whose research focuses on critical visualisation and mapping as a design process for revealing relational histories. He is Course Leader, BA (Hons) Graphic Communication Design at Central St Martins University of the Arts London.

TREsPASS Book 2 : Summer School

Series Editor : Lizzie Coles-Kemp
Editor : Peter Hall
Image Curator: Claude Heath
Design : Giles Lane | proboscis.org.uk

Published by Royal Holloway University of London

ISBN : 978-1-905846-76-4
978-1-905846-77-1 (ebook)

Acknowledgements:
Sketchnotes created by Miriam Sturdee
Photographs: Claude Heath and Makayla Lewis
Comic strip templates and icons: Makayla Lewis
Risk Literatures: curated from speaker literature contributions

The material presented in this book was originally produced in the following publications:
The TREsPASS Project, D4.2.2. (2016). *Methods for visualization of information security risks.* (Deliverable D4.2.2)
The TREsPASS Project, D4.3.3. (2016). *Visualisations of socio-technical dimensions of information security risks*. (Deliverable D4.3.3)
These publications are available from: http://trespass-project.eu/

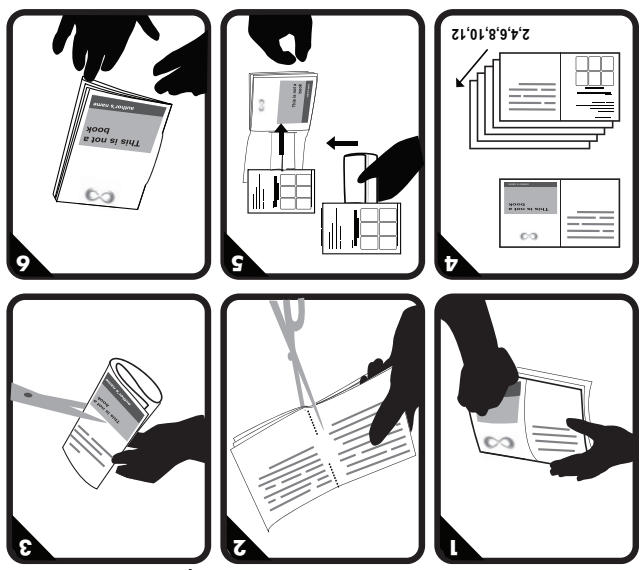
A collection of the TREsPASS visualisation work (including visualisation prototypes) can be found at: https://visualisation.trespass-project.eu/

front cover : Illustration of Founder's Building Royal Holloway (Artist: Miriam Sturdee)

Funded through the European Commission's Seventh Framework Programme: Grant Agreement No. 318003 (TREsPASS)

www.trespass-project.eu

http://bklt.r.it/2cue27n



made with **booklet**eer.com from **proboscis**

TRESPASS

Summer School

Lizzie Coles-Kemp

2016-10-31 & © RHUL & contributors 2016

Published by Royal Holloway University of London

TREsPASS Exploring Risk: Book 2

Contents

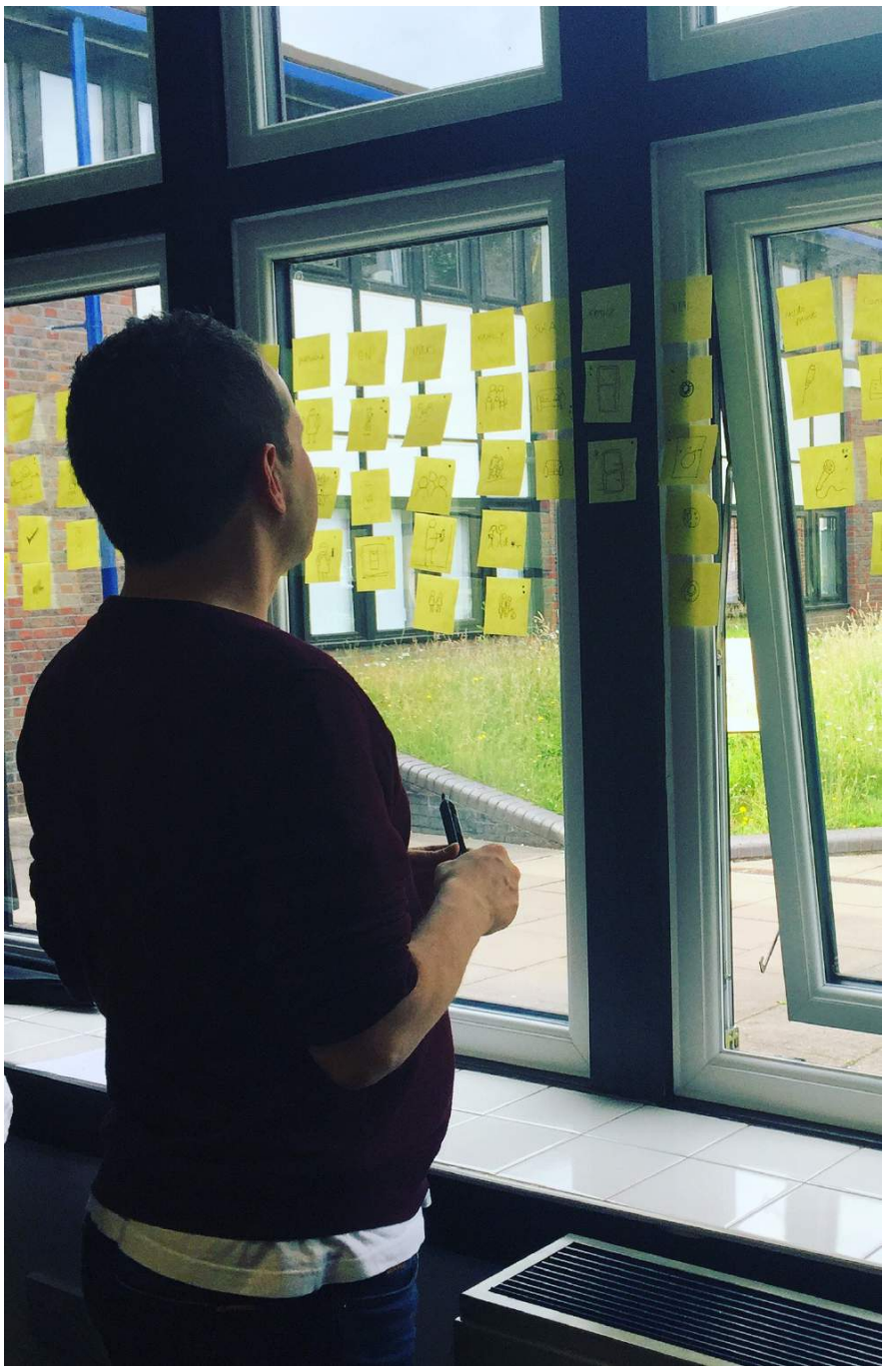
Introduction

The talks presented in this book were delivered as part of a summer school held at Royal Holloway University of London between the 20th and the 23rd of June 2016. The focus of the summer school was social aspects of cyber security risk and was an engagement and dissemination activity for the EU FP7 project, TREsPASS. The TREsPASS project was focused on developing methods to quantitatively assess cyber security risks from both technical and social perspectives and this summer school invited a number of prominent speakers from academia and industry to present an aspect of the social perspective.

