New resources

Andrew Martin

Professor of Systems Security, University of Oxford

contact@cybok.org
www.cybok.org

CyBOK development

CyBOK

- Our "Knowledge Areas" represent substantial bodies of work around established topics in Cyber Security.
    - Not all knowledge is captured there.
- If CyBOK is to remain relevant, it must be a living document.
- This implies
    - ✓ processes for updates, periodic scope reviews, refactoring, etc.
    - ✓ ongoing programme of resources for users (curriculum designers, course leaders, recruiters, etc.)
    - → developing content at the *edges*

- There is scope to add:
    - emerging areas: those which are less well-established or less substantial in their penetration in the community
    - guides for particular application areas, and particular technologies/clusters, linking existing CyBOK topics across the KAs
- Knowledge captured at the edges *could* be candidate for inclusion in future revisions of CyBOK
    - with caveats!

Content Types

Knowledge Area

- Codify ***foundational*** and generally recognised knowledge in cyber security following broad community engagement nationally and internationally
- Supported by processes for selection, review, change, and updating

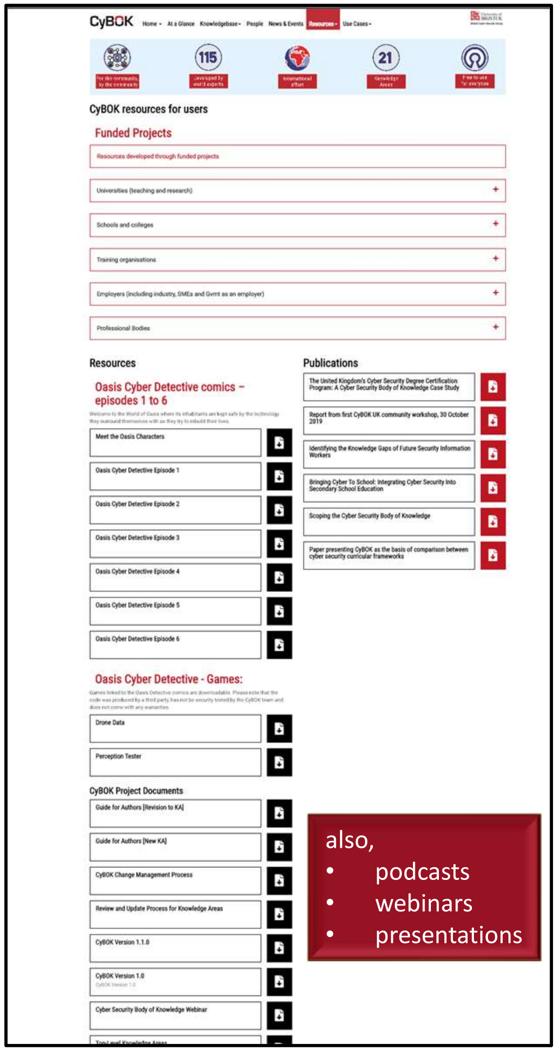
Knowledge Guide

- Review of relevant literature on a topic ***(typically on an emerging topic)*** that captures the current state of the field, key issues that learners should know about, emerging techniques to address those issues and open research problems.

Topic Guide

- Draw together topics from across a number of KAs, to give a unified treatment to a collection of topics distributed across CyBOK.

www.cybok.org/resources



CyBOK resources for users

Funded Projects

Resources developed through funded projects

Universities (teaching and research) +

Schools and colleges +

Training organisations +

Employers (including industry, SMEs and Gvmt as an employer) +

Professional Bodies +

Resources

Oasis Cyber Detective comics – episodes 1 to 6

Welcome to the World of Oasis where its inhabitants are kept safe by the technology they surround themselves with as they try to rebuild their lives.

Meet the Oasis Characters

Oasis Cyber Detective Episode 1

Oasis Cyber Detective Episode 2

Oasis Cyber Detective Episode 3

Oasis Cyber Detective Episode 4

Oasis Cyber Detective Episode 5

Oasis Cyber Detective Episode 6

Oasis Cyber Detective - Games:

Games linked to the Oasis Detective comics are downloadable. Please note that the code was produced by a third party, has not be security tested by the CyBOK team and does not come with any warranties.

