Institution: Royal Holloway, University of London		
Unit of Assessment: 11 Computer Science and Informatics		
Title of case study: Transforming Cyber Security into a Socially Inclusive Practice		
Period when the underpinning research was undertaken: 2013-2020		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Lizzie Coles-Kemp	Professor of Information Security	2008-date
Period when the claimed impact occurred: 1st August 2013-2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Cyber-crime costs the UK billions of pounds and threatens national security. However, the effects of cyber insecurities on everyday life are not widely acknowledged. Professor Coles-Kemp's research demonstrated how people are often cyber security's strongest link, rather than the weakest. It shows that for cyber security to be effective, security professionals must address the security issues that people across society face in their everyday lives. This work has led to a transformation of professional cyber security practice and the development of security guidance by the UK's National Cyber Security Centre (NCSC) that is centred on people and their daily lives.

2. Underpinning research

Digital technology has moved beyond the controlled environments of corporate and government settings, and it is now ubiquitous in every aspect of life: political, social, corporate and institutional. All parts of society – from welfare claimants to school children and grandparents - are now expected to be on-line and this presents a real challenge to those tasked with ensuring cyber security: how do they engage people across a broad social spectrum and achieve secure practices in the context of diverse day-to-day experiences? The importance of socially inclusive cyber security policies was emphasised by the then CEO of NCSC, Ciaran Martin, in a speech to the Confederation of British Industry in 2017 *(*E.5.5): "*First and foremost, among these is the importance of human factors in designing security policies and controls: every solution must survive contact with the user."*

Prior to Coles-Kemp's research there was little focus on the challenges of widening participation in cyber security programmes. Since 2008, she has researched the social experience of cyber security with a focus on marginalised and under-served communities, often deemed 'hard to reach'. Using community-based participatory research methods, she has worked with families of prisoners, refugees and economically deprived communities as well as office workers who feel excluded by digital programmes. This research showed that framing cyber security advice and policy in line with their security goals as well as in the context of the day to day lives of communities increases their participation in cyber security implementation and training programmes. (R.3.1, R.3.3, R.3.2).

A creative securities approach has been developed through Coles-Kemp's peer-reviewed robust research on the design and use of participatory research methods to address issues of cyber security (R.3.4). Working with the NCSC's Sociotechnical Security Group, Coles-Kemp both developed and tested participatory methods within organisations from the corporate sector, central and local government and in community settings using workshops, focus groups and interviews (R.3.1, R.3.3, R.3.4 and R.3.5) and over the course of the last eight years has worked

with 1,470 research participants. The research showed that if technology is not useful to people, or if it damages their wellbeing, they are less likely to comply with cyber security policies and practices (R.3.1). It also showed that some of the insecurities people face in their everyday lives both result from and are amplified by their interactions with digital technology; and that these everyday issues must be considered when security practitioners frame cyber security advice and promote safer digital practices (R.3.1). This research resulted in digital design principles and methods to both teach and deliver safer, more inclusive digital services (R.3.2, R.3.6). The research tested and developed participatory methods of engagement, termed "*creative securities*", to uncover the fundamental barriers and challenges to safer digital practices.

The creative securities approach was used to investigate how security practices and policies could take account of the political, economic and social aspects of cyber security risk, and the impacts such aspects have on the cyber security concerns of each participant group (R.3.3). These research methods effectively revealed that people consider issues of cyber security in relation to the benefits they derive from digital technology and therefore expert advice must be carefully aligned with these benefits to work effectively. Since 2013 Coles-Kemp has conducted research with 270 cyber security practitioners and digital service providers to better understand their engagement methods and explore how these might be made more people-centred to widen participation in cyber security programmes (R.3.5, R.3.6). Between 2016 and 2019 she also used a creative securities approach to research the cyber security concerns of 240 Syrian and Iraqi refugees in Sweden, leading to greater understanding of the benefits of digital service access via mobile phones (R.3.2, R.3.3). By engaging multiple communities and working in different organisational settings, Coles-Kemp's research has produced robust methods to widen participation in cyber security programmes and improve the take-up of safer digital practices.

In 2020 Coles-Kemp was commissioned by the Department for Digital, Culture, Media & Sport (DCMS) to undertake research as part of a wider digital identity consultation. The brief was to focus on issues of digital inclusion and e-safety as well as the opportunities, barriers and challenges to digital identity use, set-up and maintenance as a part of access to essential everyday digital services. The research was undertaken with grassroots community groups and took place against the backdrop of the COVID-19 pandemic. As a result, the research also identified some of the pressures and challenges of safely using digital technologies during COVID lockdowns.

3. References to the research

These research outputs have been published in peer-reviewed venues, and are underpinned by research funded by EPSRC, ESRC, TSB, EU FP7 and AHRC.