Since the mid-1990s, the assessment and treatment of risk in the context of information management has been economically and technically focused. This focus has begun to change as technology and network communications have become pervasive and ubiquitous and access to technology can no longer be centrally controlled; in addition to economic and technical perspectives, risk is being understood from broader social, political and individual perspectives. This change has also been accompanied by a growing interest (in the social sciences and design discourse) in participatory methods of gathering and modelling information on risk and vulnerability. The talks at this summer school aimed to give doctoral students and post-doctoral researchers part of this wider perspective.

The summer school was organised by two researchers, Peter Hall (design) and Lizzie Coles-Kemp (information security), who have design and social science interests in cyber security risk. Peter and Lizzie led a team of designers as part of the TREsPASS project and in this work confronted the challenges of fleshing out the social landscape in which to explore and evaluate cyber security risk. In the spirit of the design-orientated work that they led on the TREsPASS project, the programme presents different perspectives on the social, political and individual aspects of risk and summaries of those talks are presented in this book. During the summer school we worked with illustrator and researcher Miriam Sturdee to visually represent the content of each talk. The students who took part in this summer school came from several disciplines and by producing infographics for each talk, we intend to produce an artefact that will stimulate further reflection and that can be used by each discipline as well as in interdisciplinary discussion.

Lizzie Coles-Kemp
Information Security Group
Royal Holloway University of London

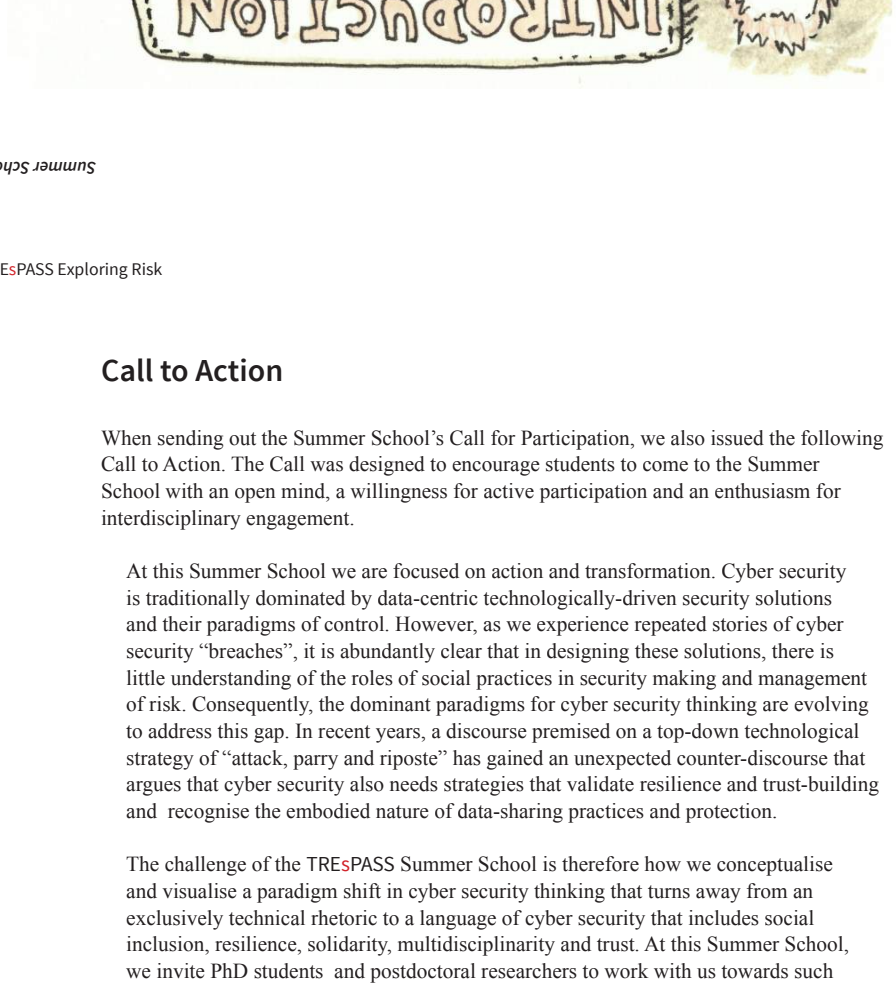


Call to Action

When sending out the Summer School's Call for Participation, we also issued the following Call to Action. The Call was designed to encourage students to come to the Summer School with an open mind, a willingness for active participation and an enthusiasm for interdisciplinary engagement.

> At this Summer School we are focused on action and transformation. Cyber security is traditionally dominated by data-centric technologically-driven security solutions and their paradigms of control. However, as we experience repeated stories of cyber security "breaches", it is abundantly clear that in designing these solutions, there is little understanding of the roles of social practices in security making and management of risk. Consequently, the dominant paradigms for cyber security thinking are evolving to address this gap. In recent years, a discourse premised on a top-down technological strategy of "attack, parry and riposte" has gained an unexpected counter-discourse that argues that cyber security also needs strategies that validate resilience and trust-building and recognise the embodied nature of data-sharing practices and protection.
>
> The challenge of the TREsPASS Summer School is therefore how we conceptualise and visualise a paradigm shift in cyber security thinking that turns away from an exclusively technical rhetoric to a language of cyber security that includes social inclusion, resilience, solidarity, multidisciplinarity and trust. At this Summer School, we invite PhD students and postdoctoral researchers to work with us towards such a transformational change through a programme of interdisciplinary talks and workshops that encourage hands-on engagement with the concepts presented in the Summer School talks.
>
> To help us work together to conceptualise and visualise a cyber security paradigm shift we have invited speakers from a wide range of disciplines.

The following pages present each of the talks given. Each description presents the talk's title, abstract, speaker bio and an infographic reflecting the content of the talk. Each infographic was drawn by Miriam Sturdee.



