Mapping cyber-enabled roles to CyBOK through co-inquiry

Technical Report

Sam Attwood & Rupak Kharel

School of Engineering and Computing

University of Central Lancashire, UK

Correspondence: SAttwood3@uclan.ac.uk

July 2023

Background: The UK Cyber Skills Gap stifles economic growth and amplifies the risk of cyber-attacks. The gap is known to be an issue for cyber-enabled practitioners–whose primary responsibilities are not related to Cyber Security–as well as practitioners whose primary responsibilities are related to Cyber Security.

Objective: We aim to map cyber-enabled job roles to knowledge areas within the Cyber Security Body of Knowledge (CyBOK). In doing so, we aim to raise awareness and adoption of the CyBOK amongst cyber-enabled practitioners, which will help to address the UK Cyber Skills Gap.

Method: We held a mapping workshop with cyber-enabled practitioners and worked together to map their job roles to the CyBOK. After the workshop, we created resources and held a showcase event to disseminate the mappings to a wider audience of cyber-enabled practitioners.

Results: We present the mappings as results alongside an evaluation of the mapping workshop we held. Together, these results demonstrate the value of holding further mapping workshops (using session plans and supplementary resources we have created).

Conclusion: Further work is needed to build on the preliminary mappings presented in this report. We recommend the workshop resources that we have developed and trialed are used to co-produce mappings with greater quantity and variety of cyber-enabled practitioners.

Keywords: CyBOK, Cyber Security, Cyber-Enabled Practitioners, Co-Inquiry

Version History

Version No.	Date	Comment
0.0.1	07.07.23	Initial version for comments.
0.0.2	25.07.23	Actioning initial comments.
1.0.0	27.07.23	Camera ready version.

Contents

List of Figures

1 Introduction

1.1 Context and motivation

The UK Cyber Security Body of Knowledge aims to systematise established knowledge that is related to Cyber Security. This project is a response to the CyBOK and a call for funded outreach, adoption, and awareness projects. In this project, we have co-produced mappings of job roles to CyBOK knowledge areas to raise awareness of the CyBOK and make it easier for cyber-enabled practitioners to adopt.

The UK Cyber Skills Gap is the primary motivation for this work. Specifically, we are motivated by a series of government reports that highlight a skills gap with respect to cyber-enabled practitioners. In general, skills gaps in general stifle economic growth, output, and productivity. In the case of Cyber Security skills gaps, there is an additional issue as the risk of cyber-attacks is amplified, which can result in broader harms to wider society. We are aiming to raise awareness and adoption of the CyBOK to help address this issue.

1.2 Objective and Research Question

The objective of this research is to raise awareness and adoption of the CyBOK. To achieve this, we have worked with cyber-enabled practitioners to co-produce mappings of their job roles to CyBOK knowledge areas and answer the research question:

What CyBOK knowledge areas are the most relevant for cyber-enabled practitioners?

We also begin to explore the utility and accessibility of the CyBOK to cyber-enabled practitioners more generally. We present preliminary results that help to answer the questions, however, our main contribution is a collection of resources that can be used to do further work raising awarness and adoption of the CyBOK.

1.3 Contributions

- Session plan and learning materials for a mapping workshop, designed to help raise cyber-enabled practitioner awareness and adoption of the CyBOK (with the initial evaluation with a small cohort suggesting it achieves this).[1]
- Cyber-enabled practitioner roles mapped to CyBOK high-level categories and knowledge areas. These mappings aimed to share the findings of the mapping workshop with a wider group of cyber-enabled practitioners, such that their awareness of the CyBOK is raised and knowledge areas relevant to their role are highlighted. They were disseminated via:
  - A short mapping booklet.[2]
  - An interactive web application.[3]
  - An online showcase event at which findings were shared.[4]

1.4 Roles of Authors

The author Sam Attwood was responsible for resource creation and facilitating a mapping workshop. The author Rupak Kharel provided supervisory support and observed the mapping workshop. Both authors prepared a first draft of this report. Feedback was then provided by the funding body–the Cyber Security Body of Knowledge–and actioned by both authors.

[1] https://github.com/samattwood9/cybok-session-coinquiry
[2] https://github.com/samattwood9/cybok-coinquiry-booklet
[3] https://cybok-maps-coinquiry.streamlit.app
[4] https://github.com/samattwood9/cybok-slides-coinquiry

2 Related work

The Cyber Security Body of Knowledge (CyBOK) is a significant effort to systematise knowledge that is recognised as belonging or being related to the field of Cyber Security [11].

An initial version (1.0) of the CyBOK was arrived at through a series of consultation workshops, online surveys, and calls for position papers [11]. It was updated in response to community feedback and version 1.1 was launched July 2021 with two new knowledge areas: Applied Cryptography and Formal Methods for Security. The next phase of the CyBOK project will focus on dissemination and promotion. One of the key aims of the CyBOK is to support academia in designing curricula related to Cyber Security, though there are ambitions for it to be used in industry and government also.[5] To date, CyBOK has been most widely adopted in academia. In [5], curricula frameworks are characterised by their mapping to CyBOK knowledge areas. Furthermore, the CyBOK is now used as a tool to help certify degrees in the UK [10].

