Cyber Security Body of Knowledge

CyBOK Team

Professor Awais Rashid (PI)
Professor George Danezis
Dr Howard Chivers
Professor Andrew Martin
Professor Emil Lupu
Yvonne Rigby

@cy_bok
www.cybok.org

Motivation

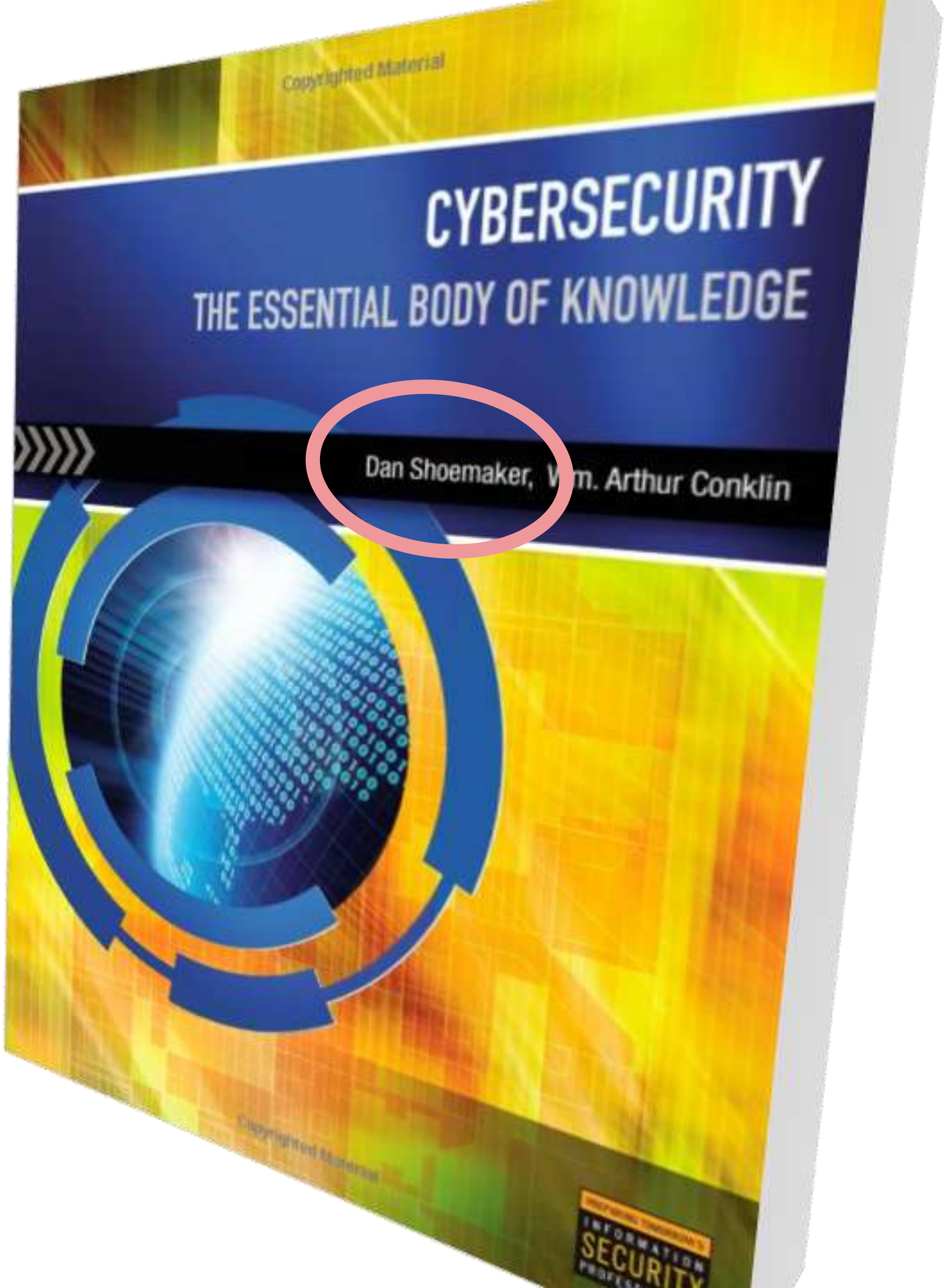
CyBOK

- What is its definition and scope
- What's in; what's out

- IEEE/ACM/IFIP Joint Task Force on Cyber Security Education
- European Cyber Security Centres of Expertise: Taxonomy
- Professional Skills Frameworks and BOKs (IISP, CISSP, ...)