LEGO modelling with Pallion Action Group, Sunderland

Literatures of Risk

We asked our speakers to cite the literatures of risk that they felt were most relevant to the theme of the Summer School. Our speakers came up with the following list:

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.

Adams, J. (1999). Cars, cholera, and cows. *Policy Analysis*, (335), 1-49.

Amoore, L. (2013). *The politics of possibility: Risk and security beyond probability*. Duke University Press.

Baskerville, R. (1991). Risk analysis as a source of professional knowledge. *Computers & Security*, 10(8), 749-764

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). Sage.

Bouk, D. (2015). *How our days became numbered*. Chicago: Chicago University Press.

Castells, M. (1996) The Rise of the Network Society, *The Information Age: Economy, Society and Culture* Vol. I. Oxford, UK: Blackwell.

Crawford, K. (2014). *The anxieties of big data* : http://thenewinquiry.com/essays/the-anxieties-of-big-data/

Denney, D. (2005). *Risk and society*. Sage.

French, J. (2011). Why nudging is not enough. *Journal of Social Marketing*, 1(2), 154-162.

Gehmann, U., & Reiche, M. (Eds.). (2014). *Real Virtuality: About the Destruction and Multiplication of World (with a Preface by Gerd Stern)* (Vol. 37). transcript Verlag.

Gregory, D. (1994). *Geographical Imaginations*. Cambridge, MA: Blackwell.

Hoogensen, G., & Rottem, S. V. (2004). Gender identity and the subject of security. *Security dialogue*, 35(2), 155-171.

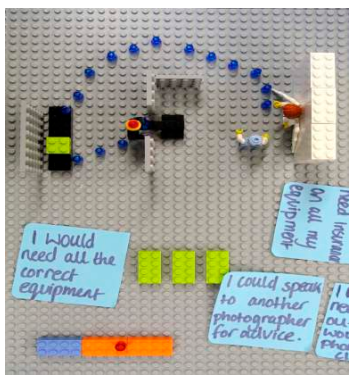
McSweeney, B. (1999). *Security, identity and interests: a sociology of international relations* (Vol. 69). Cambridge University Press.

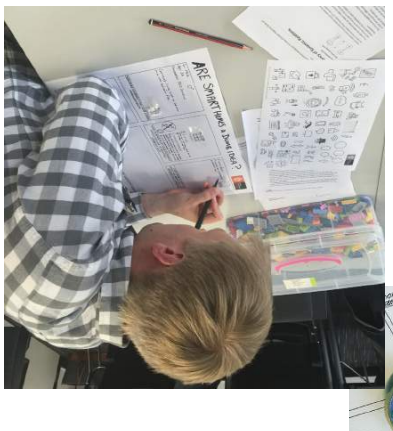
November, V., Camacho-Hübner, E., & Latour, B. (2010). Entering a risky territory: Space in the age of digital navigation. *Environment and Planning D: Society and Space*, 28(4), 581-599.

Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering & System Safety*, 59(1), 49-62.

Schaarner, C. O. (2009). *Theory U: Learning from the future as it emerges*. Berrett-Koehler Publishers

Summer School attendees try out LEGO, storyboarding and entering data into digital prototypes (the ANM)



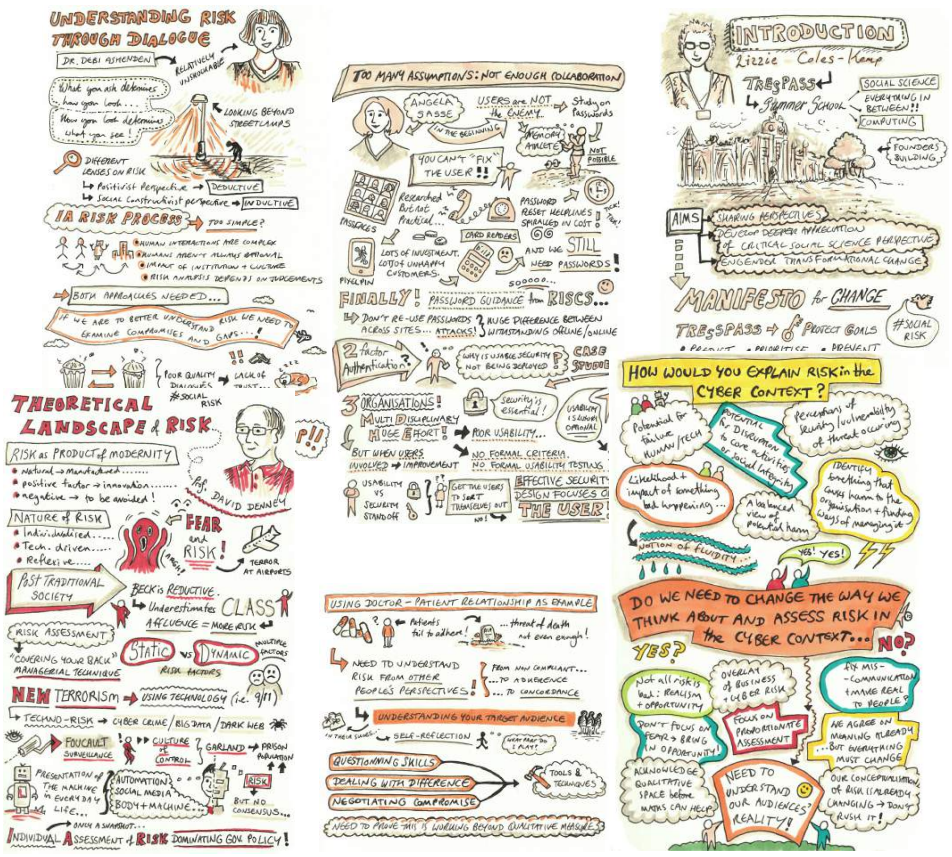


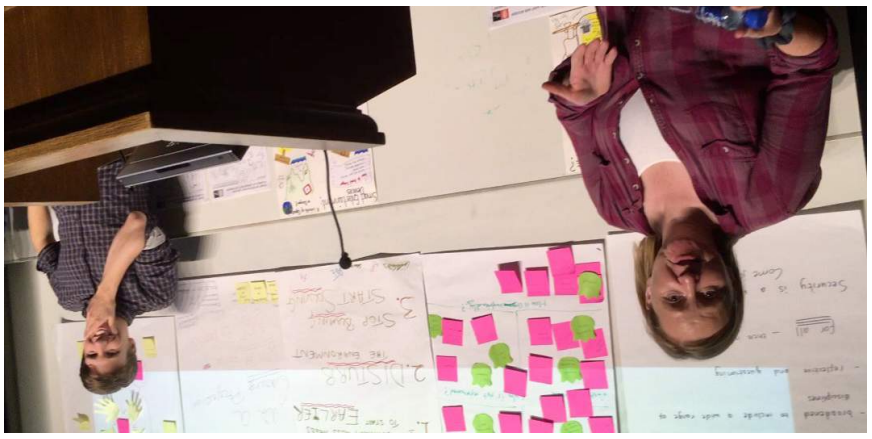
Summer Groups presented their findings on key questions, having developed comic strip narratives during the workshop.