Most of the prior mapping efforts relating to the CyBOK have focused on higher education and professional certifications; in a recent mapping booklet [9], 50 degree programmes and 6 professional certifications are mapped to CyBOK knowledge areas. Other mapping efforts include [4], which maps UK theses to CyBOK knowledge areas, and [6], which maps Cyber Security games to CyBOK knowledge areas. The latter effort highlights two challenges around mapping non-static content that are pertinent to this work given we similarly have little static content to inform our mappings:

- *Not everything is about cyber security.* When mapping games to the CyBOK, researchers found that participants playing the games scarcely talked about Cyber Security [6].
- *There isn't a lot to map.* Whilst the games studied did contain Cyber Security content, this was not reflected in the discussion of participants playing the games and there was consequently little data to map to CyBOK knowledge areas [6].

Static content such as job descriptions/listings could have been considered as a part of our mappings. A recent study presents emerging results in which developer and information technology job listings are mapped to CyBOK knowledge groups and areas using natural language processing [2]. However, such studies do not acknowledge the lived experience of practitioners, who may feel their job description is not an accurate representation of the work they do. Furthermore, when considering cyber-enabled practitioners, their roles and responsibilities relating to Cyber Security are less likely to be mentioned in job listings because they are not their core responsibilities.

In this work, we aim to recognize the lived experience of practitioners through co-operative inquiry and participatory research. There has been some prior work relating to participatory research and Cyber Security. In [3], the authors identify different forms of co-production relating to Cyber Security, with a focus on Cyber Crime. In [1], the authors aim to co-produce solutions and standards for data sharing. Overall, there is a recognized need to collaborate and co-produce solutions to improve Cyber Security.

3 Method

We have referred to our method as co-operative inquiry. Broadly, co-operative inquiry involves doing research *with* people and communities rather than *on* people and communities [7]. This is related to participatory research; a class of research methods where people with lived experiences of the topic of study are treated as co-creators of knowledge [8]. In this initial study, we have engaged in this kind of participatory research through two events:

[5] https://www.cybok.org/ataglance/

1. *A mapping workshop.* This included an introduction to the Cyber Security Body of Knowledge (CyBOK) and mapping activities.

2. *A mapping showcase.* Between the workshop and the showcase, several resources were created using the outputs of the mapping activities (see section 4). The showcase event provided an opportunity to for co-creators and the wider community to provide feedback on these resources and the mappings themselves. Invited speakers giving presentations leading into a panel discussion with audience participation.

3.1 Structure of the mapping workshop

1. The mapping workshop began with an introduction to Cyber Security, the CyBOK, and the history of the CyBOK. A facilitator explained that the CyBOK aims to systematise knowledge that is related to Cyber Security and provided an overview of the different knowledge areas. Following this, the same facilitator provided an overview of the intended learning outcomes for the mapping workshop and explained how the findings of the mapping workshop would be disseminated. This initial introduction to the workshop was kept brief; the aim was to set boundaries and expectations without the facilitator becoming a focal point for the remainder of the workshop.

2. Practitioners then formed groups based on their job roles. The aim was for practitioners with broadly similar job roles to form groups so that they could then work together to produce a mapping for that group. No restrictions were imposed on the size of the groups and practitioners were free to form their own group if they felt their role was not sufficiently similar to any other role. Once formed, practitioners created a descriptive name for their groups.

3. Each group then worked to create an initial map of their Cyber Security knowledge and was supplied with a blank sheet of paper, sticky notes, and pens. The aim of this activity was for each group to build a shared understanding/language of Cyber Security independent of the CyBOK, which would then aid their mappings to the CyBOK in the next part of the workshop. To conclude this part of the workshop, a representative of each group reported back on their initial mapping.

4. Each group then worked to map their descriptive job title/role to the CyBOK knowledge areas. Each group was supplied with a mapping worksheet to facilitate this, along with sticky notes and pens. Examples in the form of degree programme mappings [9] were shown, but no further guidance was offered from the facilitator initially. When disagreements or confusion arose the facilitator helped the group reach a meaningful and creative resolution without pushing for premature order. To conclude this part of the workshop, a representative of each group presented a summary of their collective mapping to the wider group.

5. At the end of the workshop, practitioners were encouraged to reflect on their experience and had the opportunity to share their thoughts anonymously by using stickers to answer questions relating to the workshop and the CyBOK more generally. These questions asked practitioners to agree or disagree with the following statements using a Likert scale: (1) I have a greater understanding of the CyBOK having attended todays workshop; (2) I have a greater understanding of how the CyBOK relates to my job role; (3) I think the Cyber Security is important with respect to my job role; (4) I think the CyBOK is an accessible resource and will use it support my work; (5) I think improvements need to be made to make the CyBOK more widely accessible and applicable.

3.2 Structure of the showcase

1. The showcase began with a welcome address, which included a short summary of the project overall, acknowledged the funding, and introduced the speakers.

2. Invited talk: Resilience for Cyber-Enabled Practitioners. This introduced the term cyber-enabled practitioner and highlighted relevant resources and guidance offered by the North West Cyber Resilience Centre.

3. Keynote: Mapping Cyber-Enabled Roles to the CyBOK. This communicated the findings of the mapping workshop and highlighted the resources developed as a part of the project.

4. Invited talk: Building Citizen Trust in AI through Public Engagement and Co-Production. This highlighted challenges and opportunities relating to Co-Production, with reference to several projects concerning Artificial Intelligence.

5. Panel discussion: The CyBOK and Co-Production. This provided attendees with an opportunity to give feedback on the mappings that had been created and the CyBOK itself and discuss ideas for next steps.

6. The showcase ended with the chair thanking the speakers and audience for their participation. At this point, a padlet was shared with all attendees, providing a space for anonymous feedback on the created resources to be provided.

