

# CyBOK

The Cyber Security Body Of Knowledge



## Foundations and Resources for the Community

Professor Awais Rashid

[contact@cybok.org](mailto:contact@cybok.org)  
[www.cybok.org](http://www.cybok.org)

Codify ***foundational*** and generally recognised knowledge in cyber security following broad community engagement nationally and internationally

A ***guide*** to the body of knowledge

Focus is on ***established foundation*** of the subject (not on everything that has ever been written or on still-emerging, nascent, topics)

International  
effort

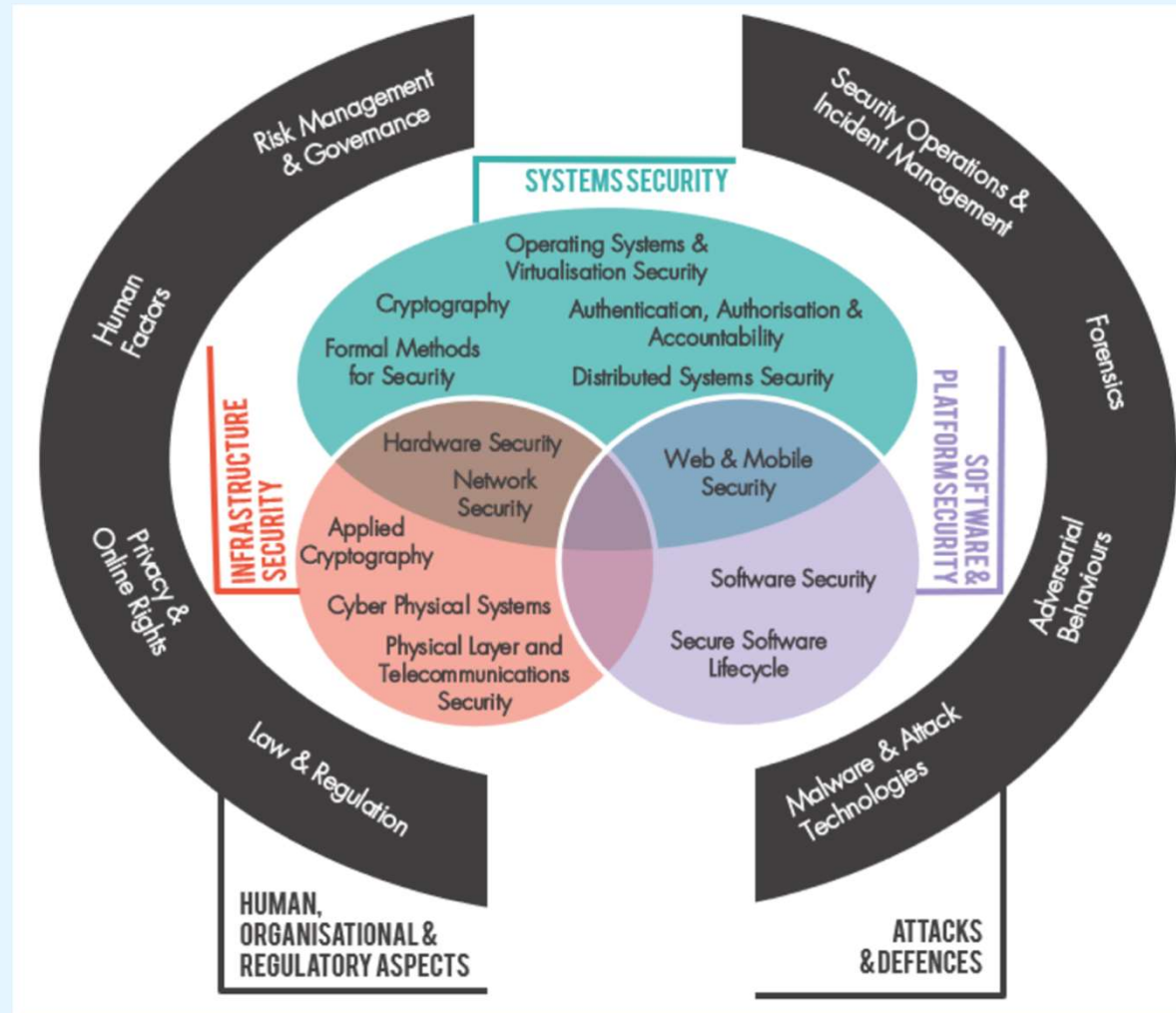
For the  
community by  
the community

Open and  
freely  
accessible

Transparency

- >115** Experts: Authors, Reviewers, Advisors
- >1000** Pages
- >2200** Authoritative sources
- >1600** Comments from wider community
- >30** Invited talks, panels and keynotes

