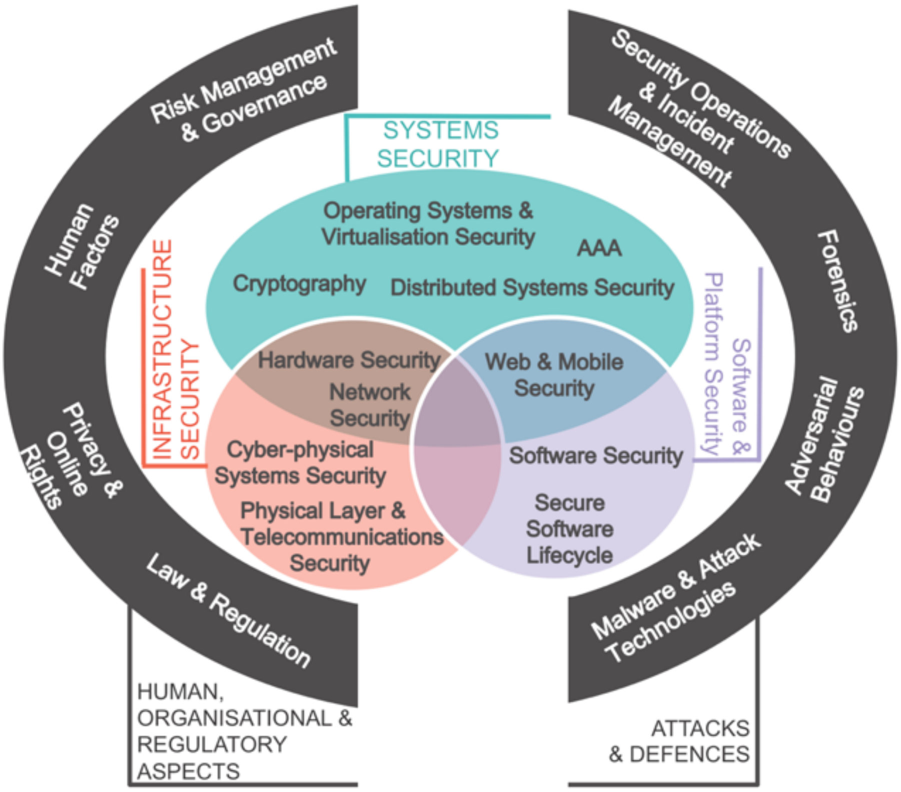
CYBER SECURITY AT SCALE: CHALLENGES FOR RESEARCH, EDUCATION AND TRAINING

Report from the first CyBOK community workshop held on 30 October 2019, Bristol, UK
Awais Rashid, Lata Nautiyal, Yvonne Rigby (University of Bristol)

The Cyber Security Body of Knowledge (CyBOK) project[1] aims to codify foundational knowledge in cyber security. Since February 2017, the project has undertaken a range of community consultations to define the scope of CyBOK[2]. Following the scoping exercise, the project has brought together 110 authors, reviewers, advisors as well as over 1400 comments from the wider community to develop CyBOK 1.0 which comprises 19 Knowledge Areas organised into five broad categories.