4 Results

4.1 Initial Mappings

Figure 1 shows the initial mappings created in the mapping workshop. These mappings demonstrate the differing depth and breadth of Cyber Security knowledge across the different groups. For example, the initial mapping created by a group of 'Software Developers' highlighted items such as 'Security Headers' and 'Wordpress Hardening Techniques', which did not feature in the initial mappings of other groups. Equally, the initial mappings highlight common knowledge that was shared across the groups. For example, all but one of the mappings featured a 'Phishing' item.

4.2 Mappings to the CyBOK

Figures 2, 3, 4, 5, 6, and 7 show the main mappings (to the CyBOK) created in the mapping workshop. These mappings highlight the knowledge areas and groups practitioners considered most relevant to their roles. Overall, the open-ended nature of the mapping activity allows for deep insights, with practitioners being free to add caveats and highlight areas of uncertainty and/or importance in their mappings. Figure 6 is an especially good example of this, with the practitioners in this group separating their management responsibilities from other the other aspects of their roles.

4.3 Project Evaluation

Figure 8 shows responses to a short survey practitioners were asked to complete after the mapping workshop. The responses show that the participating practitioners considered the CyBOK to be a useful and accessible resource, and that the mapping workshop had helped to raise their awareness of the CyBOK as well as their ability to adopt and use it as a part of their job roles.

No evaluation was done for showcase event, which was attended by an additional 12 cyber-enabled practitioners.

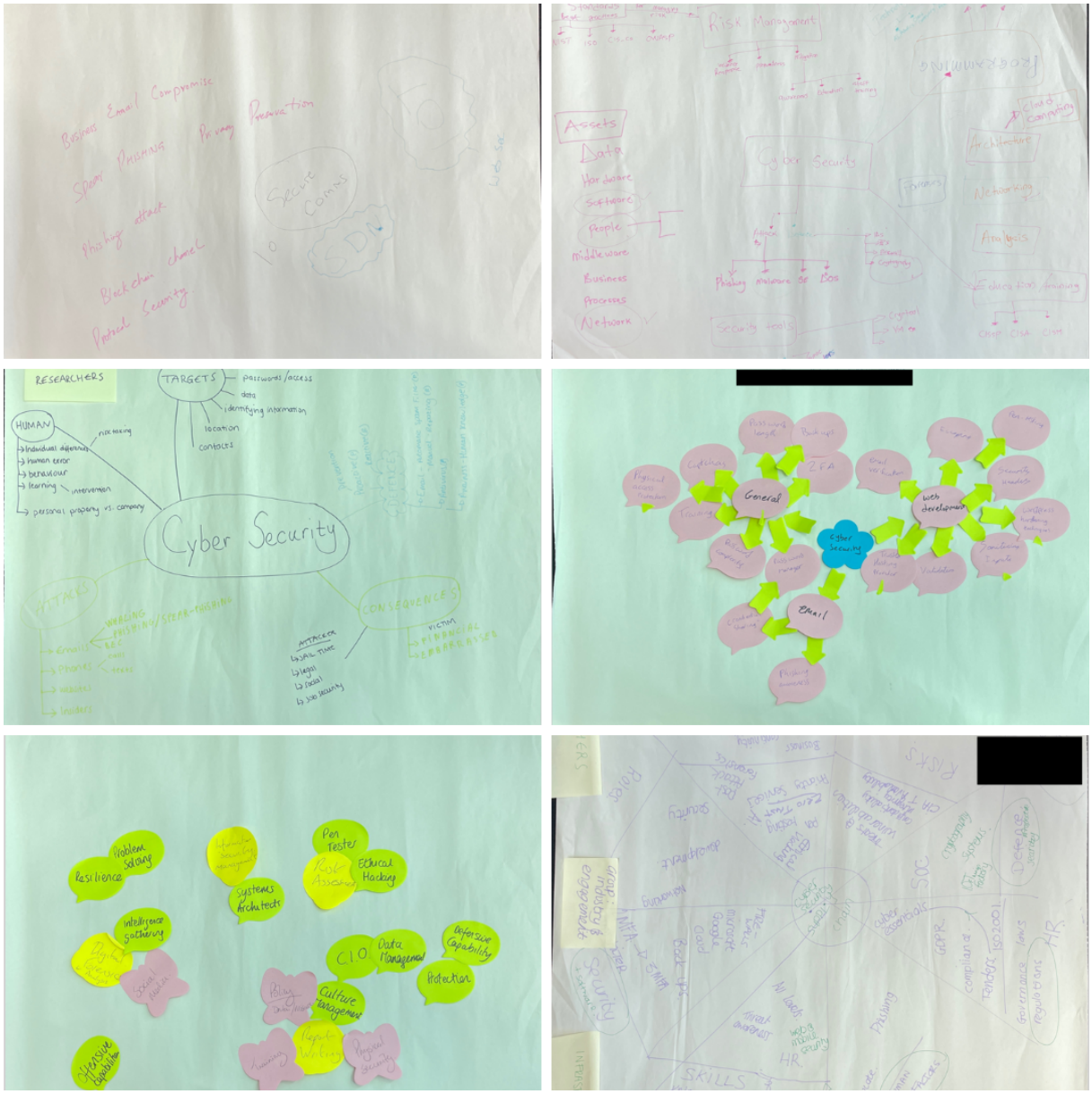

Figure 1: Initial mappings.