# CyBOK 1.1



## Keeping the Foundations Strong

Open call for proposals to update current KAs or propose new ones: *CyBOK 1.0 -> CyBOK 1.1*

Not just reactive but also proactive: *pro-active expert review of KAs in each category to identify if/where there is a need to refresh the knowledge captured within CyBOK*

Pro-actively develop guides that capture practical pathways through CyBOK or emerging knowledge in the community

## Supplementing the Foundations

***Knowledge Guides:*** Emerging topics or those that are still developing broadly agreed foundations

Security and Privacy of AI

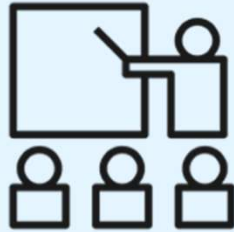
Security Economics

***Topic Guides:*** Practical applications that cut across multiple CyBOK KAs

AI for Security

*Cloud Security*




**Design new university or professional training programmes**

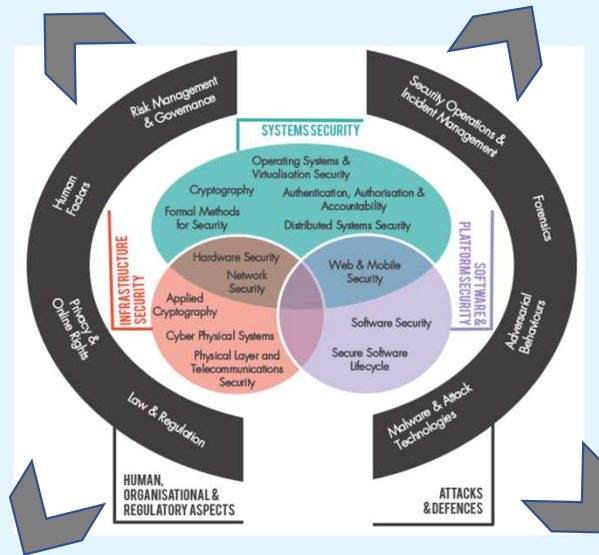


**Contrasting different programmes**



**Design new certification schemes**

	<p><b>Postgraduate Master's Degrees providing a general, broad foundation in cyber security</b> Based on the Cyber Security Body of Knowledge (CyBOK).</p> <p>PDF • 797 KB • 54 PAGES</p>
	<p><b>Postgraduate Master's Degrees focusing on a specialised area of Cyber Security</b> Based on the Cyber Security Body of Knowledge (CyBOK).</p> <p>PDF • 849 KB • 56 PAGES</p>
	<p><b>Bachelor's in Computer Science and Cyber Security</b> Two certifications: A) providing a general broad foundation and B) focusing on a specialised area of...</p> <p>PDF • 753 KB • 69 PAGES</p>



**Knowledge requirements for job roles**



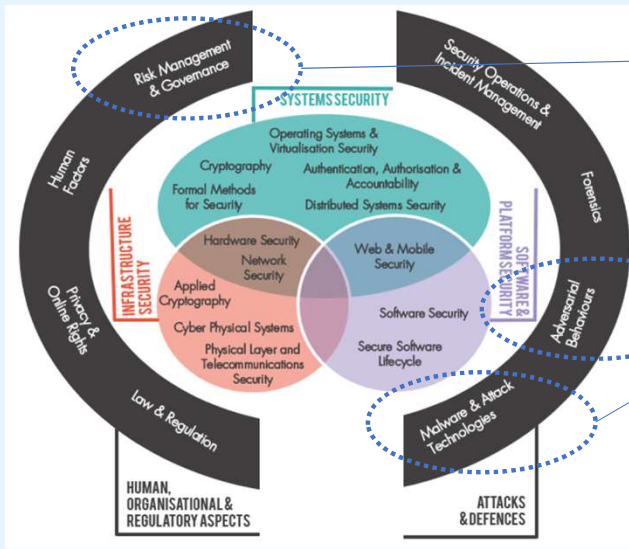
**Traceably meeting certification requirements**



