Praxis + Poetics
Research Through Design 2013

‘IT Fauna’ and ‘Crime Pays’: Using Critical Design to Envision Cyber Security Futures

Debi Ashenden
Cranfield University
Shrivenham, Swindon
SN6 8LA UK
d.m.ashenden@cranfield.ac.uk

David Benqué
Royal College of Art
david.benque@network.rca.ac.uk

Austin Houldsworth
Royal College of Art
austin.houldsworth@network.rca.ac.uk

Abstract

The research presented is a collaboration between social scientists, designers and technologists that explored whether critical design could be used to envision cyber security futures. The research imperative was to examine the use of critical design as a way of imagining future or alternative scenarios of cyber security. We evaluated research methods that would encourage cyber security practitioners and policy makers to discuss and re-consider cyber security risk.

The research used critical design to produce speculative scenarios that would encourage a new way of thinking about cyber security risk. ‘Specimens of IT Fauna’ is a visualisation and celebration of our imaginary bestiary of software. ‘Crime Pays’ is a video installation that envisions a future where there is effectively a tax on online privacy.

The artefacts were used in two workshops to encourage cyber security practitioners and policy makers to envision future risk scenarios. The research demonstrated that while there is potential for using critical design in this way there is a need to develop a bridge between the artefacts produced through critical design and the epistemological position traditionally taken towards risk by cyber security practitioners and policy makers. We conclude that future research should link critical design with systems thinking as the next step in developing tools for envisioning future cyber security risk. This will offer a structured way for moving to a more productive level of engagement with the artefacts while giving participants a license to be creative and a way of incorporating the human experience.

Author Keywords

Critical design; speculative design; cyber security; envisioning

Research Imperatives

The research outlined in this paper was part of a larger project called Visualisation and Other Methods of Expression (VOME). The VOME research was located in the relatively young research discipline of cyber security and focused on issues of privacy, identity and consent in online environments and engaging primarily with end user communities. The research explored the use of novel methods of engagement and an early outcome was the recognition of a need to ‘design culturally sympathetic research approaches’ (Coles-Kemp and Ashenden, 2012, p.2) to understand how end users perceive cyber security risks.

Figure 1. Specimens of IT Fauna Low Orbit Ion Cannon (1 of 3 models) Laser etched crystal - other models in the series are 'Blaster Worm' and 'Web Crawler'.

Figure 2. Crime Pays: Some grease to seal the deal (1 of 3 photos). Video and three photographs depicting social change as a result of the new payment system.

During the course of the research, however, the importance of engaging with cyber security practitioners and policy makers instead of just end users became clear. As a result the VOME researchers came together with designers to explore the use of critical design to engage with cyber security practitioners and policy makers. Accordingly, the research presented here examines the use of critical design as tool for imagining future cyber security risks.

The analytical approach for the research is critical design which creates 'provocative artefacts' (Dunne and Raby, 2001, p.63) by using critical theory with design to make us think about things we believe we know in new and different ways. Such artefacts are often more effective than direct questioning techniques in enabling user communities to engage with future possibilities (Bowen, 2007). Critical design offers a participatory practice approach and so continues the VOME research theme of exploring novel methods of engagement. As such, critical design was thought to be an appropriate tool for developing ways to envision cyber security risk.

Research Process

We started with an initial consultation workshop where cyber security academics explored what the impact of new, online security technologies might be on our society and culture. Following on from this there were informal discussions to share the existing research output from the VOME project with the designers. The aim of these initial discussions and workshops was to find a common ground for exchange between designers and experts. Narrative was used as a tool through exercises such as improvisation from random prompts and the creation of fictional tabloid articles. Both parties were able to collaborate on stories, then examine and discuss them.

Designers then used these exercises as a starting point to formulate more specific and nuanced stories. In the case of *Crime Pays,* this led to the imagination of a future scenario and payment system, while *Specimens of IT Fauna* focuses on existing but overlooked narratives and metaphors used to describe the internet. Artefacts were then designed within these narratives premises, giving the stories and ideas a tangible physical presence and enabling further dissemination and discussion.

Specimens of IT Fauna (Fig. 1) was designed with educational props in mind, referencing the science classroom. The small scale of the objects and the explanatory labeling encourages manipulation and discussion while the use of laser etching and lighting provides an aesthetic 'hook' and a sense of technological wonder.

The *Crime Pays* (Fig. 2) video mimics the aesthetic qualities of a corporate presentation and only the filmic letterbox format hints that this is fiction. The video brings 'The Yes Men' activist approach into a consenting corporate conference and invites the expert audience to play along. Within a workshop setting the video is displayed alongside photographs depicting three imagined social scenes. The minimalist style of these photos is intended to push the characters human interaction to the foreground, thereby directing discussions from the abstract system to the possible impact on people's lives.