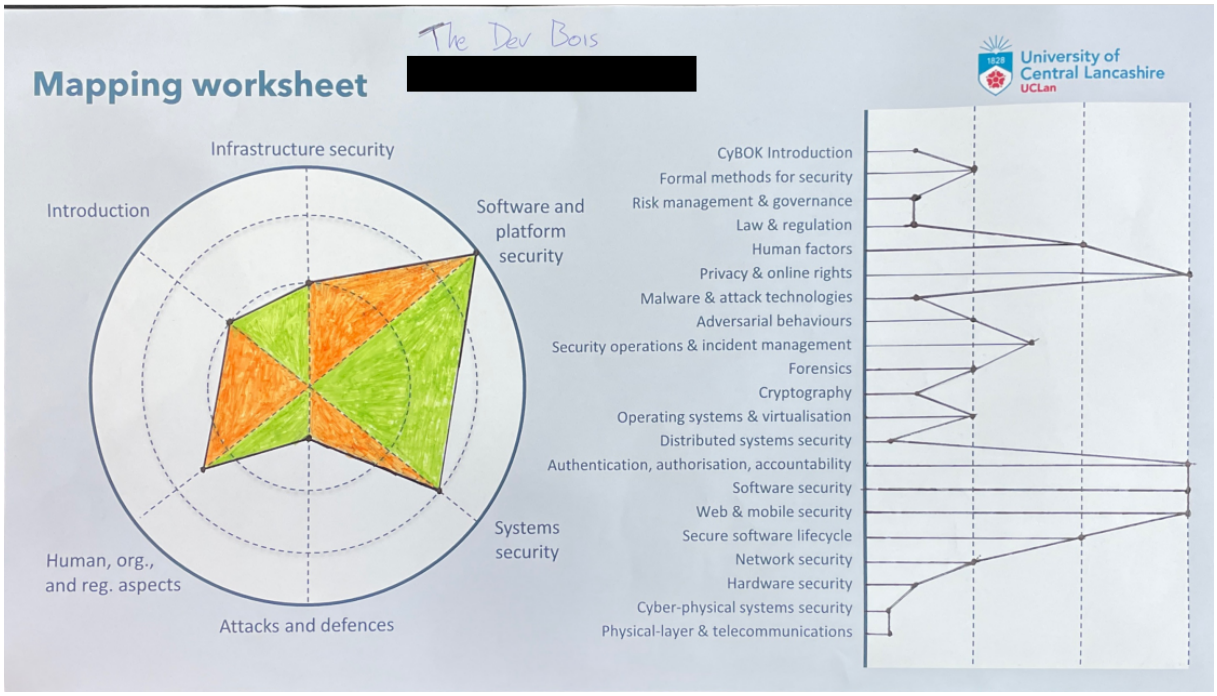

Figure 2: Mapping to CyBOK areas created by a 'Software Developer' group.

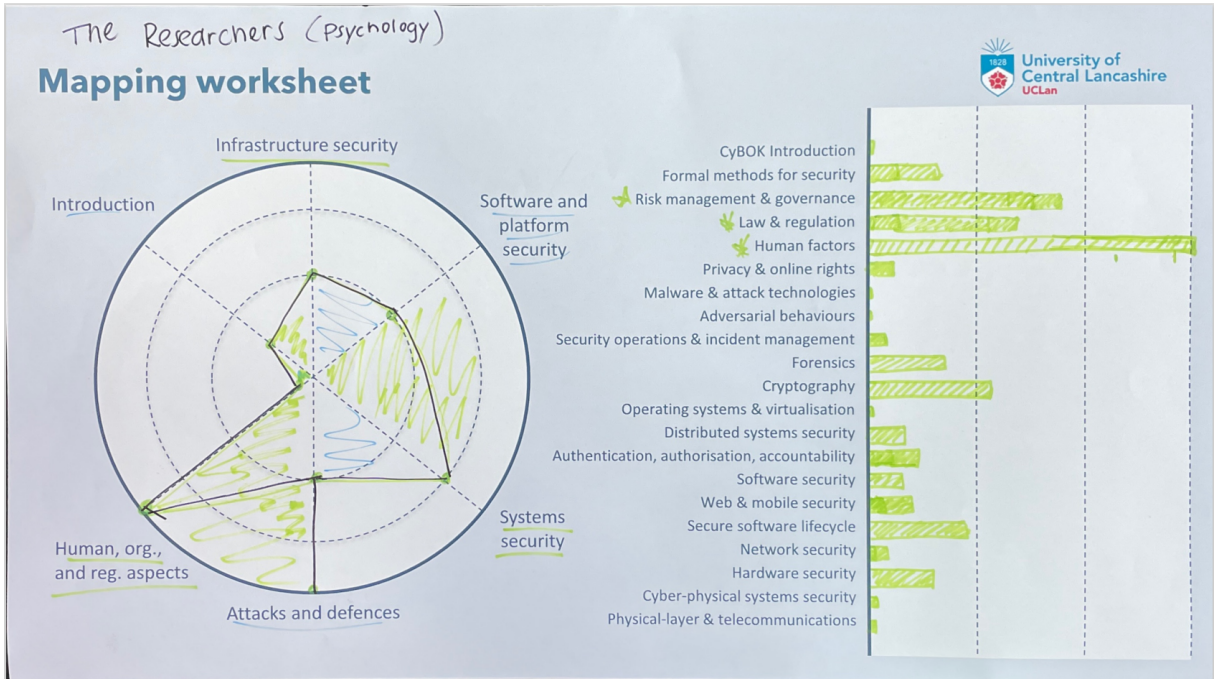

Figure 3: Mapping to CyBOK areas created by a 'Researchers (Psychology)' group.