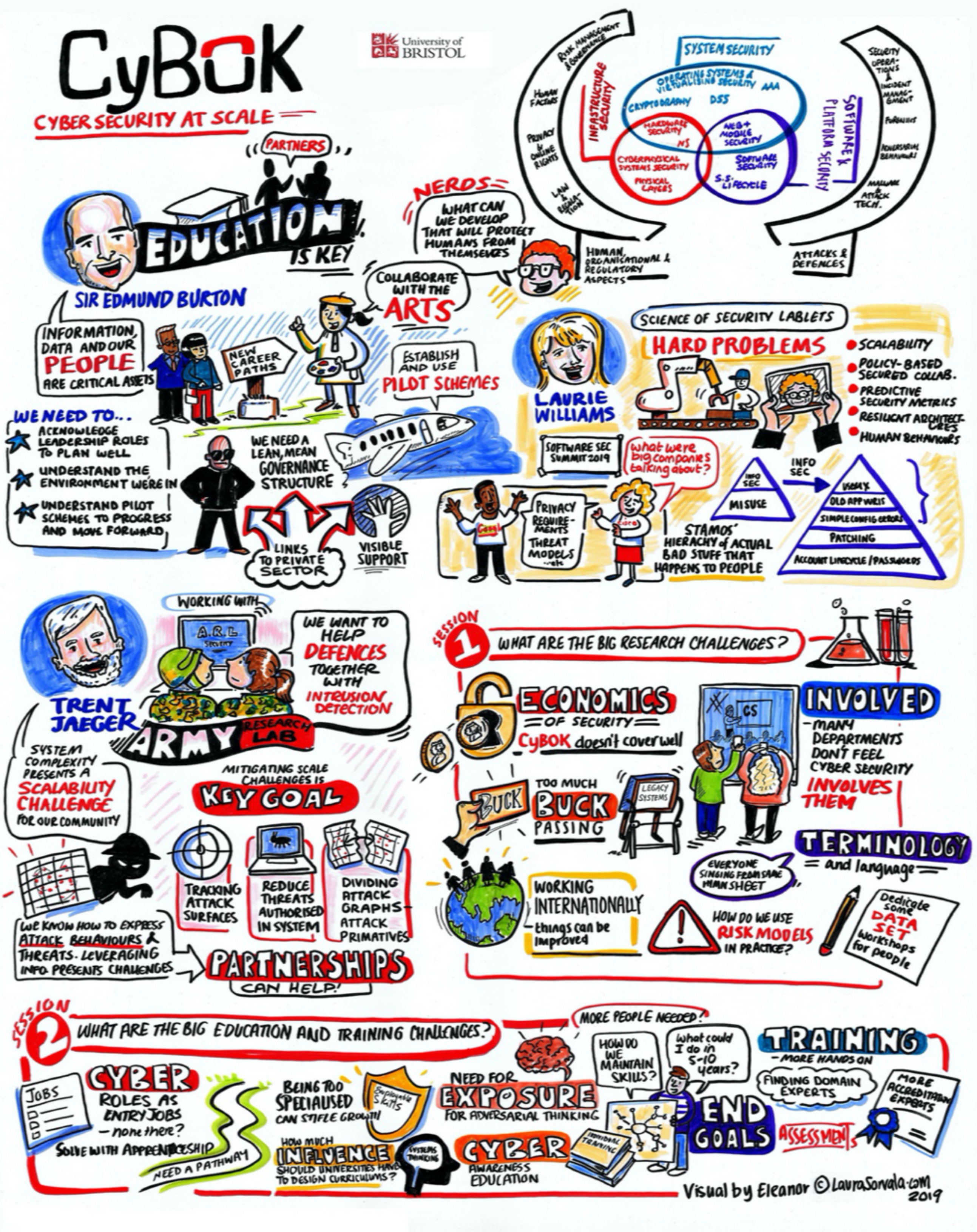

Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Cyber-physical Systems Security
Physical Layer & Telecommunications Security
Web & Mobile Security
Software Security
Secure Software Lifecycle
Software & Platform Security
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

The first community workshop and showcase took place on the 30 October 2019 at the University of Bristol, following the release of CyBOK version 1.0. The purpose of the workshop and showcase was to introduce CyBOK 1.0 to 30 key stakeholders from industry, academia and government and discuss future research, education and training challenges for cyber security that crosscut the five broad categories within CyBOK.

This report summarises the series of talks in the morning that set the scene for the group discussions amongst gathered stakeholders in the afternoon. An artist – acting as a graphic note-taker – captured the key themes of discussions visually.