- Designing and evaluating curricula and courses
- Government/industry/academia collaborations: for agreeing research areas
- Knowledge needed from potential candidates for posts
- Benchmarking capacity (in an organisation or country)

Precedents


Copyrighted Material
CYBERSECURITY
THE ESSENTIAL BODY OF KNOWLEDGE
Dan Shoemaker, Wm. Arthur Conklin

Inspiration – IEEE SWEBOK

CyBOK

Software Engineering: 15 Knowledge Areas

- Lifecycle (e.g., requirements, design) and Foundation (e.g., modelling, computation)
- Each 15 – 20 pages

3. Requirements Elicitation

[1*, c4s5] [2*, c5, c6, c9]

Requirements elicitation is concerned with the origins of software requirements and how the software engineer can collect them. It is the first stage in building an understanding of the problem the software is required to solve. It is fundamentally a human activity and is where the stakeholders are identified and relationships established between the development team and the customer. It is variously termed "requirements capture," "requirements discovery," and "requirements acquisition."

One of the fundamental principles of a good requirements elicitation process is that of effective communication between the various stakeholders. This communication continues through the entire Software Development Life Cycle (SDLC) process with different stakeholders at different points in time. Before development

https://www.computer.org/web/swebok/v3

MATRIX OF TOPICS VS. REFERENCE MATERIAL

	Sommerville 2011 [1*]	Wiegers 2003 [2*]
1. Software Requirements Fundamentals		
1.1. Definition of a Software Requirement	c4	c1
1.2. Product and Process Requirements	c4s1	c1, c6
1.3. Functional and Nonfunctional Requirements	c4	c12
1.4. Emergent Properties		

REFERENCES

[1*] I. Sommerville, *Software Engineering*, 9th ed., Addison-Wesley, 2011.

[2*] K.E. Wiegers, *Software Requirements*, 2nd ed., Microsoft Press, 2003.

[3] INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes*

[6] C. Po "Inq IEEE pp.

[7] A. va Engi Mod

Context

- Project commissioned by UK *National Cyber Security Centre* (**NCSC**)
  - Government Agency; part of GCHQ
- NCSC role to help protect critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations.
- Key element in research and education
  - Academic Centres of Excellence in Cyber Security Research (14 Universities)
  - Certified Master's Programmes (24 courses) and undergraduate programmes (4 courses)
  - Four academic research institutes
  - Development of a Cyber Security Profession; career roles and pathways

CyBOK Aim

CyBOK

To codify foundational and generally recognised knowledge in cyber security following broad community engagement nationally and internationally

A guide to the body of knowledge!

Will focus on the established foundation of the subject (not on everything that has ever been written, nor on truly still-emerging fields)

What will it look like?

- 19 *knowledge areas*
  - ~20 pages per KA
  - cross-referenced
- References to key texts
- Documented dependencies on other knowledge

CyBOK Aim

CyBOK

To codify foundational and generally recognised knowledge in cyber security following broad community engagement nationally and internationally

A guide to the body of knowledge!

Will focus on the established foundation of the subject (not on everything that has ever been written, nor on truly still-emerging fields)

NOT

- a ***curriculum***
  - but might help with design
- a ***textbook***
  - but will reference key texts
- an ***encyclopedia***
  - but will have summary content
- a ***taxonomy***
  - but should offer a structured decomposition

Why Develop a CyBOK?

CyBOK

To establish clear learning pathways from (pre-)high-school through to Bachelor's level and beyond.

Value already demonstrated in mature disciplines such as mathematics, physics, chemistry, biology, software ...

More specifically, to:

Characterise the cyber security discipline

Identify knowledge dependencies which impact learning pathways

Facilitate the design of courses from before High School to Master's as well as professional training and CPD