Drone Data

Perception Tester

CyBOK Project Documents

Guide for Authors [Revision to KA]

Guide for Authors [New KA]

CyBOK Change Management Process

Review and Update Process for Knowledge Areas

CyBOK Version 1.1.0

CyBOK Version 1.0
CyBOK Version 1.0

Cyber Security Body of Knowledge Webinar

Top-Level Knowledge Areas

Publications

The United Kingdom's Cyber Security Degree Certification Program: A Cyber Security Body of Knowledge Case Study

Report from first CyBOK UK community workshop, 30 October 2019

Identifying the Knowledge Gaps of Future Security Information Workers

Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education

Scoping the Cyber Security Body of Knowledge

Paper presenting CyBOK as the basis of comparison between cyber security curricular frameworks

also,
- podcasts
- webinars
- presentations

Content Types

Knowledge Area

- Codify ***foundational*** and generally recognised knowledge in cyber security following broad community engagement nationally and internationally
- Supported by processes for selection, review, change, and updating

CyBOK

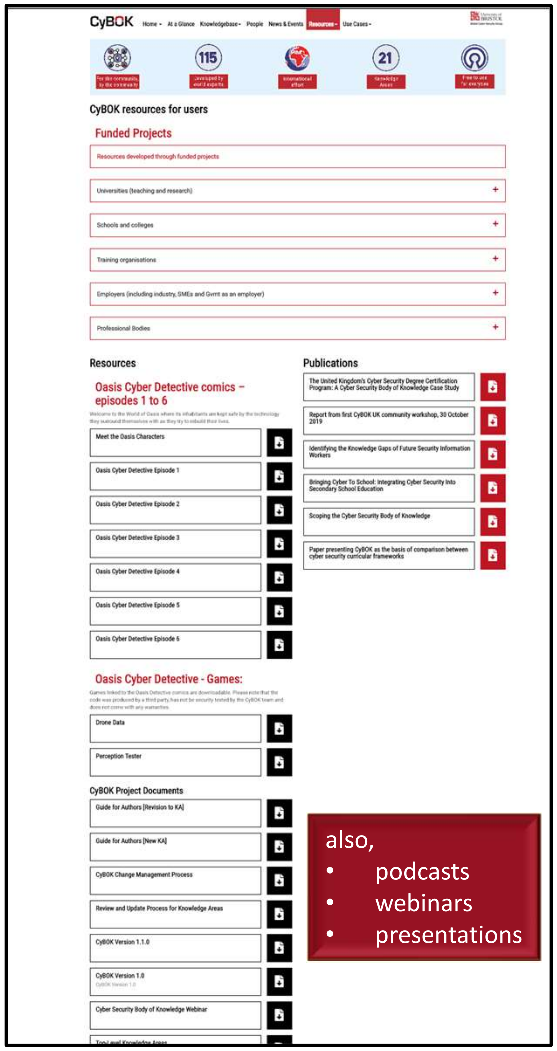
Knowledge Guide

- Review of relevant literature on a topic ***(typically on an emerging topic)*** that captures the current state of the field, key issues that learners should know about, emerging techniques to address those issues and open research problems.

Topic Guide

- Draw together topics from across a number of KAs, to give a unified treatment to a collection of topics distributed across CyBOK.

www.cybok.org/resources



CyBOK resources for users

Funded Projects

Resources developed through funded projects

Universities (teaching and research) +

Schools and colleges +

Training organisations +

Employers (including industry, SMEs and Gvmt as an employer) +

Professional Bodies +

Resources

Oasis Cyber Detective comics – episodes 1 to 6

Welcome to the World of Oasis where its inhabitants are kept safe by the technology they surround themselves with as they try to rebuild their lives.