**Benchmarking capacity**

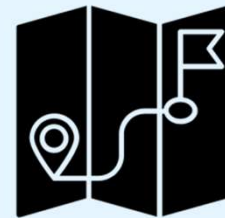




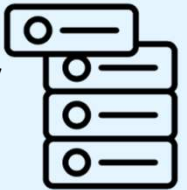


- Risk Management & Governance
- Adversarial Behaviours
- Malware and Attack Technologies

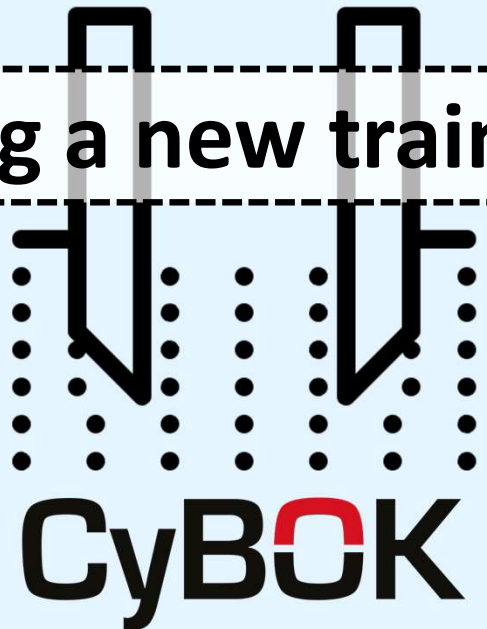
Mapping reference  
with > 13000 terms

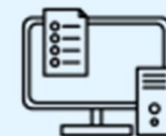
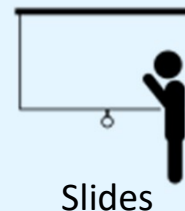
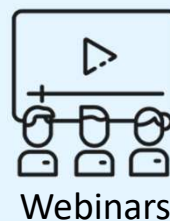
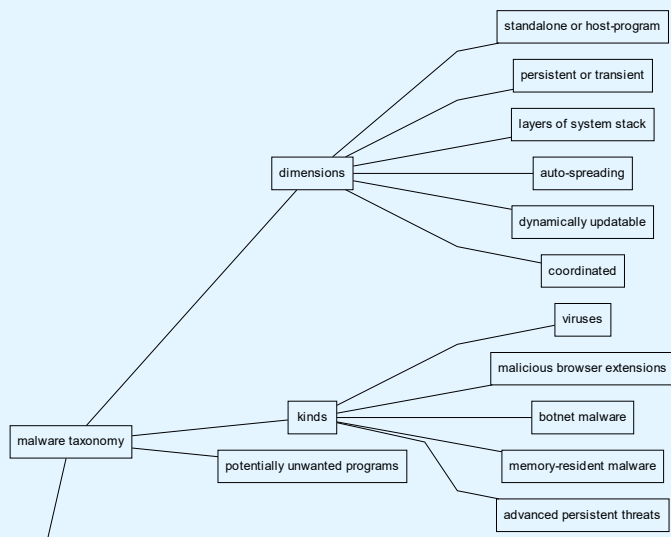


