Getting on the front foot:

Reimagining the future of Cyber Incident Response

Emma Woodward [Morris]

em2296@bath.ac.uk

Supervision

Prof Adam Joinson

Dr Barney Craggs

Prof Danaë Stanton Fraser

Why?

A fresh approach is needed to defend against the increasingly sophisticated and creative cyber attacks emerging [2]. In order to design and engineer effective solutions, there is a need for a broader contextual awareness of IR [3] that considers the sociotechnical factors holistically [4]. This is key to understanding unbiased approaches to improving IR [3] and is an area lacking research [5]. Visualising problems in complex sociotechnical systems is challenging because of the limit of human cognitive abilities [6]. Therefore, there is an opportunity to pair a systems engineering approach to develop tools to understand the complex system of IR, with design and creative methodologies to provide innovative solutions and ways to reimagine the futures of IR.

Key Research Qs

1. What methods [e.g., ethnomethodology] are appropriate to use for studying Cyber Security Incidence Response?

2. What is the best way to visualise the holistic system view of Incident Response?

   What are the challenges/ problems within Incident Response and how have they been framed?

3. What ideation techniques are successful for engaging multiple disciplines in an innovation sprint for Incident Response?

   What could the requirements of an Incident Response system be?

References

[1] L. G. E. S. Alicia Cork, David A. Ellis, Danaë Stanton Fraser and Adam Joinson, "Rethinking Online Harm: A Psychological Model of Contextual Vulnerability," 2022

[2] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," Journal of the Association for Information Science and Technology, vol. 71, no. 8, pp. 939-953, 2020-08-01 2020, doi: 10.1002/asi.24311.

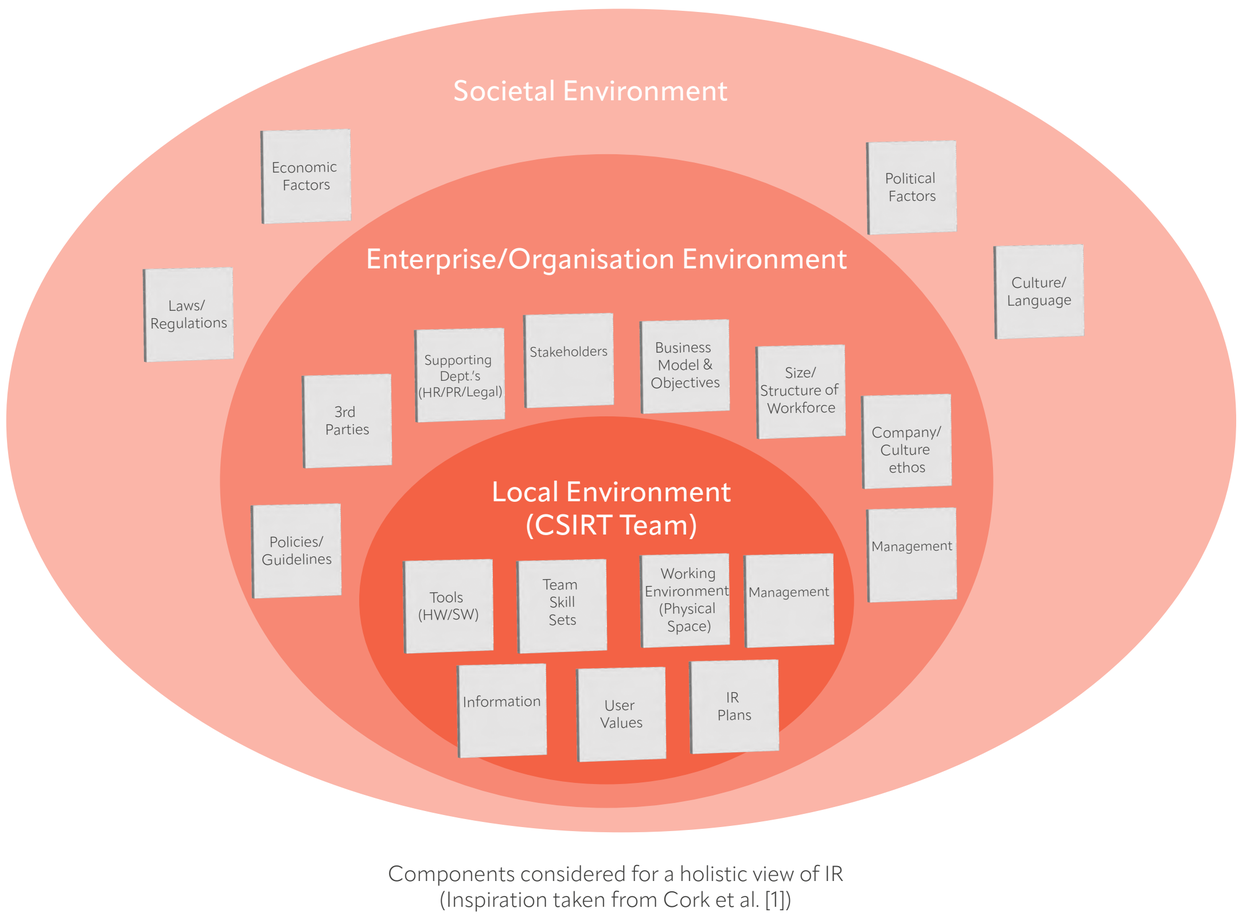
[3] M. Nyre-Yu, R. S. Gutzwiller, and B. S. Caldwell, "Observing Cyber Security Incident Response: Qualitative Themes From Field Research," Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 63, no. 1, pp. 437-441, 2019-11-01 2019, doi: 10.1177/1071181319631016.