[1] https://www.cybok.org/

[2] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, Claudia Peersman: Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy 16(3): 96-102 (2018)


CyBOK
CYBER SECURITY AT SCALE
University of BRISTOL
PARTNERS
EDUCATION IS KEY
SIR EDMUND BURTON
INFORMATION, DATA AND OUR PEOPLE ARE CRITICAL ASSETS
NEW CAREER PATHS
COLLABORATE WITH THE ARTS
ESTABLISH AND USE PILOT SCHEMES
NERDS
WHAT CAN WE DEVELOP THAT WILL PROTECT HUMANS FROM THEMSELVES
WE NEED TO...
ACKNOWLEDGE LEADERSHIP ROLES TO PLAN WELL
UNDERSTAND THE ENVIRONMENT WE'RE IN
UNDERSTAND PILOT SCHEMES TO PROGRESS AND MOVE FORWARD
WE NEED A LEAN, MEAN GOVERNANCE STRUCTURE
LINKS TO PRIVATE SECTOR
VISIBLE SUPPORT
RISK MANAGEMENT & GOVERNANCE
HUMAN FACTORS
PRIVACY & ONLINE RIGHTS
LAW & REGULATION
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
INFRASTRUCTURE SECURITY
SYSTEM SECURITY
OPERATING SYSTEMS & VIRTUALISING SECURITY
AAA
CRYPTOGRAPHY
DSS
HARDWARE SECURITY
NS
CYBERPHYSICAL SYSTEMS SECURITY
PHYSICAL LAYERS
WEB + MOBILE SECURITY
SOFTWARE SECURITY
S.S. LIFECYCLE
SOFTWARE & PLATFORM SECURITY
SECURITY OPERATIONS & INCIDENT MANAGEMENT
FORENSICS
ADVERSARIAL BEHAVIOURS
MALWARE & ATTACK TECH.
ATTACKS & DEFENCES
SCIENCE OF SECURITY LABLETS
HARD PROBLEMS
SCALABILITY
POLICY-BASED SECURED COLLAB.
PREDICTIVE SECURITY METRICS
RESILIENT ARCHITECTURES
HUMAN BEHAVIOURS
LAURIE WILLIAMS
SOFTWARE SEC SUMMIT 2019
what were big companies talking about?
PRIVACY REQUIREMENTS
THREAT MODELS
..etc
STAMOS' HIERACHY of ACTUAL BAD STUFF THAT HAPPENS TO PEOPLE
INFO SEC
MISUSE
INFO SEC
VSUMX
OLD APP VULNS
SIMPLE CONFIG ERRORS
PATCHING
ACCOUNT LIFECYCLE / PASSWORDS
TRENT JAEGER
WORKING WITH
A.R.L SECURITY
ARMY RESEARCH LAB
WE WANT TO HELP DEFENCES TOGETHER WITH INTRUSION DETECTION
SYSTEM COMPLEXITY PRESENTS A SCALABILITY CHALLENGE FOR OUR COMMUNITY
MITIGATING SCALE CHALLENGES IS KEY GOAL
TRACKING ATTACK SURFACES
REDUCE THREATS AUTHORISED IN SYSTEM
DIVIDING ATTACK GRAPHS - ATTACK PRIMATIVES
WE KNOW HOW TO EXPRESS ATTACK BEHAVIOURS & THREATS. LEVERAGING INFO. PRESENTS CHALLENGES
PARTNERSHIPS CAN HELP!
SESSION 1
WHAT ARE THE BIG RESEARCH CHALLENGES?
ECONOMICS OF SECURITY
CyBOK doesn't cover well
TOO MUCH BUCK PASSING
BUCK
LEGACY SYSTEMS
CS
INVOLVED
- MANY DEPARTMENTS DON'T FEEL CYBER SECURITY INVOLVES THEM
TERMINOLOGY and language
EVERYONE SINGING FROM SAME HYMN SHEET
WORKING INTERNATIONALLY
- things can be improved
HOW DO WE USE RISK MODELS IN PRACTICE?
Dedicate some DATA SET workshops for people
SESSION 2
WHAT ARE THE BIG EDUCATION AND TRAINING CHALLENGES?
MORE PEOPLE NEEDED!
HOW DO WE MAINTAIN SKILLS?
What could I do in 5-10 years?
TRAINING - MORE HANDS ON
FINDING DOMAIN EXPERTS
MORE ACCREDITATION EXPERTS
JOBS
CYBER ROLES AS ENTRY JOBS - none there?
SOLVE WITH APPRENTICESHIP
NEED A PATHWAY
BEING TOO SPECIALISED CAN STIFLE GROWTH
Employable Skills
NEED FOR EXPOSURE FOR ADVERSARIAL THINKING
HOW MUCH INFLUENCE SHOULD UNIVERSITIES HAVE TO DESIGN CURRICULUMS?
SYSTEMS THINKING
CYBER AWARENESS EDUCATION
INDIVIDUAL TRAINING
END GOALS
ASSESSMENTS
Visual by Eleanor ©LauraSorvala.com 2019