An index for easy  
look up of terms



Designing a new training course





Lesson Plans,  
Labs and  
Exercises

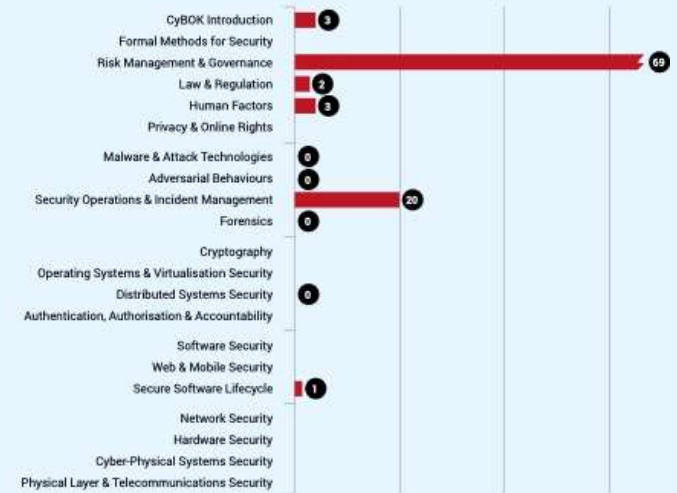
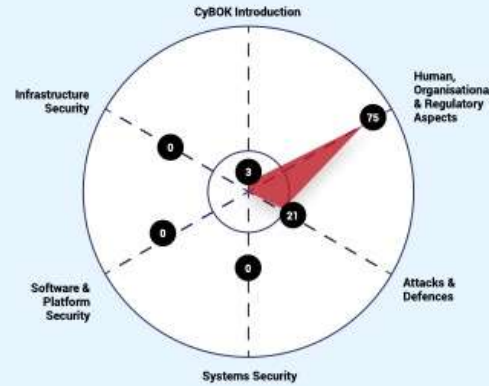
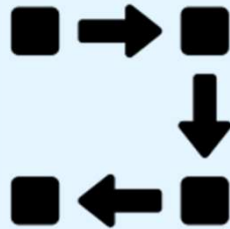
# Designing a new training course



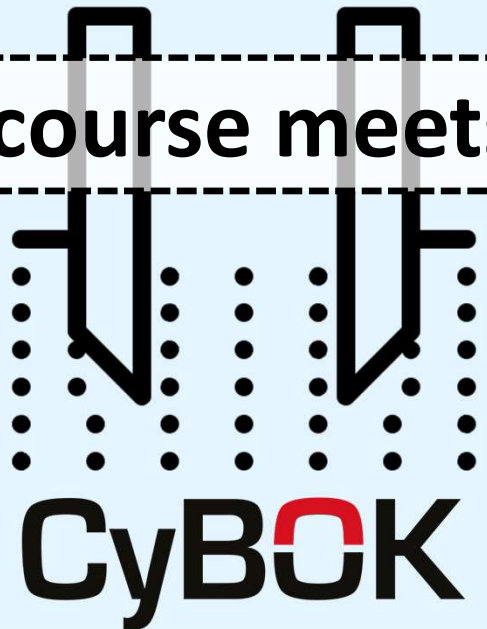
Mapping reference  
with > 13000 terms

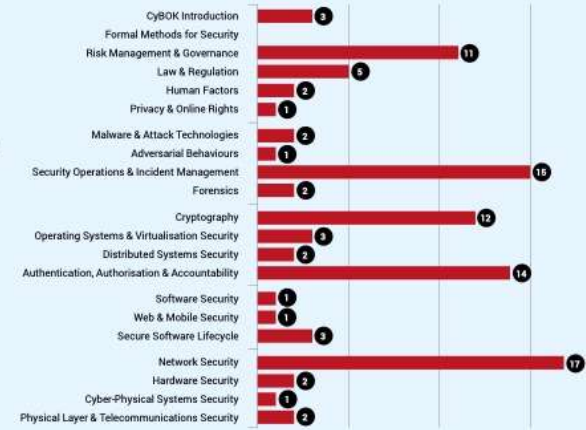
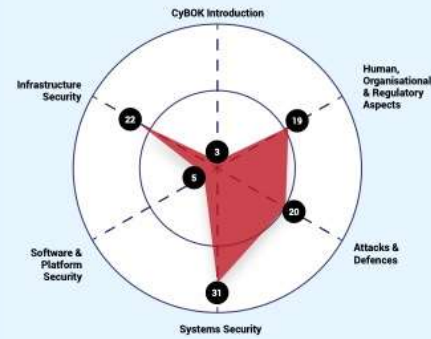
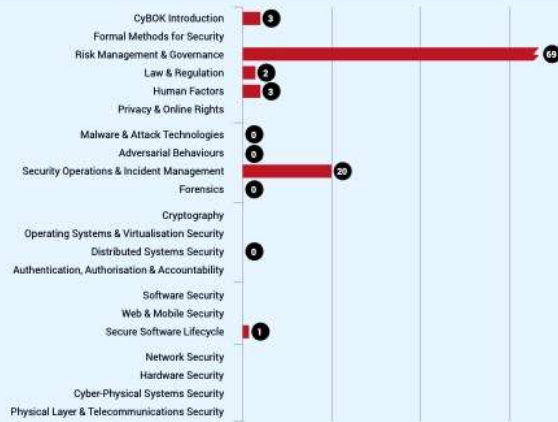
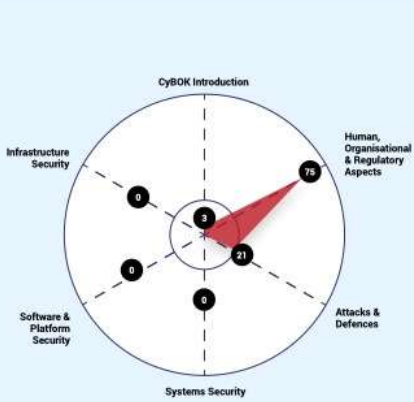