Provide a foundation for the development and accreditation of programmes

CyBoK Principles

CyBOK

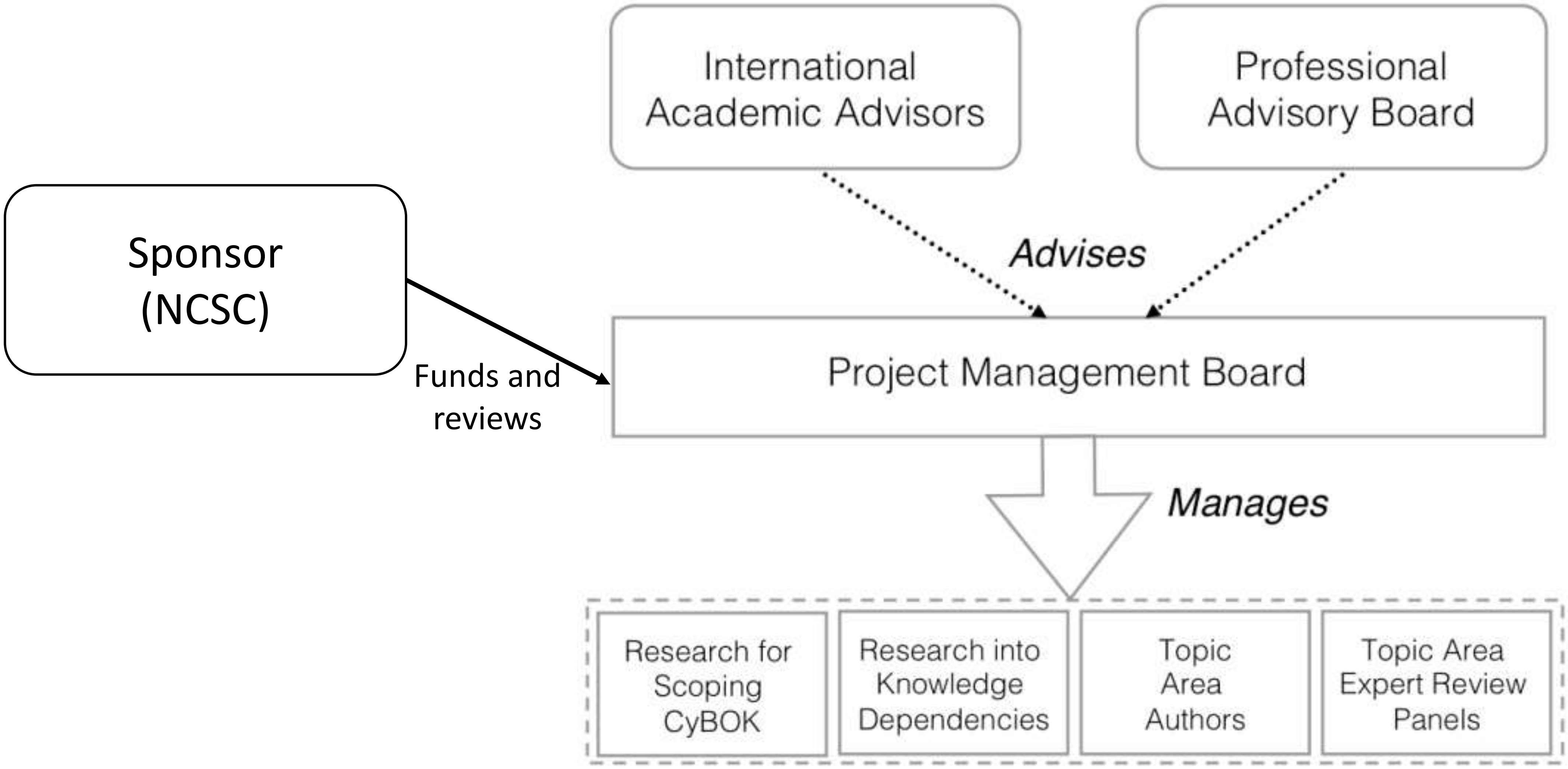
International effort

For the community by the community

Open and freely accessible

Transparency

Governance Structure



Advice

International Academic Advisors

- **Bart Preneel**
  - *KU Leuven, Belgium*
- **Mira Mezini**
  - *Technische Universität Darmstadt, Germany*
- **Jill Slay**
  - *La Trobe University, Australia*
- **L. Jean Camp**
  - *Indiana University*
- **Trent Jaeger**
  - *Pennsylvania State University*

Professional Advisory Board

- **Sir Edmund Burton** (Chair)
- **Ben Laurie** (industry representative)
  - Google
- **Diana Burley** (representative of)
  - ACM Joint Task Force on Cyber Security Education
- **Claire Vishik** (industry representative)
  - Intel
- **Nick Coleman** (representative of)
  - Institute of Engineering and Technology (IET)
- **Amanda Finch** (representative of)
  - Institute of Information Security Professionals (IISP)
- **Dave King** (industry representative)
  - Legal & General
- **Bill Mitchell** (representative of)
  - British Computing Society (BCS)
- **Andrew Rose** (industry representative)
  - National Air Traffic Services (NATS)

Timeline

Feb 2017
- Sprint 1: scoping

May 2017
- Sprint 2: workshops

Aug 2017
- Sprint 3: synthesis

Nov 2017
- Sprint 4: first KA authoring

Feb 2018
- Sprint 5: reviews; new KAs kicked-off

May 2018
- Sprint 6: ongoing; early KAs in public review

…

July 2019
- project ends; CyBOK (first version) complete

Phase I: Scoping Research

CyBOK

Online Survey	41 responses received
Analysis of relevant texts	43 separate texts analysed
In-depth interviews with key experts	10 interviews undertaken
Community workshops across the UK	11 workshops 106 attendees
Call for positions statements	13 statements received
Panel at Advances in Security Education Workshop at USENIX Security Symposium, Vancouver, Canada, October 2017	Paper-based exercise with 28 attendees

Data Collection Activity	Academic (%)	Practitioner (%)
Online survey	51	49
Interviews with key experts	50	50
Community workshops	55	45
Position statements	62	38