Sketchnoting Cyber Security Research

Miriam Sturdee

Approaching an unfamiliar topic to sketchnote can be a daunting prospect, especially if that topic contains a great deal of technical information and is pitched at a high level. Having a good overview of the event helps, followed by reading all of the speaker biographies and details. Afterwards, spending some time preparing the page with the title from the programme and a space for a speaker portrait is a common approach to sketch noting – after which you can really get stuck into the presentation. I take a very much simple approach when faced with the unknown – start drawing and work my way straight down the page. You don't have to stick to one page of work, but I love the way they form succinct mini-summaries – although sometimes a speaker has so much interesting work that you just have to go over! The best thing about working on the social risk theme was just how much I learnt whilst making the notes, and how much sketch noting enables you to recall afterward. The other great thing is having truly engaged and exciting speakers who are passionate about their work – great presenters almost sketchnote themselves.





Professor Peter Adey & Dr Rikke Jensen
Royal Holloway University of London
Geography

Blu-tack, Mobile Phones and an RAF Base: creative practice and social media in the UK military

In this presentation we explore the relationship between social media and risk through a military community examining how different members of that community conceptualise particularly risky spaces, objects, people, networks and structures. While the military has tended to perceive social media as a potential risk worthy of practices that seek to securitise social media technologies (such as mobile phones), those who use them, and the apparently leaky spaces through which social media is performed, there is strong evidence to suggest that the practices and systems that have attempted to curtail social media risks are rather counter-productive. We illustrate the erosion of personnel and family well-being, morale and trust in the military institution, as well as the production of subversive practices that creatively find ways around the military's efforts to police them, from junior personnel to senior management.

Peter Adey is Professor of Human Geography at Royal Holloway University of London. His research sits at the interface of cultural and political geography with a particular interest in the relationship between mobility and security in various modes of suspension: from histories of flight and the aerial view; to military personnel and their families caught in the limbo of their itinerant lives; to the technologies and techniques of emergency and evacuation.

Rikke Bjerg Jensen is a post-doctoral researcher in the School of Law, Royal Holloway University of London. Her research positions itself in the intersection of new media studies, sociology/ criminology and geography, thus, blurring boundaries between a number of discreet areas of study. More specifically, her work focusses on the relationship between media, defence and security, and the mediatisation of conflict and crisis. She has undertaken extensive fieldwork within defence and security organisations such as the UK military and NATO in order to explore how approaches to and policies on emerging media are formulated, implemented and maintained.

Craig Templeton
Information Security Office, ANZ Bank
Security Enablement

"Everyone Has a Plan..." : Why is Cyber-risk Hard?

The world is connected like never before – "always-on, always available". This hyper-connectivity has enabled new business models to emerge such as the sharing economy and utility computing. The velocity of change and scale at which services can be delivered has equally been harnessed by criminals, protestors, political dissidents and governments. Risks related to digital activity are no longer isolated to an industry segment or single businesses but are now systemic and pervasive. This is further compounded by a growing reliance on technology rather than being assisted by it. This talk discusses how these factors come together to call into question the effectiveness of traditional approaches to identifying and evaluating security risks and prompt security practitioners to reach out for new approaches to conceptualising and examining cyber security risk.

Craig is a graduate of Computer Science from the University of Ulster in Northern Ireland and is regularly invited to speak at industry conferences on the topic of cyber security. Emigrating from Ireland to Australia in March 2010, Craig joined ANZ bank where he has been Manager, Strategy Manager, and more recently Principal, Cyber Security Research. This role involves understanding industry trends, emerging technologies, and determining the potential impact of threats to the bank for future investment. In 2015, Craig was awarded Information Security Professional of the Year at the Australian Information Security Association (AISA) National Conference in Melbourne for his work promoting cyber security as a human problem and not a purely technical discipline.

Craig's current role as Head of Security Enablement is focused on establishing strategic partnerships with leading academic and research institutes that provides ANZ with insight into leading approaches to solving cyber security problems, particularly concerning secure behaviours and culture change. His professional interests include the challenge of securing the human perimeter, the psychology of cyber security and cultural change; he is currently an advisor to several international research initiatives centred on human aspects of security.

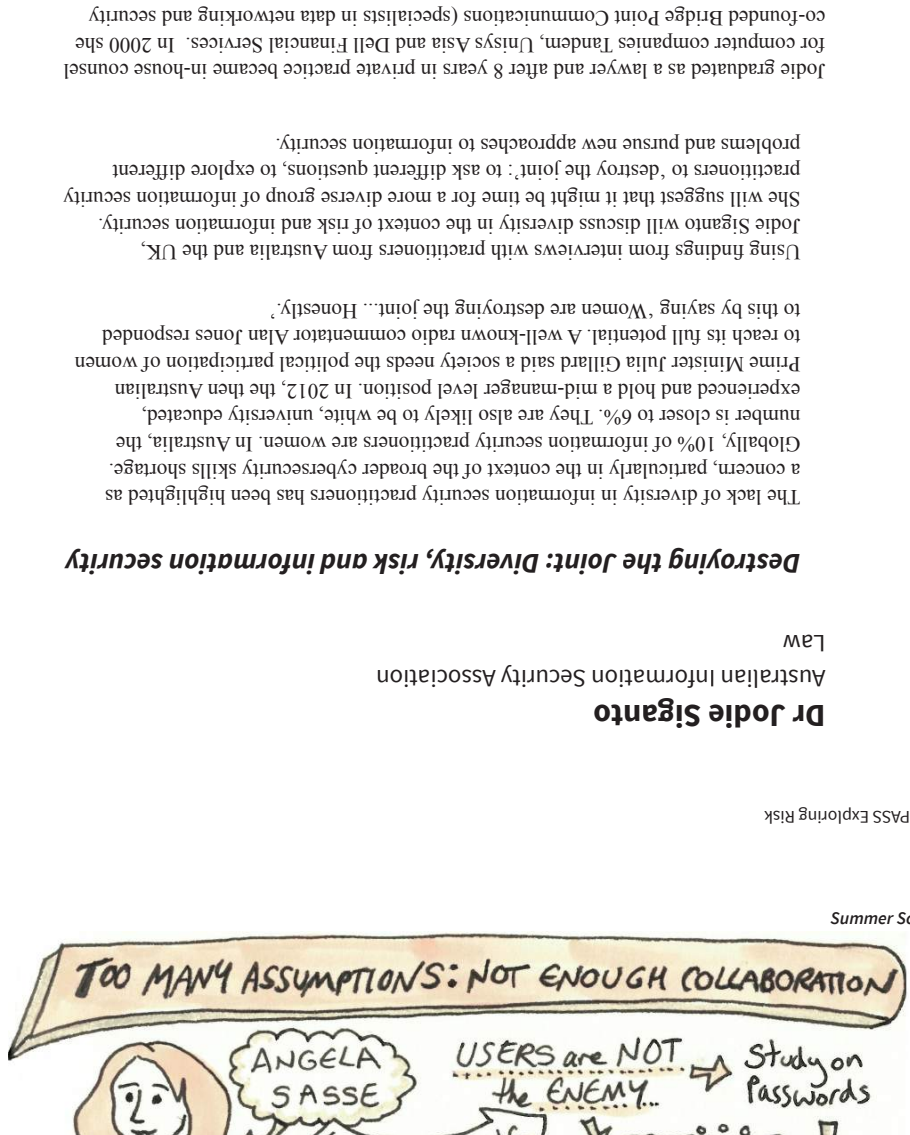
Craig curates a security blog on Flipboard called the "Book of Security Foo".