Mapping  
Framework

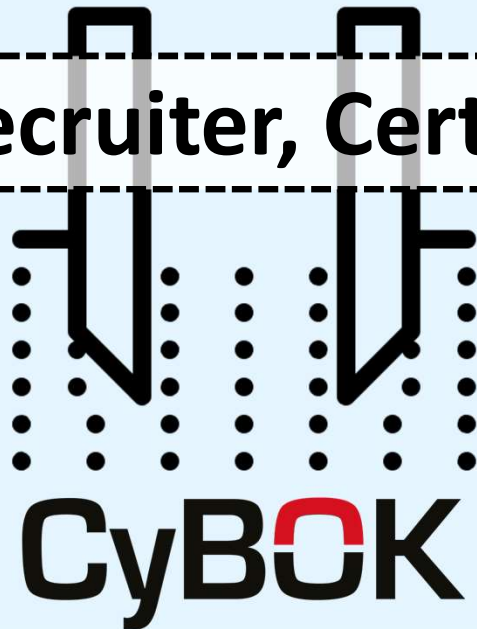


Showing a course meets training needs





**Learner, Recruiter, Certification Body**



**6 Professional Programmes**

**51 University Degrees**

**CyBOK**

**The Cyber Security  
Body of Knowledge**

**Mappings of University  
and Professional Training  
Programmes to CyBOK**

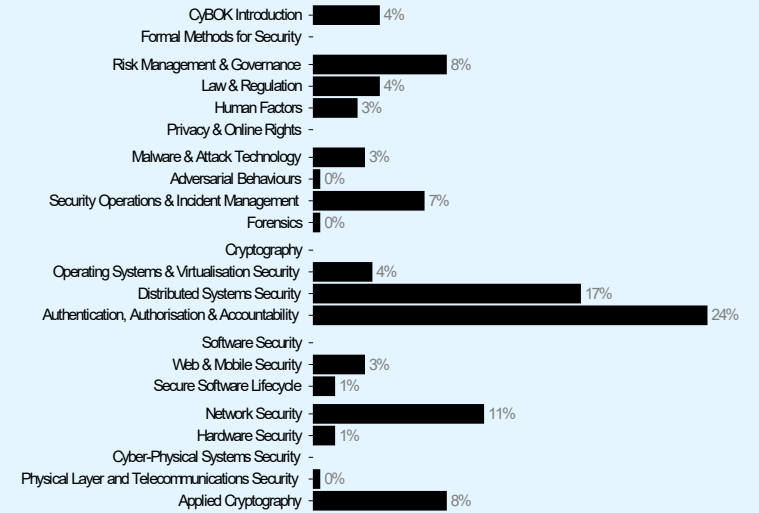
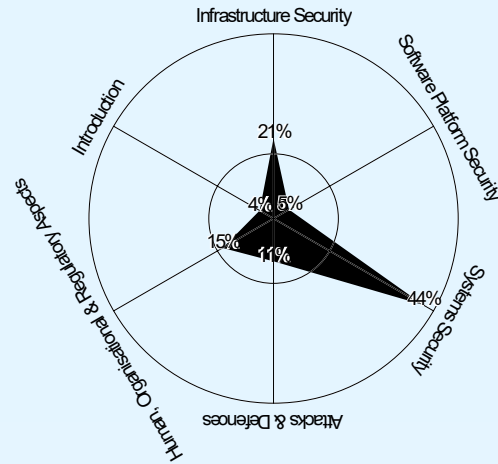


© Crown Copyright 2024.