1 SETTING THE SCENE

Professor Awais Rashid from University of Bristol (Lead for the CyBOK project) opened the proceedings by providing a detailed overview of the scoping process that led to identification of the 19 Knowledge Areas (KAs) within CyBOK. He then discussed the process of developing each of the KAs before moving on to discussing the emerging large-scale highly connected infrastructures and the cyber security challenges they pose. Using CyBOK as a basis, he discussed the challenges that the field will face emerging from the scale of connectivity of such emerging and future infrastructures, the potential scale of attacks and associated disruptions and their impact on citizens and the economy. He also discussed the need for cyber security professionals to tackle such challenges – emphasising that there isn't a singular cyber security expert and different systems and sectors require different combinations of knowledge to address the cyber security challenges they face. Through various exemplars of academic and professional certification programmes, he highlighted how different cyber security professionals bring different combinations of knowledge from CyBOK and recognising and embracing such distinctions is key to addressing the cyber security workforce shortages nationally and globally.

Sir Edmund Burton, who chaired the CyBOK Professional Advisory Board during the development of CyBOK 1.0 and is currently chairing the CyBOK Steering Committee, noted that information, data and people are key assets. He noted that, in order to protect these, we need to understand the surrounding environment and its inherent complexities and acknowledge the need for leadership roles and diverse career paths. He highlighted the need for interdisciplinarity and partnerships across academia, industry and government and the importance of pilot schemes to test the potential of innovative ideas to meet the cyber security needs of the future.

Professor Laurie Williams, from North Carolina State University, USA, author of the CyBOK KA on Secure Software Lifecycle and currently a member of the Steering Committee, argued for the need to tackle hard problems using the Science of Cyber Security Lablets in the USA as an example. Specific problems she highlighted included scalability, resilient architectures, policy-based secured collaboration, human behaviours and the need for predictive security metrics. Using a keynote from USENIX Security Symposium as a reference, she highlighted that the research community often tackles a very small specialised proportion of a very large problem space and that there is a need for cyber security research advances that arise from the complexity of real-world systems and the constraints and trade-offs encountered in-the-wild.

Professor Trent Jaeger, from Pennsylvania State University, a member of the Academic Advisory Board for CyBOK 1.0 and currently a member of the Steering Committee, also raised the challenge of complexity – and that it presents a scalability challenge for the cyber security community. He noted the need for partnerships to mitigate such scalability challenges as tracking attack surfaces, reducing threats authorised in systems and improved techniques to reason about complex attacks.

2 CHALLENGES FOR RESEARCH, EDUCATION AND TRAINING

Following the scene setting talks, there were group discussions to elicit key challenges for research, education and training. The first set of group discussions focused on research challenges while the second on education and training. In each case, groups used the following questions as a guide:

- What are the big challenges (research or education & training) with regards to cyber security at scale – using the five CyBOK categories as broad themes?
- What are the drivers and barriers with regards to interdisciplinary and cross-sectoral collaboration to addressing them? How would progress be measured? What would be the success indicators?

Below we discuss findings from the two discussion sessions.