Example: Community Workshops

IN THE BIN
KNOWLEDGE AREAS TO BE DISCARDED FROM THE CYBER SECURITY BODY OF KNOWLEDGE

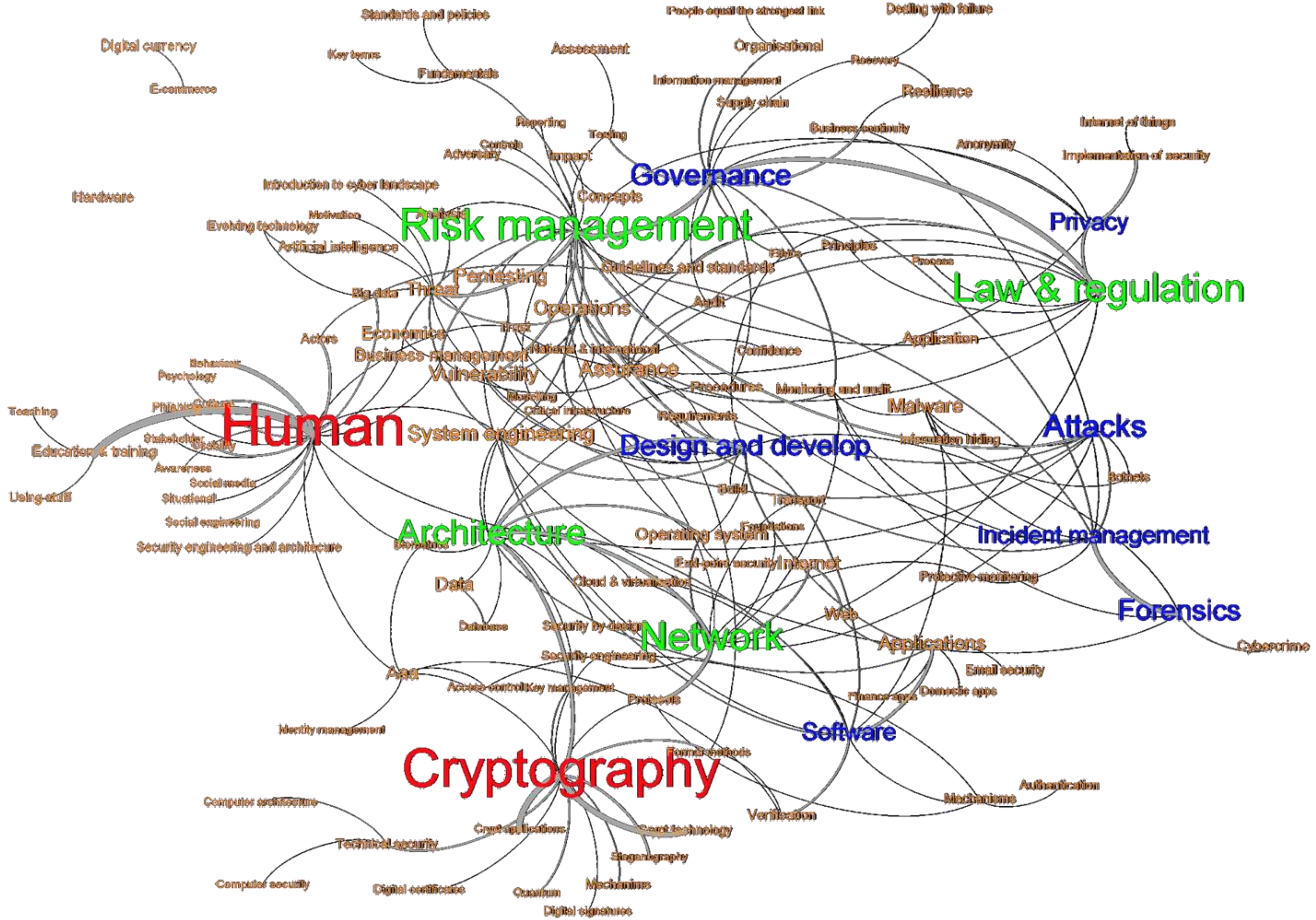
ON THE SHELF
KNOWLEDGE AREAS TO BE DISCUSSED FURTHER

ON THE SHOPPERS HEART
KNOWLEDGE AREAS THAT ARE OF INTEREST BUT NOT NECESSARILY BE INCLUDED IN THE CYBER SECURITY BODY OF KNOWLEDGE