Meet the Oasis Characters

Oasis Cyber Detective Episode 1

Oasis Cyber Detective Episode 2

Oasis Cyber Detective Episode 3

Oasis Cyber Detective Episode 4

Oasis Cyber Detective Episode 5

Oasis Cyber Detective Episode 6

Oasis Cyber Detective - Games:

Games linked to the Oasis Detective comics are downloadable. Please note that the code was produced by a third party, has not be security tested by the CyBOK team and does not come with any warranties.

Drone Data

Perception Tester

CyBOK Project Documents

Guide for Authors [Revision to KA]

Guide for Authors [New KA]

CyBOK Change Management Process

Review and Update Process for Knowledge Areas

CyBOK Version 1.1.0

CyBOK Version 1.0
CyBOK Version 1.0

Cyber Security Body of Knowledge Webinar

Top-Level Knowledge Areas

Publications

The United Kingdom's Cyber Security Degree Certification Program: A Cyber Security Body of Knowledge Case Study

Report from first CyBOK UK community workshop, 30 October 2019

Identifying the Knowledge Gaps of Future Security Information Workers

Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education

Scoping the Cyber Security Body of Knowledge

Paper presenting CyBOK as the basis of comparison between cyber security curricular frameworks

also,
- podcasts
- webinars
- presentations

CyBOK Knowledge Guide

CyBOK **Knowledge Guide** represents a review of relevant literature on a topic ***(typically on an emerging topic)*** that captures the current state of the field, key issues that learners should know about, emerging techniques to address those issues and open research problems.

It should be readable as a stand alone document but should make reference to relevant foundational knowledge within CyBOK.

This would take the form of a review of relevant literature (typically 10-15 pages), excluding references.

It will be authored by a leading expert and peer reviewed by at least three expert reviewers under the stewardship of an editor.

CyBOK Topic Guide

CyBOK **Topic Guide** draws together topics from across a number of KAs, to give a unified treatment to a collection of topics distributed across CyBOK. In general, these will be ***crosscutting themes*** where practitioner knowledge is more prominent than academic thinking.

The great majority of a Topic Guide's content should be a synthesis of concepts from existing KA topics, but a small amount of additional material (with suitable references) should be included as needed to provide a comprehensive treatment of the topic.

It will be authored by a leading expert and peer reviewed by at least three expert reviewers under the stewardship of an editor.

New Topic Guide: AI for Cyber Security

CyBOK

- *what cyber security experts should know*
  - AI use cases in cyber security, what problems it solves in such use cases and what challenges arise
  - *dos* and *don'ts* of AI in cyber security
  - Practical considerations when evaluating AI models and tools for usage in cyber security
  - Human-in-the-loop
  - Emerging use cases
- **Status:** scoping workshop held; change request written and approved; author identified; currently identifying reviewers

New Knowledge Guide: Security and Privacy of AI

CyBOK

- *what AI experts should know about security threats and potential attacks when they are deploying AI within systems*
  - Attack strategies,
    - including model extraction, evasion, inversion, and poisoning; adversarial attacks on Models
  - Threat modelling,
    - categories of threats related to the AI lifecycle: data collection; training; deployment.
  - Defences against the range of possible attacks
    - transparency, testing and accountability
  - Privacy
  - Practical case studies
- **Status:** workshop held; change request written and approved; currently identifying authors and reviewers.

Cyber Security Economics

CyBOK

- To complement the Risk Management and Governance KA
  - Summary of Economics concepts (as related to Cyber Security)
  - Security Investments
    - modelling, optimisation, cost-benefit analysis; metrics; sustainability; game theoretic analysis
  - Economics of human behaviour
  - Economics and psychology of cybercrime
  - Supply-chain security
  - Cyber Insurance
- **Status:** workshop held; scope defined; under consideration by Executive and Steering Committee

Community Visibility and Input

- Security Economics proposal will be forthcoming
- Knowledge Guides and Topic Guides will be published following internal review
- Change Requests always welcome
  - against existing KAs
  - for new KAs, KGs, and TGs.