Professor Debi Ashenden
University of Portsmouth
Cyber Security

Understanding Risk Through Dialogue

The quality of the working relationship between security and the business is a key factor in ensuring the effectiveness of cyber security processes. When a project works well it is because these working relationships are underpinned by mutual trust and there is full disclosure of factors that may impact on risk. When trust is lacking, however, the process suffers: project stakeholders do not engage early enough; insufficient time is available to implement security and an incomplete view is formed of risks to the business. If the issue of trust is not addressed, there is a real danger that security arguments will be ignored or overlooked in the drive to meet business needs and exploit novel technologies. Improving security dialogues, however, between security practitioners and end users builds constructive interactions that have an overall positive benefit for the security posture of an organisation. This session will start with an interactive exercise before moving on to discuss ongoing work researching how to improve security dialogues.

Debi is Professor of Cyber Security in the School of Computing at the University of Portsmouth. Until recently she was previously Head of the Centre for Cyber Security & Information Systems at Cranfield University at the Defence Academy of the UK where she was responsible for the MSc in Cyber Defence & IA (which has provisional certification from GCHQ) and the MSc in Cyberspace Operations. She is the CREST lead for Protective Security & Risk. Debi is also the first National Technical Authority Fellow appointed by CESG. Debi has had a number of articles on information security published, presented at a range of conferences and has co-authored a book for Butterworth Heinemann, 'Risk Management for Computer Security: Protecting Your Network & Information Assets'. Her research has been funded by: EPSRC, ESRC, Technology Strategy Board, Home Office, Fujitsu, Police IT Organisation, MoD, DTI, Cabinet Office, Dstl and CESG.



Dr Jodie Siganto
Australian Information Security Association
Law

Destroying the Joint: Diversity, risk and information security

The lack of diversity in information security practitioners has been highlighted as a concern, particularly in the context of the broader cybersecurity skills shortage. Globally, 10% of information security practitioners are women. In Australia, the number is closer to 6%. They are also likely to be white, university educated, experienced and hold a mid-manager level position. In 2012, the then Australian Prime Minister Julia Gillard said a society needs the political participation of women to reach its full potential. A well-known radio commentator Alan Jones responded to this by saying 'Women are destroying the joint... Honestly.'

Using findings from interviews with practitioners from Australia and the UK, Jodie Siganto will discuss diversity in the context of risk and information security. She will suggest that it might be time for a more diverse group of information security practitioners to 'destroy the joint': to ask different questions, to explore different problems and pursue new approaches to information security.

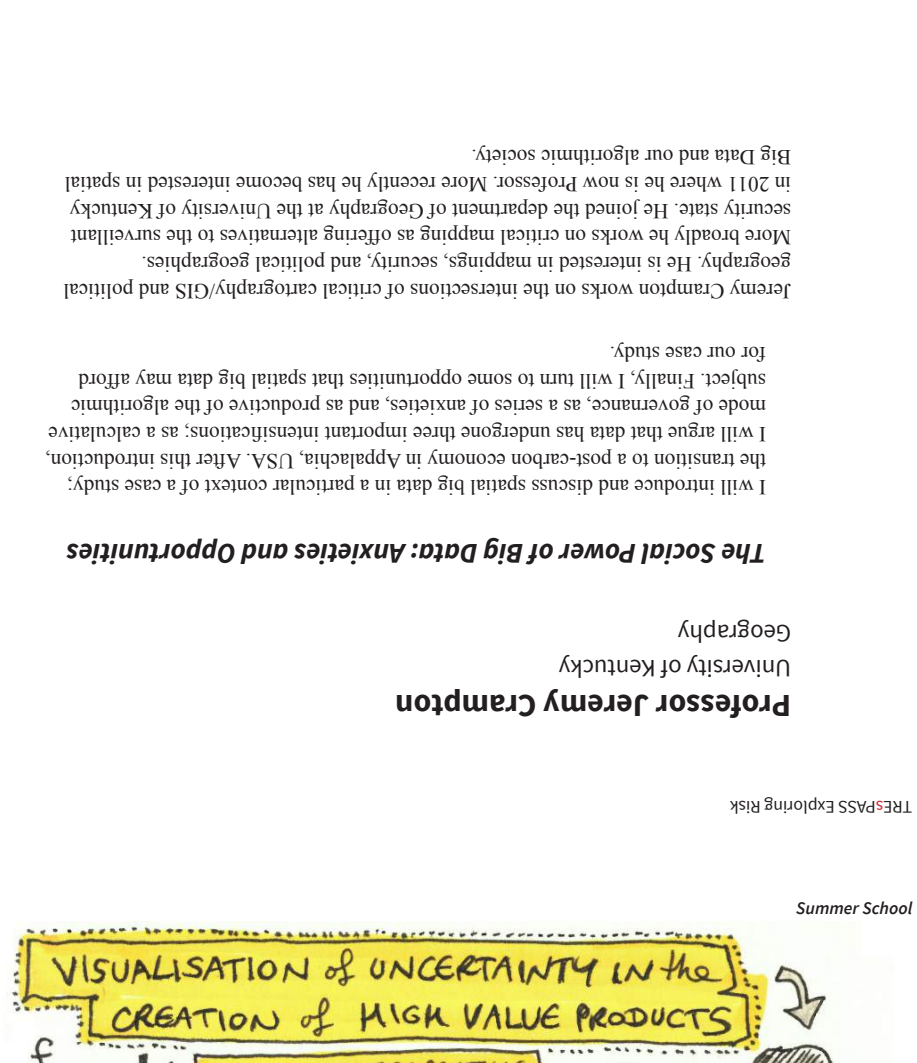
Jodie graduated as a lawyer and after 8 years in private practice became in-house counsel for computer companies Tandem, Unisys Asia and Dell Financial Services. In 2000 she co-founded Bridge Point Communications (specialists in data networking and security services) where she worked in security management consultancy. Following her time at Bridge Point, Jodie has led IT Security Training Australia, a company delivering training and education in privacy and data, focusing on the intersection of law and technology. Completing a PhD at QUT in 2015, Jodie has been an active researcher into information security issues, contributing to a range of projects including the Cyber Security Cartographies Downunder study with colleagues from Royal Holloway University of London and most recently working on a report into the Australian cyber security skills shortage for the Australian Information Security Association (AISA). In 2016, Dr Siganto was appointed Director, AISA Cyber Security Academy where she is responsible for ensuring that Australian public and private organisations are well served by a skilled and knowledgeable cyber security workforce.