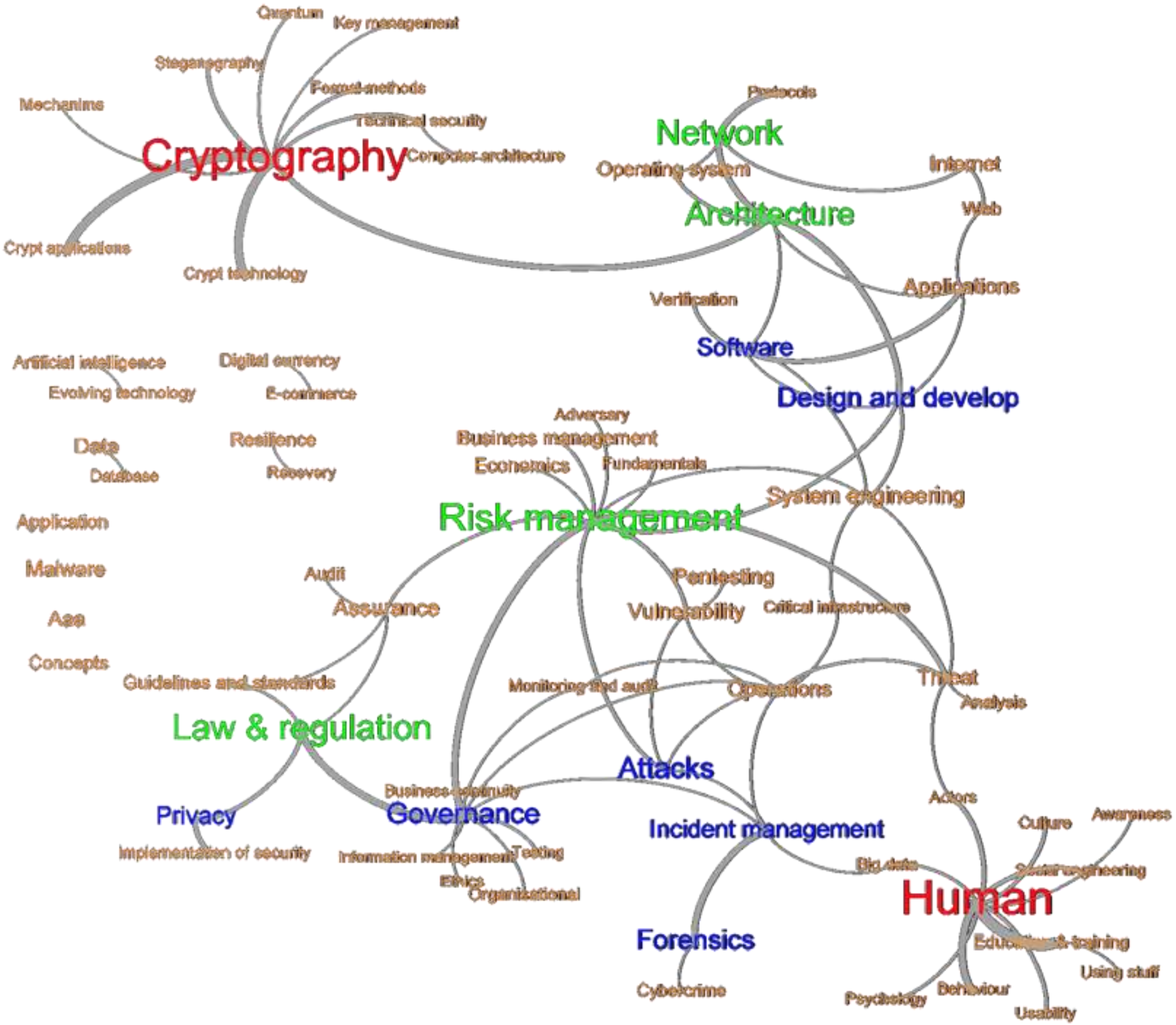
IN THE TROLLEY
KNOWLEDGE AREAS TO BE INCLUDED IN THE CYBER SECURITY BODY OF KNOWLEDGE

15 ITEMS OF LESS
SORTING 'IN THE TROLLEY' ITEMS INTO UPPER LEVEL THEMES (FUNDAMENTAL KNOWLEDGE OF CYBER SECURITY) TO CHECK OUT