[R.3.1] Coles-Kemp, L., Zugenmaier, A., & Lewis, M. 2014. "Watching You Watching Me: The Art of Playing the Panopticon". Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment, ISBN 978-1-61499-450-3. Chapter Available from HEI on Request.

[R.3.2] Jensen, R.B, Coles-Kemp, L & Talhouk, R 2020, When the Civic Turns Digital: Designing Safe and Secure Refugee Resettlement in *ACM CHI Conference on Human Factors in Computing Systems: CHI'20.* ACM, pp. 1-14. https://doi.org/10.1145/3313831.3376245

[R.3.3] Coles-Kemp, L., Jensen, R.B. and Talhouk, R., 2018, April. In a new land: mobile phones, amplified pressures and reduced capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-13). https://doi.org/10.1145/3173574.3174158

[R.3.4] Dunphy, P., Vines, J., Coles-Kemp, L., Clarke, R., Vlachokyriakos, V., Wright, P., McCarthy, J., Olivier., 2014, Understanding the experience-centeredness of security and privacy technologies**.** in *Proceedings of the 2014 New Security Paradigms Workshop*. ACM, 2014. p. 83-94. https://doi.org/10.1145/2683467.2683475

[R.3.5] Coles-Kemp, L., Jensen, RB., Heath CP., 2020, Too Much Information: Questioning Security in a Post-Digital Society. in *CHI '20: CHI Conference on Human Factors in Computing Systems.* ACM, pp. 1-14. https://doi.org/10.1145/3313831.3376214

[R.3.6] Williams, P & Coles-Kemp, L 2019, Teaching as a Collaborative Practice: Reframing Security Practitioners as Navigators. in Z Pan (ed.), Transactions on Edutainment . vol. XV, Lecture Notes in Computer Science, vol. XV, Springer, pp. 108-128. https://doi.org/10.1007/978-3-662-59351-6_10

4. Details of the impact

"Professor Coles-Kemp's research has shown that people's needs, values and preferences have hitherto not been part of cyber security goals and yet are integral to building a more secure organisation…. Professor Lizzie Coles-Kemp's research and thought leadership in the field has been central to this mindset shift, along with a portfolio of multidisciplinary research that we recognise to being critical to the success of NCSC's endeavours both now and well into the future". Head of Research, National Cyber Security Centre (E.5.5).

Coles-Kemp's research has transformed how the National Cyber Security Centre (NCSC) engages with stakeholders and increased socially inclusive forms of cyber security practice. Her research provided an evidence-based approach that has driven a culture change, resulting in marginalised neighbourhoods and other communities putting in place digital security practices appropriate to their situations. Safer digital inclusion has gained greater political focus during the COVID pandemic and the importance of a digital security for all has come to the fore. Coles-Kemp's research has informed policy discussions and shaped cyber security practice at a national level in the UK, and as well as providing guidance to communities in the UK, Australia and Sweden.

Informing a step-change in cyber security policy and practices:

The primary beneficiary of Coles-Kemp's research is NCSC, the UK's major source of cyber security knowledge for business, industry, government and third sector. Coles-Kemp's research on the wider social dimensions to security practice has been adopted by the NCSC. It has been central to the organisation, changing the way they design security policies and controls to include with the people who use it. This has led to a significant step-change in its objectives and methods used when engaging with stakeholders resulting in wider participation in cyber security practices and the recognition of a more diverse range of cyber security issues.

This step change was first signalled in the NCSC's keynote speech at the leading industry conference, CyberUK, in March 2017 (E.5.1)**.** In 2019, NCSC published guidance, **You Shape Security** (E.5.2, E.5.5), which emphasises the need for wider engagement practices using approaches such as creative securities to build trust between people and security practitioners. Engagement with the You Shape Security guidance has been extensive, receiving 5,500 unique page views, and a recommendation as a resource by the Centre for the Protection of National Infrastructure (CPNI) (E.5.4). NCSC has used this guidance and Coles-Kemp's **Creative Security engagement toolkit (**E.5.2, E.5.5**)** to engage private and public organisations and the wider cyber security community and promoted this approach across its client base. The benefits of this people-centred approach are described by a NCSC client as: "*new trust and communication channels between our employees and the security practitioners in understanding day-to-day frustrations and barriers to good behaviours and in wanting to develop practical, usable solutions that fit with [our] operations and culture*." General Manager, Cyber Resilience, AXELOS (E.5.7).

NCSC has adopted Coles-Kemp's creative security methods to deliver parts of its sociotechnical events programme. Examples include the use of creative security methods to run workshops at CyberUK, a security industry conference that attracts approximately 8,000 delegates each year (E.5.5). In 2016 her creative methods were used in a CyberUK workshop to encourage people-centred approaches among cyber security practitioners, and their feedback helped NCSC to position the You Shape Security guidance. In 2017, NCSC used Coles-Kemp's toolkit in a CyberUK workshop where circa 50 security practitioners used creative engagements to describe and explore their career paths into cyber security (E.5.5). The approach was also used to

encourage more girls to consider computing and cyber security as a career. The technical architect of the CyberFirst Girls competition for Year 8 girls applied Coles-Kemp's thinking, reaching more than 4,000 girls in 2018 (E.5.5).