Dr Matt Butchers
Knowledge Transfer Network
Knowledge Transfer

Visualisation of Uncertainty in the Creation of High Value Products

New paradigms in virtual engineering are allowing engineers to handle uncertainties in manufacturing in a systematic way. Designs can be created which are robust to these uncertainties and confidence can be built in early design concepts for mitigating the risk these uncertainties introduce. Despite this promise there exist multiple difficulties in communicating uncertainty and risk in multi-disciplinary organisations which is a key road block for the uptake in uncertainty-savvy design.

Matt leads the industrial mathematics and uncertainty quantification & management communities in the Knowledge Transfer Network; the UK's organisation for bridging the gap between academia, Government, and industry. We aim to boost the UK economy by capturing the impact of innovative ideas. Matt is an experimental physicist who has worked across academia, industry and Government and is well connected across these stakeholders.

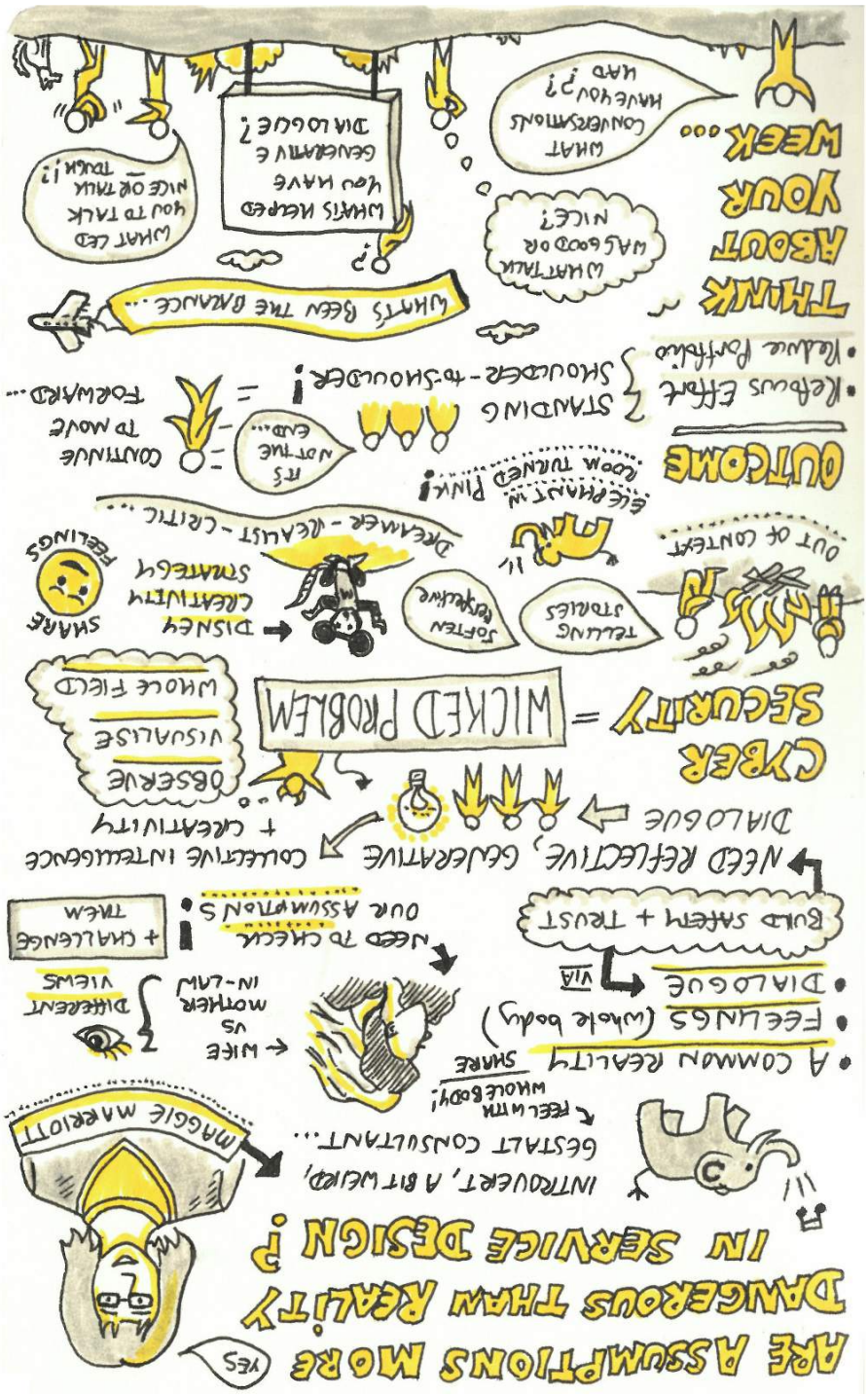


Professor Jeremy Crampton
University of Kentucky
Geography

The Social Power of Big Data: Anxieties and Opportunities

I will introduce and discuss spatial big data in a particular context of a case study; the transition to a post-carbon economy in Appalachia, USA. After this introduction, I will argue that data has undergone three important intensifications; as a calculative mode of governance, as a series of anxieties, and as productive of the algorithmic subject. Finally, I will turn to some opportunities that spatial big data may afford for our case study.