2.1 Key research challenges

Participants discussed the growing hyper-connectivity of the digital world – 'things' that are supposed to be simple physical objects are now transformed into 'smart objects', having the capability of sensing, processing and sending data. There was acknowledgement that, though the traditional security solutions are applicable, the scope of this applicability is limited. Consequently, the role of cyber security is no longer merely about securing the networks that service traditional enterprise systems but much larger and wider – encompassing the cyber-physical environment. Devices and smart objects in such cyber-physical settings need new security solutions, as the range and diversity of threats and attacks are evolving rapidly.

Coupled with this are the complex intersections between humans and technologies and how they shape the cyber security landscape. There was recognition that this required interdisciplinary approaches that combine expertise in social and behavioural sciences with traditional computer security and information security research to understand both human and organisational factors that shape cyber security.

Several key potential themes of research were identified and the importance of international collaboration was highlighted as a key to addressing them:

1. **Economics of cyber security at-scale.** There is a body of research on economics of information security and there is some coverage of this in the Introduction to CyBOK as a crosscutting theme. However, as we build more complex interconnected systems, how do we establish the trade-offs that are required to provide an optimal level of security – taking into account technical, organisational and human factors.
2. **The need to consider legacy systems.** This is a well-known challenge in the context of cyber-physical systems, especially those used in industrial environments and critical infrastructures. The systems were designed with little or no cyber security built-in as they weren't expected to be connected to other networked systems. With advances in technologies, need for remote monitoring and control and optimisation of business processes, they are increasingly connected to enterprise systems exposing their vul-

nerabilities to a range of threat actors. We already know that replacing such systems at scale is expensive and hard – often leading to a combination of legacy and non-legacy environments. However, today's contemporary systems are tomorrow's legacy systems and as we build complex infrastructures such as smart cities and autonomous transportation systems, we need to account for the long-term challenges of security combinations of legacy and non-legacy environments at scale.

3. **Positive security cultures.** Cyber security often suffers from *passing the buck*. Many departments in organisations do not think that cyber security involves them. As we build more complex systems, e.g., smart cities, where the infrastructure is not under the control of a single stakeholder, there is a need to consider what would positive security culture mean in this context? How do we create a shared responsibility for cyber security in such settings? And how do we create realistic risk models and use them in practice? The importance of shared terminology, language and concepts is important in this regard and resources such as CyBOK may offer an important bridge in this regard.
4. **Need for research datasets.** In order to study cyber security at scale as a research problem, good and realistic datasets are key. This was emphasised in various discussions and there was a call for workshops dedicated to discussing existing datasets, their limitations and curation to make them accessible to the wider research community internationally.

2.2 Key education and training challenges

One of the main themes of discussion here was that of fixing the talent pipeline. This is one of the major challenges facing the field and it was noted that initiatives such as CyBOK have a key role to play in this regard. However, it was also recognised that knowledge must be complemented by hands-on experience – to enable the workforce to put that knowledge into practice. This is even more critical as the future of work changes – with increasingly mobile and remote working by workers in the digital economy. The evolution of the infrastructures that service society and our daily lives poses another challenge with regards to maintaining the capabilities of the workforce. The need for continuing education and training is therefore paramount.

Several key areas of focus for education and training were identified.

1. **Need for more general cyber security awareness and education.** As cyber security and threats to it become mainstream, there is a need to raise more general awareness for cyber security in the wider population. This is not meant to push the burden of security on to users – but in the same way as safety has become part of the wider societal consciousness, cyber security should be too. Cyber security professionals are needed who can develop and engage in such wider awareness programmes – both within organisations and the wider society.
2. **There are multiple pathways to being a professional.** The role of universities in addressing the talent pipeline is clear. But it is also important to consider that traditional university education is one pathway to becoming a cyber security professional. Apprenticeships can offer an alternative pathway especially if there are no entry level cyber security roles. There was also a concern that over-specialisation – though valued in research – may stifle continuing development in a practitioner setting. It is, therefore, important to establish and provide clear pathways for continuing professional develop-

ment – not only maintaining the knowledge and skills that are relevant in current context but identifying and developing those that would be needed in 5-10 years time.