Example: Community Workshops

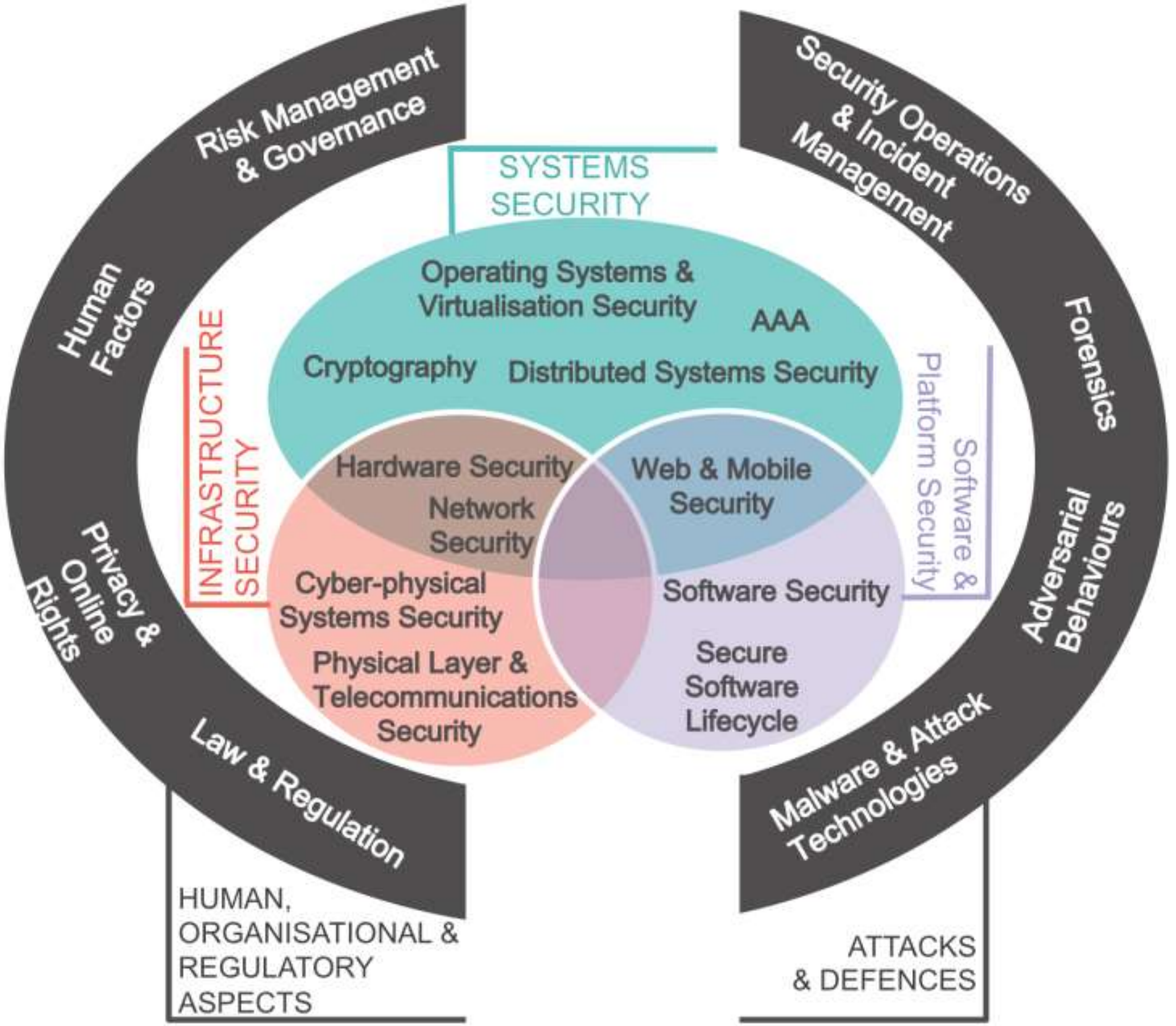


Digital currency
E-commerce
Hardware
Standards and policies
Key terms
Fundamentals
Assessment
People equal the strongest link
Organisational
Dealing with failure
Recovery
Information management
Supply chain
Resilience
Reporting
Testing
Controls
Adversary
Impact
Business continuity
Anonymity
Internet of things
Implementation of security
Governance
Introduction to cyber landscape
Concepts
Motivation
Analysis
Evolving technology
Risk management
Privacy
Artificial intelligence
Ethics
Principles
Process
Guidelines and standards
Big data
Threat
Pentesting
Law & regulation
Audit
Operations
Actors
Economics
Trust
National & international
Application
Confidence
Business management
Behaviour
Psychology
Vulnerability
Assurance
Procedures
Monitoring and audit
Modelling
Critical infrastructure
Malware
Teaching
Human
Requirements
Attacks
System engineering
Stakeholder
Information hiding
Education & training
Design and develop
Awareness
Botnets
Social media
Build
Using-stuff
Situational
Transport
Social engineering
Operating system
Incident management
Architecture
Security engineering and architecture
Biometrics
End-point security
Internet
Protective monitoring
Cloud & virtualisation
Data
Forensics
Web
Database
Security by design
Network
Applications
Cybercrime
Security engineering
Email security
Access control
Key management
Protocols
Finance apps
Domestic apps
Identity management
Software
Formal methods
Authentication
Mechanisms
Cryptography
Computer architecture
Verification
Crypt applications
Smart technology
Technical security
Steganography
Computer security
Digital certificates
Quantum
Mechanisms
Digital signatures



Quantum
Key management
Steganography
Mechanims
Formal methods
Technical security
Cryptography
Computer architecture
Crypt applications
Crypt technology
Protocols
Network
Operating system
Internet
Architecture
Web
Applications
Verification
Software
Design and develop
Artificial intelligence
Evolving technology
Digital currency
E-commerce
Data
Database
Resilience
Recovery
Adversary
Business management
Economics
Fundamentals
System engineering
Risk management
Application
Malware
Aas
Concepts
Audit
Assurance
Pentesting
Vulnerability
Critical infrastructure
Guidelines and standards
Monitoring and audit
Operations
Threat
Analysis
Law & regulation
Attacks
Business continuity
Privacy
Governance
Incident management
Actors
Culture
Awareness
Implementation of security
Information management
Testing
Ethics
Organisational
Big data
Human
Education & training
Forensics
Using stuff
Cybercrime
Psychology
Behaviour
Usability

Knowledge Areas



Human, Organisational and Regulatory Aspects

Risk Management and Governance	Security management systems and organisational security controls, including standards, best practices and approaches to risk assessment and mitigation.
Law and Regulation	International and national statutory and regulatory requirements, compliance obligations and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Covers usable security, social and behavioural factors impacting security, security culture and awareness as well as impact of security controls on user behaviours.
Privacy & online rights	Techniques for protecting personal information, including communications, applications and inferences from databases and data processing. Also, other systems supporting on-line rights touching upon censorship and circumvention, covertness, electronic elections and privacy in payment and identity systems.