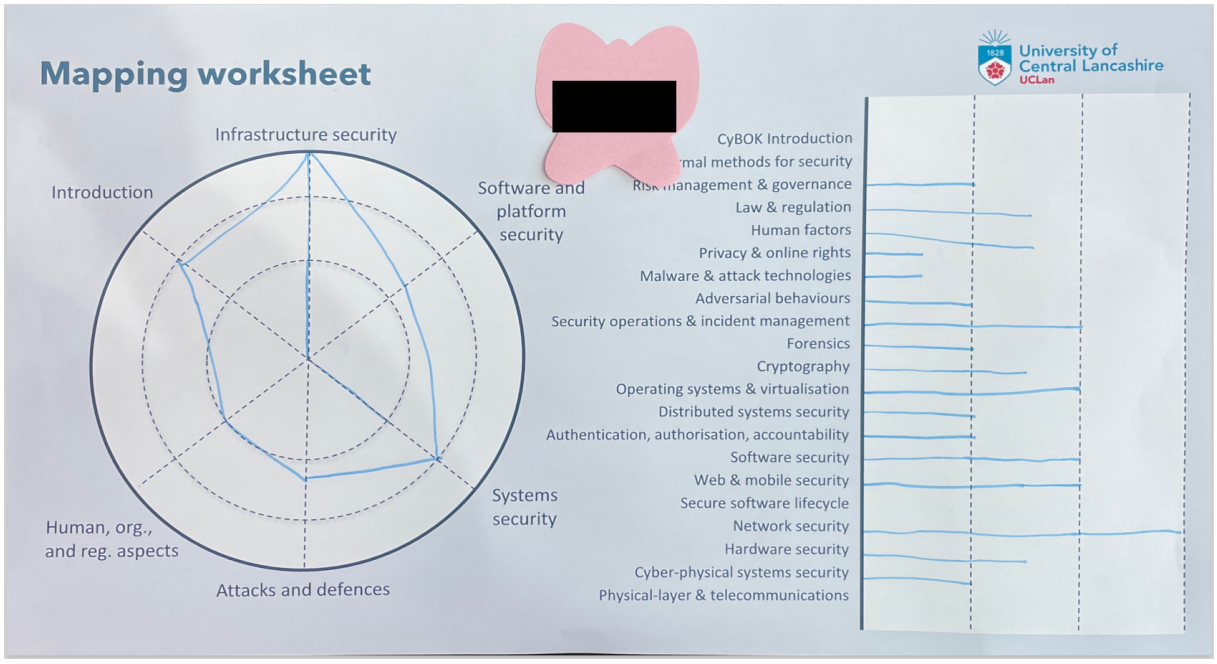

Figure 4: Mapping to CyBOK areas created by an 'Education' group.

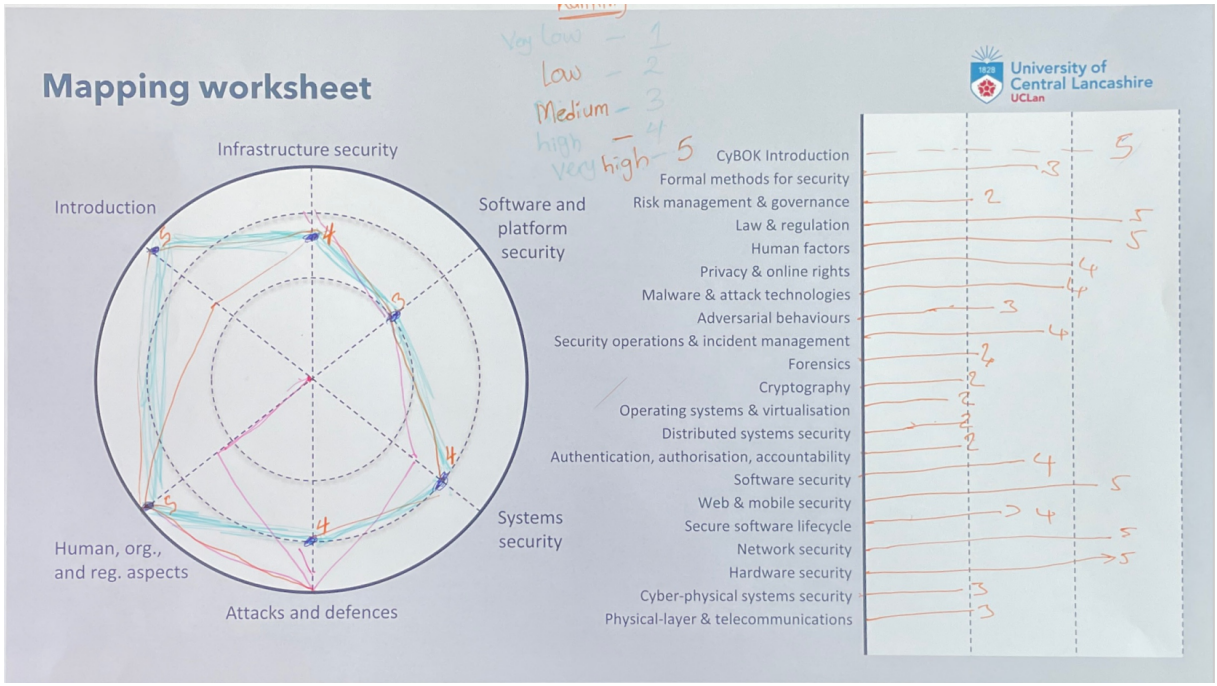

Figure 5: Mapping to CyBOK areas created by a 'Future Educators' group.