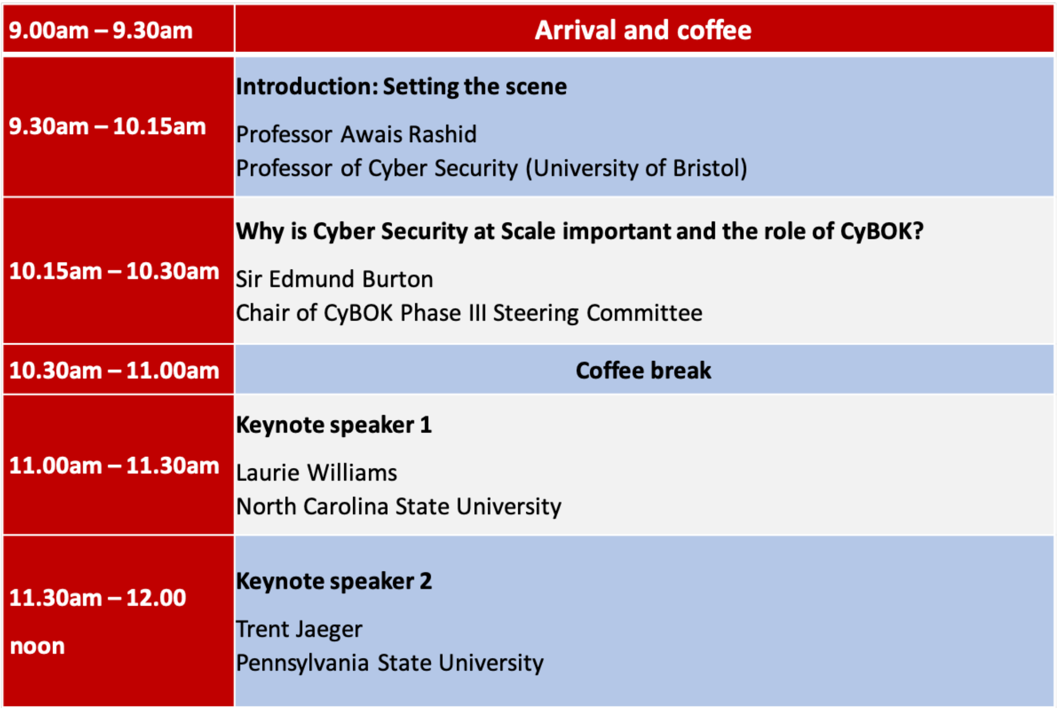
3. **Exposure to adversarial thinking.** This was identified as a key characteristic for the cyber security professional – in order to identify where weaknesses in systems or potential risks may lie in order to be able to mitigate against them. Such adversarial thinking can be developed both by studying anatomies of complex attacks and through hands-on training on experimental systems and infrastructures – that provide a first-hand experience of attacks and defences in a realistic cyber security incident.