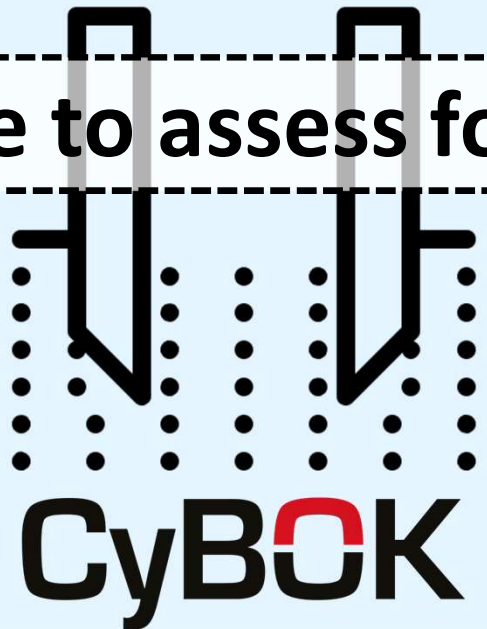
Mapping Booklet Version 2.2  
Mappings are based on either CyBOK v1.0.0 + Formal Methods for Security or CyBOK v1.1.0

**CyBOK**

# NCSC Cyber Advisor (Cyber Essentials)



What knowledge to assess for particular roles?



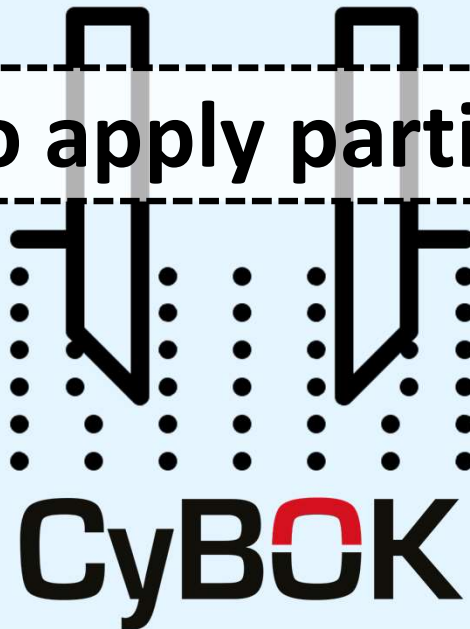


Practical exercises,  
labs and CTFs



Case studies

**Learning skills to apply particular knowledge**



# Labs for multiple CyBOK KAs (*Cliffe Schreuders*)

## Lab Scenarios and CyBOK

The Cyber Security Body of Knowledge (CyBOK) is a body of knowledge that aims to encapsulate the various knowledge areas present within cyber security. Scenarios within SecGen now contain XML elements linking them to CyBOK knowledge areas and specific topics within those knowledge areas. Additionally, video lectures for scenarios are tagged with CyBOK associations.

## Scenarios Indexed By CyBOK Knowledge Area (KA)

Human Factors (HF)

Adversarial Behaviours (AB)

Malware & Attack Technology (MAT)

Applied Cryptography (AC)

Forensics (F)

Privacy & Online Rights (POR)

Network Security (NS)

Security Operations & Incident Management (SOIM)

Software Security (SS)

Authentication, Authorisation & Accountability (AAA)

Operating Systems & Virtualisation (OSV)

Cyber-Physical Systems Security (CPS)

Web & Mobile Security (WAM)

Cryptography (C)



# CTFs for multiple CyBOK KAs (*Cliffe Schreuders*)

## CTF Scenarios and CyBOK

The Cyber Security Body of Knowledge (CyBOK) is a body of knowledge that aims to encapsulate the various knowledge areas present within cyber security. Scenarios within SecGen now contain XML elements linking them to CyBOK knowledge areas and specific topics within those knowledge areas. Additionally, video lectures for scenarios are tagged with CyBOK associations.

## Scenarios Indexed By CyBOK Knowledge Area (KA)

Authentication, Authorisation & Accountability (AAA)

Operating Systems & Virtualisation (OSV)

Cryptography (C)

Malware & Attack Technology (MAT)

Software Security (SS)

Security Operations & Incident Management (SOIM)

Web & Mobile Security (WAM)

Adversarial Behaviours (AB)

Forensics (F)

Privacy & Online Rights (POR)

Network Security (NS)