Jeremy Crampton works on the intersections of critical cartography/GIS and political geography. He is interested in mappings, security, and political geographies. More broadly he works on critical mapping as offering alternatives to the surveillant security state. He joined the department of Geography at the University of Kentucky in 2011 where he is now Professor. More recently he has become interested in spatial Big Data and our algorithmic society.



Professor Angela Sasse
University College London
Human Centred Security

Too Many Assumptions: Not Enough Collaboration

Within less than two decades, the Internet and mobile communications have become an integral part of business and people's lives. Most transactions are now carried out online, and criminals have followed 'because that's where the money is'. Security specialists develop policies and security mechanisms to stop them, but find in practice that people make mistakes, or don't comply with the instructions. We now know that treating people as components whose behaviour can be mandated is unrealistic. In this talk, I will show this does not only apply to so-called 'end-users' – consumers and citizens – but the people involved in the design and implementation of technology, and propose changes to knowledge, skills and practices that we need to initiate to make progress.

M. Angela Sasse FREng is the Professor of Human-Centred Technology in the Department of Computer Science at University College London, UK. She read psychology in Germany and obtained an MSc in Occupational Psychology from Sheffield University before obtaining a PhD in Computer Science from the University of Birmingham. sShe started investigating the causes and effects of usability issues with security mechanisms in 1996. Her 1999 seminal paper with her then Phd student Anne Adams, *Users are Not the Enemy*, is the most cited paper in usable security. She became a full professor in 2003, and has led several multi-disciplinary projects, working with economists, mathematicians and crime scientists. She worked with many international companies and received Faculty Awards from Intel in 2012 and IBM in 2013. She became Director of the UK Research Institute for Science of Cyber Security (RISCS), co-funded by the EPSRC and GCHQ in 2012, and was elected a Fellow of the Royal Academy of Engineering in 2015.

Conn Crawford
Sunderland City Council
Client Development

Public Service Design and Risk

Sunderland is a mid-sized ‘Key City’ in the North of England. It produces more cars than the whole of Italy and has a growing technology scene. However, it also sustains chronic ill-health, persistent deprivation, declining and ageing populations and a growing skills gap. The impact of central government’s programme of austerity and the emergence of the Community Leadership Council, the new ‘Sunderland way of working’ has become that of being prepared and able to let others lead. This change in position has meant that perceptions of value, security, trade-offs and complexity, all of which are fundamental to a position on risk, have changed. Approaches to co-creation and co-maintenance, ecosystems and marketplaces are emerging as new forms of service design and also results in the need for changes to evaluating risk. In this talk I shall present this context and discuss with the summer school participants how we might have better discussions on risk management, safeguards, gateways and other controls in this new reality and ask in what ways might the risk proposition might they be made more compelling and sustainable for participants?

Conn Crawford is a veteran of almost thirty years in North East local government services, with spells in economic and community development merging into ICT around the turn of the millennium, when he joined Sunderland City Council. Conn feels that council’s emerging role as a Community Leadership Council – convening communities of interest as well as of place and combining intelligence use of service data with support for commissioning and innovation, is a case-study for the realisation of Trusted Services. Conn currently leads on next generation (5G) connectivity for the North East Combined Authority and has collaborated with RHUL since working with Lizzie on the EPSRC/ESRC/TSB funded VOME project in 2008.

Maggie Marriott
Enki Consultants
Organisational Change

Are Assumptions More Dangerous Than Reality in Service Design?

In today’s business when we’re working at a frenetic pace with less funding, less people and more demands to deliver it seems easier to build products and services based on our assumptions. It’s hard to remember the importance of stopping to check our assumptions, to see the reality of the situation and the urgent need to change. Instead our psychological immune system closes our minds.

In this talk I’ll reflect on how I believe changing conversations and examining our assumptions together enables us to keep an open mind as we design services through mutual helping. I’ll use illustrations from my own work in Government to explain how I encourage highly technical leaders to include more reflective and generative dialogue in their service design.

Maggie Marriott is an independent business consultant and coach who is passionate about bringing humane approaches to organisational and business change. She has worked extensively in the private and public sector, especially in Security and Intelligence. Although Maggie started out as a programmer and technical analyst her desire to build systems for the people that need them has led her to specialise in the psychology and philosophy of change in organisations.