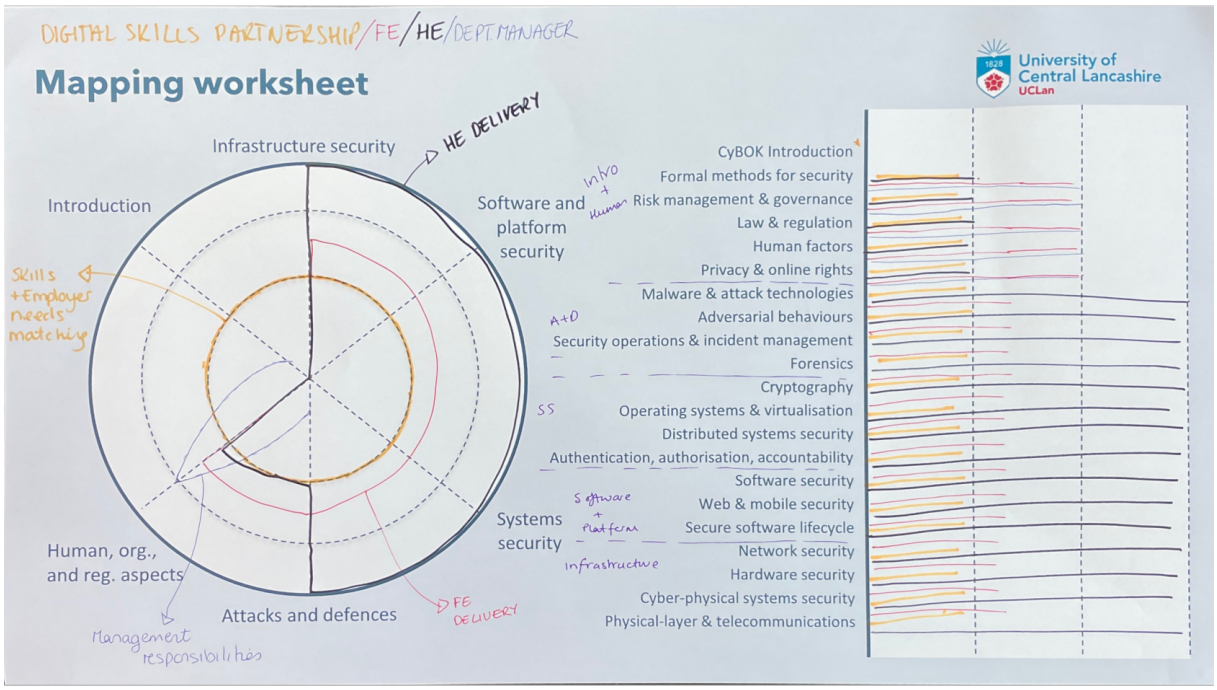

Figure 6: Mapping to CyBOK areas created by an 'Education & Partnerships' group.

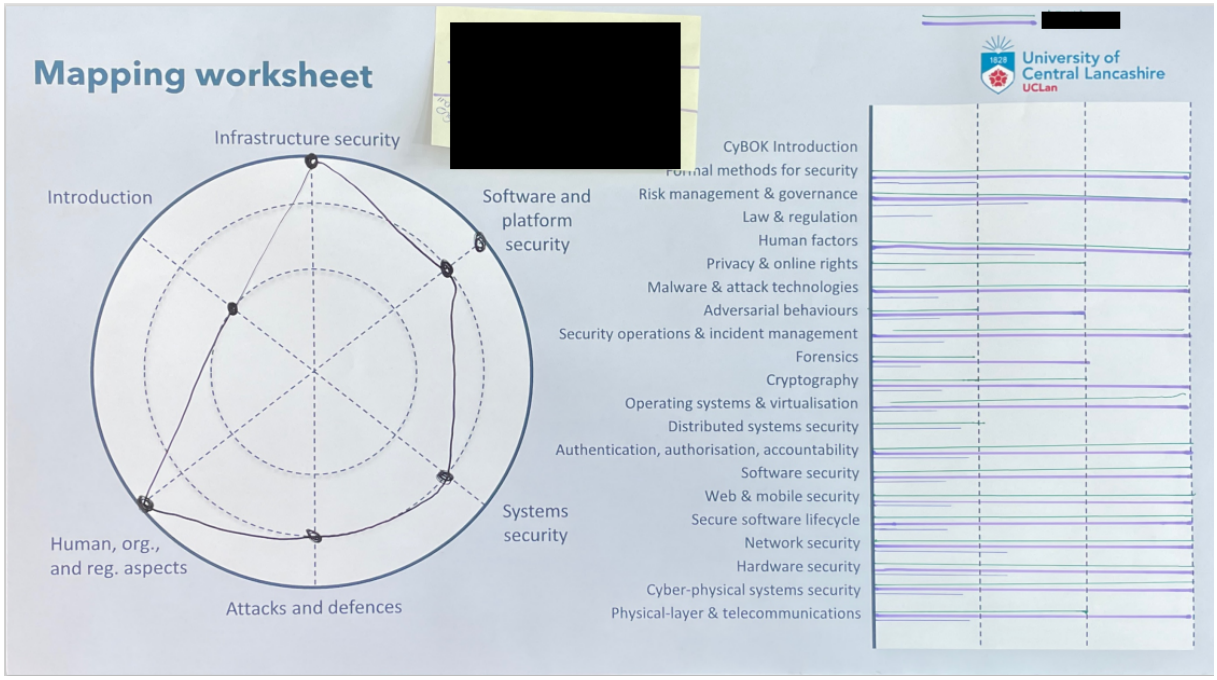

Figure 7: Mapping to CyBOK areas created by a 'Business Development' group.