We subsequently ran two workshops to showcase the artefacts and to explore their use as ways of envisioning cyber security future risk. The workshops were held at the British Computer Society in London – a venue where it was believed that participants (working in the field of cyber security) would feel comfortable. Participants were self-selecting as the workshops were publicized through existing networks for cyber security practitioners and policy makers. There were twelve attendees at each workshop and each workshop was three hours in length. The workshops started with a short presentation to set the context of cyber security risk and critical design and this was followed by the designers introducing the artefacts. Participants were then encouraged to ask questions,

discuss with each other and reflect on the artefacts. Their outputs were captured on 'post-it' notes as well as rich-pictures drawings.

Research Outcomes

Please describe the resulting knowledge that arose from the practice-based research. This should be placed in the context of an existing disciplinary body of knowledge through the use of references.

Cyber security risk has traditionally been encapsulated by the engineering and physical sciences where risk is seen as knowable and measurable. The potential value, however, of cyber security risk artefacts for 'interpretively expressing professional knowledge' (Baskerville, 1991, p.749) has been suggested and the Blackett Review on 'High Impact Low Probability Risks (Government Office for Science, 2011,) concluded that there is a need for tools that will allow experts to imagine risks in a way that will 'expand the boundaries of their mental models' (p.11).

Accordingly the aim of this research was to evaluate the use of critical design as a research technique for imagining future cyber security risk. We wanted to move beyond the approaches used in VOME and towards a future-looking, creative approach with a practitioner and policy maker user community. We learned three lessons through the workshops.

Firstly, it takes effort for participants to become engaged and conversant with critical design artefacts and there was initial confusion over the purpose and use of the artefacts presented. In time, however, participants commented that the artefacts made them realise how they had become 'dependent on a common language' within their field of expertise and that 'it's hard to move past that'. They did feel that the pieces gave a 'different perspective', that made them 'think differently' and realize, 'how we have normalized images'. While they were beginning to engage in self-reflection it was difficult to move them beyond this to a more future-thinking level of engagement.

Secondly, participants needed to be given a license to be creative. They had a tendency to retreat to what they have already experienced or believed to be true. This was demonstrated in references to practical questions about cyber security ''where are the boundaries to defend – in the cloud, at the end of a network, in a device, or in the user's heads?' and citing of specific implementations of technology such as, 'Mondex, c1993, Natwest' (the unsuccessful invention of an electronic cash system by the National Westminster bank).

Thirdly, participants needed to understand how the artefacts could be experienced. They felt that the artefacts would be 'comprehensible by mums (and dads)' but that, 'they [IT Fauna] need a narrative'. They needed to see how others experienced these artefacts and asked, 'where is the human element?' commenting that the artefacts needed to be 'user activity based'. One participant pointed out that 'the internet is entirely experiential – this is where the art should focus'.

Conclusion

Critical design for research is often used in the development of new technologies or products. In this research, however, we were exploring its use as part of the risk assessment process for cyber security. The lessons we learned demonstrate that while there is potential for using critical design in this way we need to develop a bridge between the artefacts and the epistemological position traditionally taken towards risk by cyber security practitioners and policy makers. In the next phase of the research we will aim to link critical design with systems thinking as a further development of tools for imaging future cyber security risk. This may well offer a structured way for moving to a more productive level of engagement with the artefacts while giving participants a license to be creative and a way of incorporating the human experience.

References

1. Baskerville, R. (1991). 'Risk Analysis as a Source of Professional Knowledge', Computers & Security, 10, pp. 749-764
2. Bowen, S. (2007). 'Crazy ideas or creative probes? Presenting critical artefacts to stakeholders to develop innovative product ideas', Proceedings of the European Academy of Design Conference [CD ROM], Izmir, Turkey
3. Coles-Kemp, L. and Ashenden, D. (2012). 'Community-centric engagement: lessons learned from privacy awareness intervention design', Proceedings of HCI 2012 – People & Computers XXVI, The 26th BCS Conference on Human Computer Interaction, Birmingham, UK, 12-14 September 2012
4. Dunne, A. and Raby, F. (2001). Design noir: The secret life of electronic objects. Birkhauser
5. Government Office for Science (2011). 'Blackett Review of High Impact Low Probability Risks' [Online]. Available at: http://www.bis.gov.uk/assets/goscience/docs/b/12-519-blackett-review-high-impact-low-probability-risks (Accessed 31 May 2013)