Attacks and Defences

CyBOK

Malware and Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviours	The motivations, behaviours and methods used by attackers, including malware supply chains, attack vectors and money transfers.
Security Operations & Incident Management	The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence
Forensics	The collection, analysis and reporting of digital evidence in support of incident or criminal events.

Systems Security

CyBOK

Operating Systems & Virtualisation Security	Operating systems protection mechanisms, implementing secure abstraction of hardware and sharing of resources, including isolation in multi-user systems, secure virtualisation and security in database systems.
Distributed Systems Security	Security mechanisms relating to larger scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multi-tenant data centers, and distributed ledgers.
Authentication, Authorisation & Accountability	Covers all aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.
Cryptography	Covers the core primitives of cryptography as presently practiced and emerging algorithms, techniques for analysis of these and the protocols which use them.

Infrastructure Security

CyBOK

Network Security	Security aspects of networking and telecommunication protocols, including the security of routing, network security elements and specific cryptographic protocols used for network security.
Hardware Security	Addresses security in the design, implementation, and deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.
Cyber-Physical Systems Security	Covers security challenges in cyber-physical systems, such as IoT and industrial control systems, attacker models, safe-secure designs, security of large-scale infrastructures.
Physical Layer & Telecomms Security	Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.

Software and Platform Security

CyBOK

Software Security	Explores known categories of programming errors resulting in security bugs, and techniques for avoiding these errors - both through coding practice and improved language design, and tools, techniques and methods for detection of such errors in existing systems.
Web and Mobile Security	Addresses issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
Secure Software Lifecycle	The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.

Phase 2

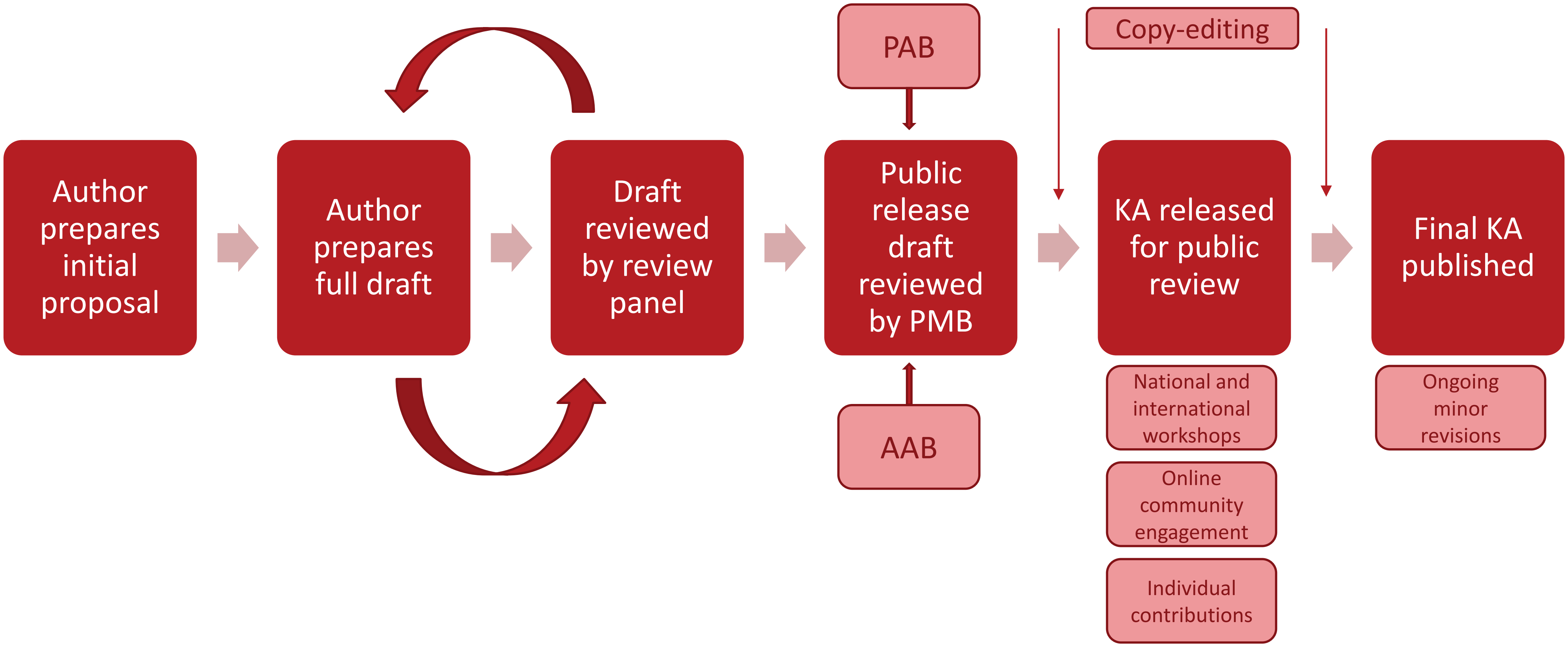
- Recruiting Specialist Authors for Knowledge Areas
  - *mostly* academics; international expertise
- Recruiting Specialist Reviewers for Knowledge Areas
  - around six; mix of academics and industrialists; international. diverse
- Write-Review cycle
- Public Review of each Knowledge Area
- Progressive Publication of Full Document
- Development of Learning Pathways