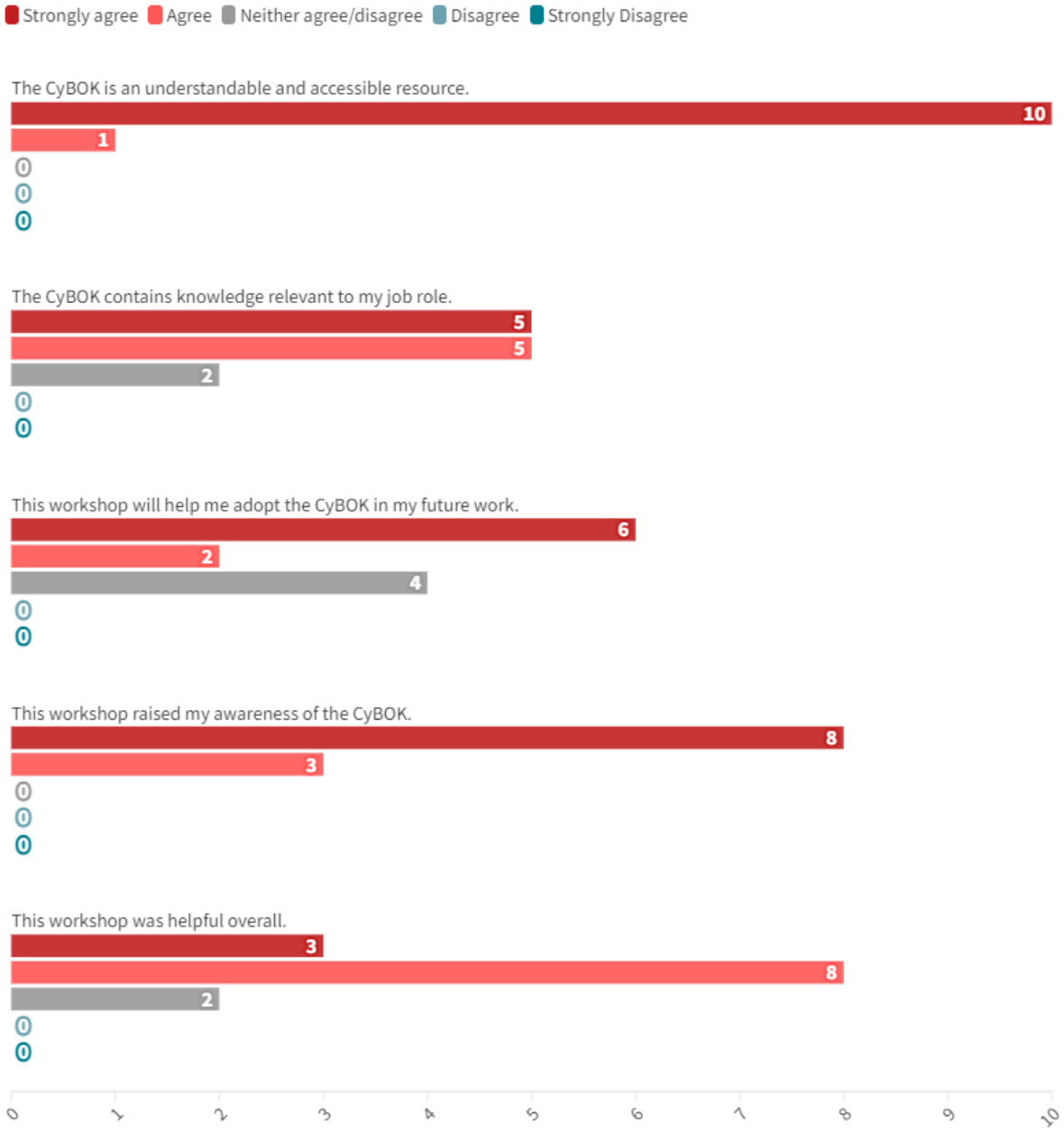

Figure 8: Evaluation of the mapping workshop.

4.4 Supplementary Resources

The left panel of figure 9 shows a page from the short mapping booklet that was created to disseminate the mappings to a wider group of cyber-enabled practitioners. The right panel shows a screenshot of an interactive web application that was created for the same reason. Links to both resources are available in section 1.