3 CONCLUSION

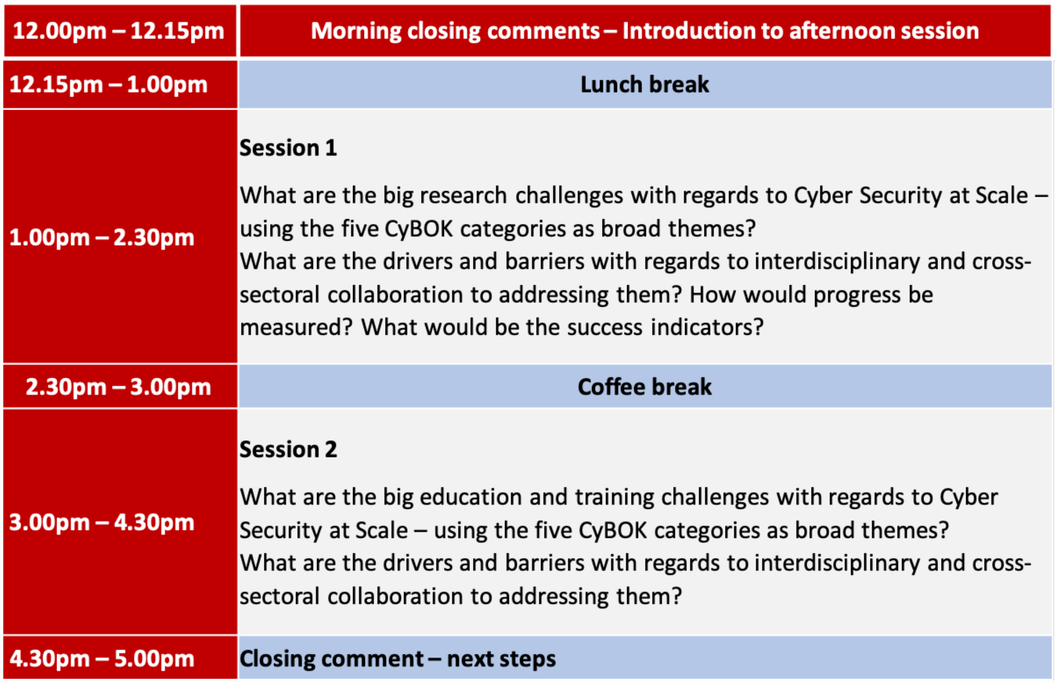
The workshop brought together a number of key experts in academia, industry and government, both nationally and internationally to discuss the challenges for cyber security research, education and training in the emerging and future large-scale connected environments. A number of key areas of future research and education & training needs were identified. There were some themes that were recurrent across these discussions – the need for international collaboration, the need for partnerships across academia, industry and government, the need for interdisciplinary approaches and the importance of cyber security to the day-to-day functioning of society. CyBOK 1.0 offers an important element in providing rigorous foundations for cyber security education and training – and also mapping the foundational concepts established through many years of research and practice. These have been developed collectively by members of the cyber security community. We now need to build on these resources to address the key challenges identified and noted above.

Acknowledgements. We thank all colleagues who participated in the workshop and offered their insights and input. We also thank Brittany Davidson, Matthew Edwards, Joseph Hallett, Emil Lupu and Sanjay Rawat for taking notes that enabled us to synthesise the insights from the discussions.

4 APPENDIX: WORKSHOP SCHEDULE



9.00am – 9.30am	Arrival and coffee
9.30am – 10.15am	**Introduction: Setting the scene** Professor Awais Rashid Professor of Cyber Security (University of Bristol)
10.15am – 10.30am	**Why is Cyber Security at Scale important and the role of CyBOK?** Sir Edmund Burton Chair of CyBOK Phase III Steering Committee
10.30am – 11.00am	**Coffee break**
11.00am – 11.30am	**Keynote speaker 1** Laurie Williams North Carolina State University
11.30am – 12.00 noon	**Keynote speaker 2** Trent Jaeger Pennsylvania State University



12.00pm – 12.15pm	Morning closing comments – Introduction to afternoon session
12.15pm – 1.00pm	**Lunch break**
1.00pm – 2.30pm	**Session 1** What are the big research challenges with regards to Cyber Security at Scale – using the five CyBOK categories as broad themes? What are the drivers and barriers with regards to interdisciplinary and cross-sectoral collaboration to addressing them? How would progress be measured? What would be the success indicators?
2.30pm – 3.00pm	**Coffee break**
3.00pm – 4.30pm	**Session 2** What are the big education and training challenges with regards to Cyber Security at Scale – using the five CyBOK categories as broad themes? What are the drivers and barriers with regards to interdisciplinary and cross-sectoral collaboration to addressing them?
4.30pm – 5.00pm	**Closing comment – next steps**