## Practical Exercises for Specific KAs

Memory Analysis Workshop <i>(Joakim Kävrestad)</i>	<b>Forensics</b> <b>Malware and Attack Technologies</b>
Practicals for Formal Methods <i>(Martin Lester)</i>	<b>Formal Methods for Security</b>
GSM Labs <i>(Denis Nicole)</i>	<b>Physical Layer and Telecommunications Security</b>
Wireless Remote Control Labs <i>(Denis Nicole)</i>	<b>Physical Layer and Telecommunications Security</b>
Mapping of Cyber Security Games <i>(Joseph Hallett)</i>	<b>Human Factors</b> <b>Risk Management and Governance</b>
Secure Coding Game-based Lab <i>(Manuel Maarek)</i>	<b>Software Security</b> <b>Secure Software Lifecycle</b>
Interactive Cyber-physical Systems Lab <i>(Phil Legg)</i>	<b>Cyber-Physical Systems Security</b>

## Case Studies for multiple CyBOK KAs (*Nancy Mead*)

Cat.	Knowledge Area	Case Study Mapping	CyBOK version
Human, Organizational and Regulatory Aspects	Risk Management & Governance	ACME Water	1.0
		Archetypal Users – Personae non Gratae	1.0
		FAA ERAM Outage	1.0
		GPS Spoofing of UAV	1.0
		National Cybersecurity Governance	1.1
		National Grid SAP Adoption	1.0
		Organization Risk Management: The Widget Company	1.0
		Penetration Test	1.1
		Ransomware	1.1
		Secure LAN	1.1
	Law & Regulation	National Cybersecurity Governance	1.0
		Ransomware	1.1
	Human Factors	ACME Water	1.0
		FAA ERAM Outage	1.0
	Privacy & Online Rights	ACME Water	1.0
		Driver Assistance System Safety & Security	1.0
		Penetration Test	1.1
		Role Based Access Control	1.1

## Case Studies for multiple CyBOK KAs (*Nancy Mead*)

Attacks and Defences	Malware & Attack Technologies	Deciphering	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Ransomware	1.1
		Using Malware Analysis to Improve Security Reqs	1.1
		Wireshark	1.1
	Adversarial Behaviours	Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Ransomware	1.1
	Security Operations & Incident Management	Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		National Cybersecurity Governance	1.1
		Penetration Test	1.1
		Ransomware	1.1
	Forensics	Mt. Gox Bitcoin Theft	1.0
		Wireshark	1.1

## Case Studies for multiple CyBOK KAs (*Nancy Mead*)

Systems Security	Cryptography	Deciphering	1.1
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
	Operating Systems & Virtualisation Security	Deciphering	1.0
		Heartland Payment System Breach	1.0
		Penetration Test	1.1
		Secure LAN	1.1
	Distributed System Security	Driver Assistance System Safety & Security	1.0
		Secure LAN	1.1
		Wireshark	1.1
	Formal Methods for Security	Deciphering	1.1
		Tokeneer ID Station Project	1.0
	Authentication, Authorisation & Accountability	ACME Water	1.0
		Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
Role Based Access Control		1.1	
Secure LAN		1.1	

## Case Studies for multiple CyBOK KAs (*Nancy Mead*)

Software Platform Security	Software Security	Driver Assistance System Safety & Security	1.0
		FAA ERAM Outage	1.0
		Penetration Test	1.1
	Web & Mobile Security	Driver Assistance System Safety & Security	1.0
		Role Based Access Control	1.1
		Secure LAN	1.1
	Secure Software Lifecycle	ACME Water	1.0
		Aircraft Service Application	1.0
		Drone Swarm	1.0
		National Grid SAP Adoption	1.0
		Secure Acquisition	1.0
		SQUARE	1.0
		Tokeneer ID Station Project	1.0
Using Malware Analysis to Improve Security Reqs	1.1		

## Case Studies for multiple CyBOK KAs (*Nancy Mead*)

Infrastructure Security	Applied Cryptography	Deciphering	1.1
		Penetration Test	1.1
	Network Security	Role Based Access Control	1.1
		Secure LAN	1.1
		Wireshark	1.1
	Hardware Security	Driver Assistance System Safety & Security	1.0
	Cyber-Physical Sys Security	Driver Assistance System Safety & Security	1.0
	Physical Layer & Telecommunications	Penetration Test	1.1
		Secure LAN	1.1
		Wireshark	1.1

**For the Community  
By the Community**

**CyBOK**

[contact@cybok.org](mailto:contact@cybok.org)  
[www.cybok.org](http://www.cybok.org)