[4] H. L, "A sociotechnical approach to cyber security," vol. 2022, ed. National Cyber Security Centre, 2022.

[5] A. A. Ashley O'Neil, Sean B. Maynard, "Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training," Australasian Conference on Information Systems, 2021.

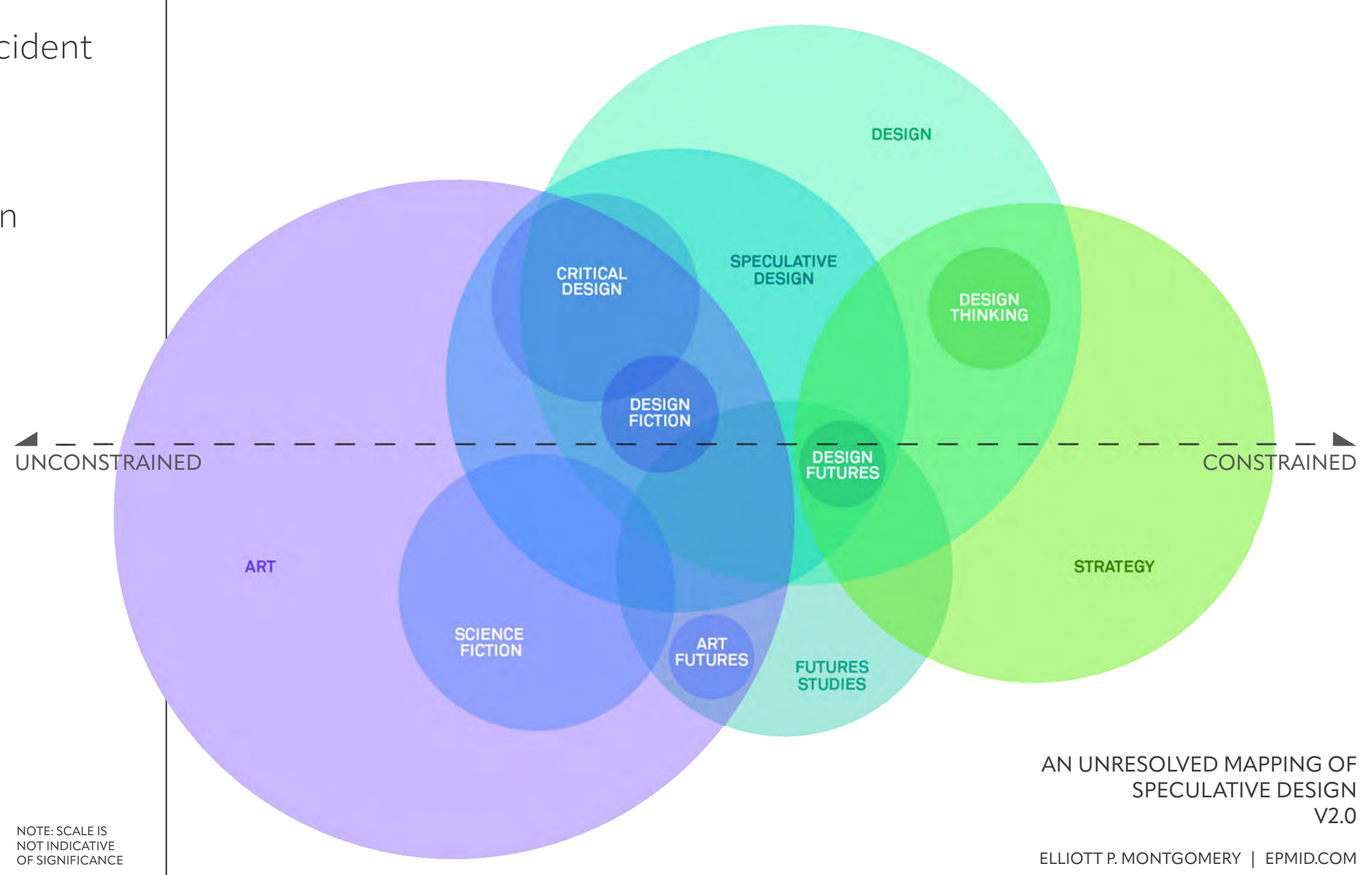
[6] H. L, "Sociotechnical Security Group Handbook: An outline of the StSGs future research in Cyber Security," ed, Unknown

Merging my **design and innovation** background with a **Systems Engineering** approach to construct a **holistic view** of incident response...



Components considered for a holistic view of IR
(Inspiration taken from Cork et al. [1])

...and using **creative methodologies** to **speculate** its **futures**.



I'm looking for internships in Incident Response Teams

Engineering and Physical Sciences Research Council

University of BRISTOL

UNIVERSITY OF BATH