Coles-Kemp's research has also influenced **security practitioners in Melbourne, Australia** who are part of The Security, Influence and Trust Group – a Melbourne-based security practitioner organisation. The group has placed Coles-Kemp's people-centred approach at the core of its programme since its inception in 2016. "*This relationship helps to ensure our communities continue to benefit from new methodologies to solve complex cyber security challenges."* Co-Founder Security, Influence and Trust group, Australia *(*E.5.6*).*

Creating digital security resilience within marginalised communities and young people:

Coles-Kemp's collaborative research with third sector and educational organisations has shaped understandings of digital security issues leading to process, practice and policy change.

Marginalised communities: Coles-Kemp's research in Sunderland between 2013 and 2016 led community groups (Pallion Action Group, Parker Trust and the Jubilee Centre) to identifying the security issues that affect them. This enabled community workers to develop support programmes that engaged a wider community in digital security issues. For example, digital welfare research conducted with Pallion Action Group enabled community workers to plan for changes to the welfare system (E.5.8). The Director of Parker Trust and Manager of Pallion Action Group explains the research has (E.5.8): "*given us a sense of the challenges that our community is likely to experience as a result of the services going on-line and this enabled us to plan ahead and put the necessary support in place."* Coles-Kemp's research was also used by Pallion Action Group to set-up a support group for families separated by prison.

Between 2018 and 2020, Coles-Kemp extended this mode of engagement to work with hard-to-reach groups in Hull to support the establishment of practical programmes for safer digital inclusion. She then used the same approach with two schools in Southern Sweden that specialised in supporting refugees to re-settle in Sweden in order to help the schools develop safer digital inclusion programmes.

Young People: Coles-Kemp's research has been adopted by those working with young people to address issues of digital safety and develop a pupil-centered e-safety programmes. For example, a secondary school in Oxfordshire used Coles-Kemp's participatory approach to establish a pupil committee that works together with staff and senior management to develop and implement school e-safety policies. The research has led to a transformation of the school's e-safety programme and practice, leading to more controlled mobile phone and social media use, the reduction of pupil stress-levels and a programme of collaborative engagement with parents and pupils (E.5.9).

Safer Digital Inclusion in a Post-COVID Society

In the build-up to the UK's COVID lockdown in March 2020, Coles-Kemp's expertise was sought after to inform programmes orientated towards community digital service delivery. As part of her work as Co-Investigator on the EPSRC-funded Network+ Not-Equal, Coles-Kemp worked with other members of Not-Equal to consult with 20 non-academic partners, predominantly from the Third Sector, to find out what challenges they faced in their work to support communities (E.5.3). This consultation enabled Coles-Kemp to understand the pressures and challenges of safely using digital technologies during COVID lockdowns. This informed the community research that Coles-Kemp undertook during the latter half of 2020, including a consultation on digital identity commissioned by DCMS.

DCMS used this report to inform its digital identity programme. The need to focus on safer digital inclusion has become even more apparent in the shift to digital delivery and engagement necessitated by the COVID pandemic and, as a result, the consultation report has been of use to

a number of other government departments and agencies, including the Ministry of Justice, Office for National Statistics and NCSC. The work was described by Matt Warman, the Minister for Digital Infrastructure, as "*vital research on digital identity and inclusion that will inform our policy development going forward, ensuring everyone who wants a digital identity can have one.*" (E.5.10)

5. Sources to corroborate the impact

[E.5.1]: People-centered security webpages and transcript: https://www.ncsc.gov.uk/speech/peopl the-strongest-link

[E.5.2]: You Shape Security guidance with reference to creative security webpages: https://www.ncsc.gov.uk/collection/you-shape-security

[E.5.3]: Not-Equal COVID Action Report: https://not-equal.tech/wp-content/uploads/2020/07/Not-Equal_COVID-19_CallToAction_Report.pdf

[E.5.4]: Inclusion of You Shape Security as an approach to security culture change by CPNI: https://www.cpni.gov.uk/insider-risks/security-culture

Testimonials:
[E.5.5]: Head of Research, NCSC (testimonial)

[E.5.6]: Co-founder of the Australian Security, Influence and Trust group (testimonial)

[E.5.7]: General Manager, Cyber Resilience, AXELOS (testimonial)

[E.5.8]: Manager of Pallion Action Group and Director of Parker Trust (testimonial)

[E.5.9]: Head teacher, school in Oxfordshire (testimonial)

[E.5.10]: Department for Digital, Culture, Media & Sport (testimonial)