Summer School

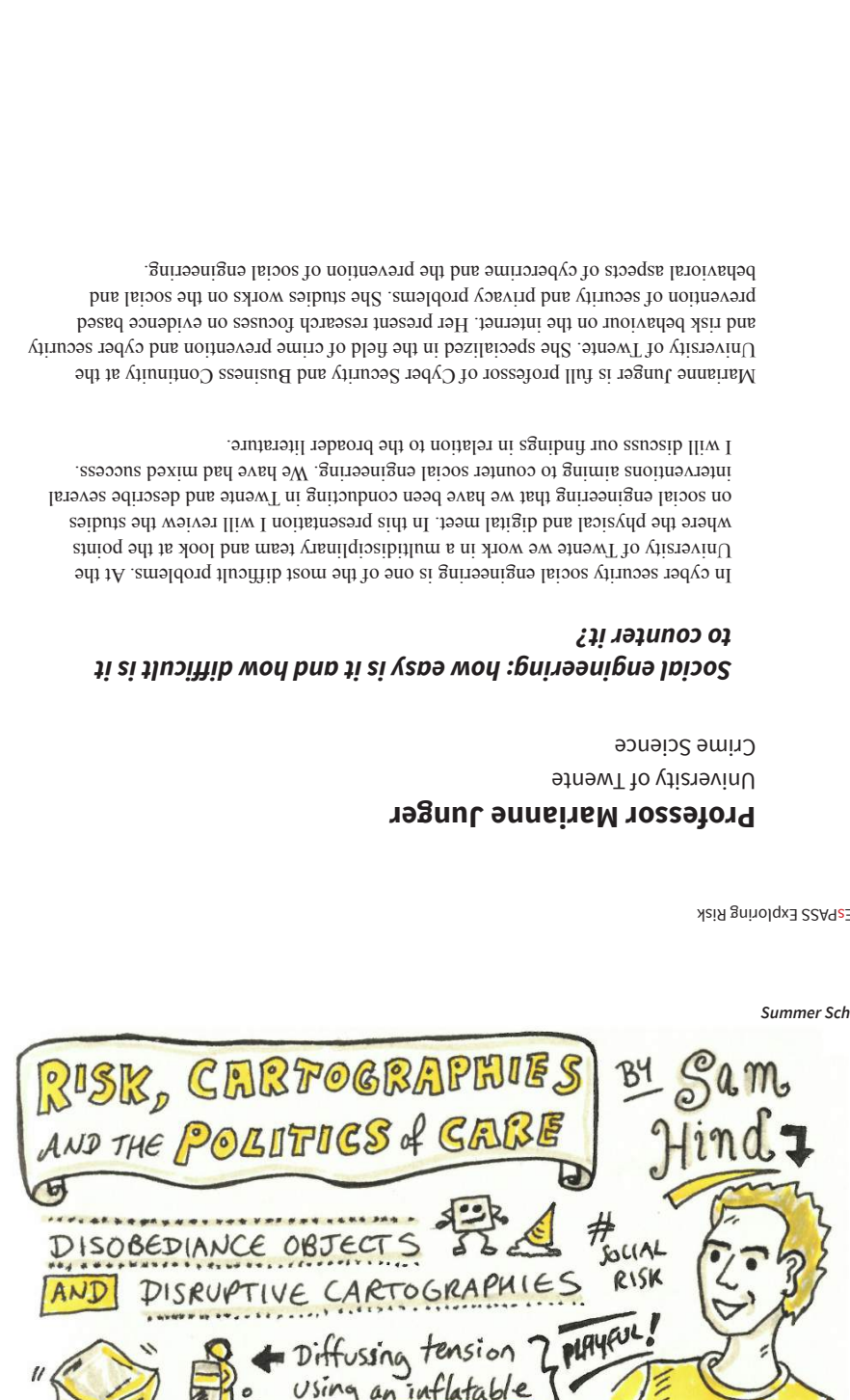
Professor David Denney

Royal Holloway University of London
Social and Public Policy

The Theoretical Landscape of Risk

The lecture focuses on the background to the emergence of a form of risk reflecting a new modernity. Drawing on the work of Ulrich Beck it focuses upon increased individualisation, reflexivity and technological determinism. It describes how manufactured risks are more fluid and all pervasive than had hitherto been the case. Liquid risks are now central to forms of employment and conceptions of what constitutes education.

Professor David Denney has extensive experience of conducting large scale international interdisciplinary research in both the private and public sectors. He has written extensively on theories of risk and the impact of perceptions of risk in society. Much of his empirical work has been concerned with human behaviour in the workplace. He was co-investigator on an ESRC-funded project which examined the impact of various forms of violence on professionals in the workplace (1998-2001). The research had a direct impact on policy formulation within the health services. He has also conducted work funded by the Canadian High Commission on various aspects of judicial perceptions. More latterly, he has developed an interest in cyber security and the workplace. He was the principal investigator on an ESRC-Dstl funded interdisciplinary project on the use of social media by the UK military (2013-2015). This project was conducted in the UK, the Falkland Islands and Cyprus. He is currently the principal investigator on a large-scale project funded by GSK, which investigates the impact of information protection training on cyber behaviour in the workplace.



Professor Marianne Junger

University of Twente
Crime Science

Social engineering: how easy is it and how difficult is it to counter it?

In cyber security social engineering is one of the most difficult problems. At the University of Twente we work in a multidisciplinary team and look at the points where the physical and digital meet. In this presentation I will review the studies on social engineering that we have been conducting in Twente and describe several interventions aiming to counter social engineering. We have had mixed success. I will discuss our findings in relation to the broader literature.

Marianne Junger is full professor of Cyber Security and Business Continuity at the University of Twente. She specialized in the field of crime prevention and cyber security and risk behaviour on the internet. Her present research focuses on evidence based prevention of security and privacy problems. She studies works on the social and behavioral aspects of cybercrime and the prevention of social engineering.

Professor Dieter Gollman

Hamburg University of Technology
Computer Science

Cyber-physical systems security in the smart home

We argue that cyber-physical systems (CPS) cannot be protected just by protecting their IT infrastructure and that the CIA approach familiar from communications security is insufficient in CPS security. Rather, the IT components should be treated as a control system, inputs to that control system should be checked for veracity, and control algorithms should be designed in a way that they can handle a certain amount of adversarial actions. We will take examples from the smart home to illustrate some open research questions that need to be addressed in this domain.

Dieter Gollmann Dipl.-Ing. Dr.techn. (Linz) Dr.habil. (Karlsruhe) received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.tech. (1984) from the University of Linz, Austria, where he was a research assistant in the Department for System Science. He was a Lecturer in Computer Science at Royal Holloway, University of London, and later a scientific assistant at the University of Karlsruhe, Germany, where he was awarded the 'venia legendi' for Computer Science in 1991. He rejoined Royal Holloway in 1990, where he was the first Course Director of the MSc in Information Security. He joined Microsoft Research in Cambridge in 1998. In 2003, he took the chair for Security in Distributed Applications at Hamburg University of Technology, Germany. Dieter Gollmann is an editor-in-chief of the International Journal of Information Security and an associate editor of the IEEE Security & Privacy Magazine. His textbook on 'Computer Security' has appeared in its third edition.

Sam Hind

University of Warwick
Cartography and Digital Mapping

Risk, Cartographies and the Politics of Care

In this talk I want to explore some conceptual connections between risk, cartography and care. I want to start this by discussing two terms: 'disobedient objects' and what I call 'disruptive cartographies'. Each of these can help us to understand the limitations of thinking about disobedience and disruption without necessarily thinking of their antonyms too. In every disobedient or disruptive act is a similar attention towards, rather than absence of or move away from, obedience and order. In fact, as I argue, both are entirely reliant upon the generation of such in combination with these 'dis-' actions. A more appropriate way of conceiving this is to consider how disobedience and disruption are as equally orientated towards generating forms of care and attention as they are towards ever-riskier outcomes. Care has a rich conceptual, feminist history that must, therefore, be mobilized in this instance. In other words: how might we consider cyber-security and risk in light of feminist or care and attention as they are towards ever-riskier outcomes. Care has a rich conceptual, feminist history that must, therefore, be mobilized in this instance. In other words: how might we consider cyber-security and risk in light of feminist conceptions of care? What might it – or does it – mean to care in a digital world? Further, how might care expand on notions of trust, disclosure and responsibility? Only recently have theorists begun to mobilize conceptualizations of care beyond traditional sites and forms of care-work (typically gendered in their operation) – primarily as a counter-strategy to forms of austerity politics. This presentation offers some tentative suggestions as to what a 'care-tographic' project might entail.

Sam Hind is a Teaching Fellow at the University of Warwick. He recently completed his PhD in the Centre for Interdisciplinary Methodologies. His research focuses on mobile, digital mapping technologies and their impact on everyday life.