KAs currently in Development

Knowledge Area	Author
Cryptography	Prof. Nigel Smart *(KU Leuven, Belgium & University of Bristol, UK)*
Software Security	Prof. Frank Piessens *(KU Leuven, Belgium)*
Human Factors	Prof. Angela Sasse *(University College London, UK)*
Malware and Attack Technologies	Prof. Wenke Lee *(Georgia Institute of Technology, USA)*
Security Operations and Incident Management	Prof. Herve Debar *(Telecom SudParis, France)*
Physical Layer and Telecommunications Security	Prof. Srdjan Capkun (*ETH Zurich, Switzerland)*
Network Security	Prof. Sanjay Jha *(University of New South Wales, Australia)*

Approach to Phase 2

KA development and review process



Approach to Phase 2

Identifying Knowledge Dependencies and Learning Pathways

- Focus on identification of **knowledge dependencies** that impact the **learning pathways** individuals may follow during their journey to becoming a cyber security expert.
- Design and implement community consultations with stakeholders and undertake desk research on cyber security curricula to:
  - Develop set of exemplar learning pathways
  - Develop and analyse case studies on the basis of CyBOK
  - Use examples of learning pathways and case studies to identify knowledge required at each education level and its dependencies on other knowledge.
- NCSC certified programmes will be used as an initial case study to identify knowledge dependencies and best routes through the developing KAs.

Promotion of the CyBOK

CyBOK

Draft KAs at public review phase

- KAs distributed around established networks.
- Consultation workshops.
- Announcements on ***www.cybok.org*** and ***@cy_bok***
- All interested contacts informed by email.
- Authors and reviewers to distribute personally.

Stable KAs

- At the end of each Sprint the developing CyBOK will be published.
- Placeholder for future KAs currently under development or scheduled for development.

www.cybok.org

CyBOK

Home | About | People | News | Events | Contact

University of BRISTOL
Bristol Cyber Security Group

The Cyber Security Body Of Knowledge

A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector

The CyBOK project aims to bring cyber security into line with the more established sciences by distilling knowledge from major internationally-recognised experts to form a Cyber Security Body of Knowledge that will provide much-needed foundations for this emerging topic. The project, funded by the **National Cyber Security Programme**, is led by the University of Bristol's **Professor Awais Rashid**, along with other leading cyber security experts - including **Professor Andrew Martin**, **Professor George Danezis**, **Professor Emil Lupu** and **Dr Howard Chivers**.

Draft Knowledge Areas (KAs) - released for comment

Following wide community consultation with both academia and industry, key knowledge areas (KAs) have been identified to form the scope of the CyBOK. The Scope document provides an overview of these top-level KAs and the sub-topics that should be covered under each.

We are very pleased to announce the release of the first KAs, Cryptography and Software Security for public review. You are invited to contribute to the development of these KAs by sending your comments to the CyBOK project team. All contributions, big or small, are welcomed so please input yourself and feel free to forward this invitation to anyone else who may be interested.

Latest news

SOFTWARE SECURITY KNOWLEDGE AREA

25 April 2018: Draft Software Security Knowledge Area (KA) now available.

Read more

CRYPTOGRAPHY KNOWLEDGE AREA

25 April 2018: Draft Cryptography Knowledge Area (KA) now available.

Read more

All news

Key documents

SOFTWARE SECURITY KNOWLEDGE AREA

Download

CRYPTOGRAPHY KNOWLEDGE AREA

Download

TOP-LEVEL KNOWLEDGE AREAS (KAs)

Download

SCOPE DOCUMENT v2

Download

Challenges to be faced

- consensus
  - value will derive from widespread acceptance
  - address editorial comments; consider under-developed topics; avoid scope-creep
- coverage and coherency
  - approach means KAs will differ in style; want to avoid overlaps and gaps
  - desirable that KAs achieve consistent depth – coverage/benchmarking metrics are inevitable
- maintenance
  - some KAs will age more quickly than others
  - long-term ‘ownership’ needed; long-term authorship/editorship will be important

Take-aways

Guide to the body of Knowledge in Cyber Security	Detailed but not encyclopædic	By the community, for the community	Work in progress
• 19 Knowledge Areas; about 20 pages per KA.	• Complements other efforts	• Openly reviewed; Freely circulated	• Community engagement throughout

CyBOK

www.cybok.org