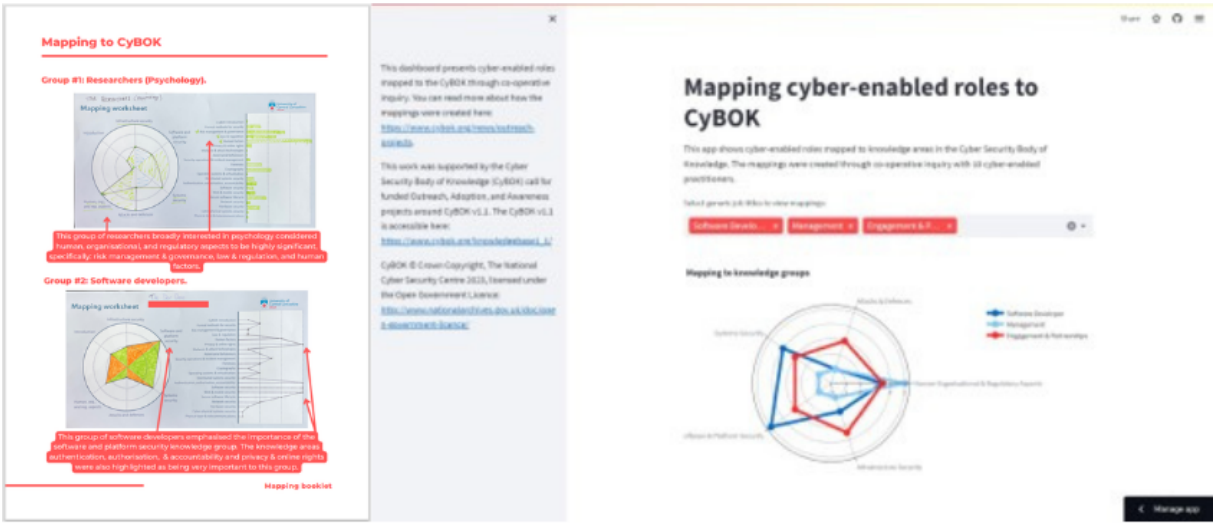

Figure 9: Page from mapping booklet (left) and screenshot of web application (right).

5 Limitations, Future Research & Conclusions

The mappings presented in this paper should be considered preliminary mappings, with the relatively low number of practitioners that helped to produce the mappings limiting their potential as mappings that are representative of any job roles in general. Moreover, we have only produced mappings for a low number of job roles: Software Developers, Psychology Researchers, and Educators. Further work needs to involve a greater number of practitioners and a greater variety of practitioners to address these limitations. Additionally, we do not currently recommend the mappings be compared to mapped degree programmes, this is because further work is needed to reconcile the different mapping approaches.

The workshop resources we have developed and trialed have received positive feedback, with survey responses suggesting these helped raise practitioner awareness of the CyBOK and also their ability to adopt and use the CyBOK. The survey responses also suggest that the CyBOK itself is an accessible and relevant resource.

In summary, further work is needed to build on the preliminary mappings presented in this report. We recommend the workshop resources that we have developed and trialed are used to co-produce mappings with greater quantity and variety of cyber-enabled practitioners.

Acknowledgements

This work was supported by the Cyber Security Body of Knowledge (CyBOK) call for funded Outreach, Adoption, and Awareness projects around CyBOK v1.1. CyBOK © Crown Copyright, The National Cyber Security Centre 2023, licensed under the Open Government Licence: http://www.nationalarchives.gov.uk/doc/open-government-licence/

We would also like to thank the cyber-enabled practitioners who helped co-produce these mappings. Without them this work would not have been possible. Additionally, our invited speakers at the showcase, Prof. Keeley Crockett, Jared Thompson, and Jacob Alcock.

References

[1] Amir Atapour-Abarghouei, A Stephen McGough, and David S Wall. "Resolving the cybersecurity Data Sharing Paradox to scale up cybersecurity via a co-production approach towards data sharing". In: *2020 IEEE International Conference on Big Data (Big Data)*. IEEE. 2020, pp. 3867–3876.

[2] Sam Attwood and Ashley Williams. "Exploring the UK Cyber Skills Gap through a Mapping of Active Job Listings to the Cyber Security Body of Knowledge (CyBOK)". In: *Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering*. EASE '23. Oulu, Finland: Association for Computing Machinery, 2023, pp. 273–278. ISBN: 9798400700446. DOI: 10.1145/3593434.3593459. URL: https://doi.org/10.1145/3593434.3593459.

[3] Lennon YC Chang, Lena Y Zhong, and Peter N Grabosky. "Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime". In: *Regulation & Governance* 12.1 (2018), pp. 101–114.

[4] Virginia Franqueira, Jason Nurse, Shujun Li, and Rahime Belen Saglam. *Mapping PhD Theses of UK Universities to CyBOK*. Tech. rep. University of Kent, Oct. 2021.

[5] Joseph Hallett, Robert Larson, and Awais Rashid. "Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks". In: *USENIX Workshop on Advances in Security Education*. 2018.

[6] Joseph Hallett and Benjamin Shreeve. *Mapping of cybersecurity games onto CyBOK*. Tech. rep. University of Bristol, Feb. 2022.

[7] John Heron and Peter Reason. "The practice of co-operative inquiry: Research 'with'rather than 'on'people". In: *Handbook of action research: Concise paperback edition* (2006), pp. 144–154.

[8] Caroline Lenette, Nelli Stavropoulou, Caitlin Nunn, Sui Ting Kong, Tina Cook, Kate Coddington, and Sarah Banks. "Brushed under the carpet: Examining the complexities of participatory research". In: *Research for All* 3.2 (2019), pp. 161–179.

[9] *Mappings of University and Professional Training Programmes to the CyBOK*. Tech. rep. University of Bristol, Apr. 2023.

[10] Lata Nautiyal, Awais Rashid, Joseph Hallett, and Ben Shreeve. *The UK's Cyber Security Degree Certification Programme: A CyBOK Case Study*. Tech. rep. May 2020.

[11] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. "Scoping the Cyber Security Body of Knowledge". In: *IEEE Security & Privacy* 16.3 (2018), pp. 96–102. DOI: 10.1109/MSP.2018.2701150.