COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 41–48
DOI: 10.17645/pag.v6i2.1333

Article

Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen

Lizzie Coles-Kemp [1,*], Debi Ashenden [2] and Kieron O'Hara [3]

[1] Information Security Group, Royal Holloway University of London, Egham, TW20 0EX, UK;
E-Mail: lizzie.coles-kemp@rhul.ac.uk
[2] School of Computing, University of Portsmouth, Portsmouth, PO1 2UP, UK; E-Mail: debi.ashenden@port.ac.uk
[3] Electronics & Computer Science, University of Southampton, Southampton, SO17 1BJ, UK; E-Mail: kmo@ecs.soton.ac.uk

* Corresponding author

Submitted: 30 December 2017 | Accepted: 7 March 2018 | Published: 11 June 2018

Abstract
Assumptions are made by government and technology providers about the power relationships that shape the use of technological security controls and the norms under which technology usage occurs. We present a case study carried out in the North East of England that examined how a community might work together using a digital information sharing platform to respond to the pressures of welfare policy change. We describe an inductive consideration of this highly local case study before reviewing it in the light of broader security theory. By taking this approach we problematise the tendency of the state to focus on the security of technology at the expense of the security of the citizen. From insights gained from the case study and the subsequent literature review, we conclude that there are three main absences not addressed by the current designs of cybersecurity architectures. These are absences of: consensus as to whose security is being addressed, evidence of equivalence between the mechanisms that control behaviour, and two-way legibility. We argue that by addressing these absences the foundations of trust and collaboration can be built which are necessary for effective cybersecurity. Our consideration of the case study within the context of sovereignty indicates that the design of the cybersecurity architecture and its concomitant service design has a significant bearing on the social contract between citizen and state. By taking this novel perspective new directions emerge for the understanding of the effectiveness of cybersecurity technologies.

Keywords
cybersecurity; cyberspace; power; social contract; sovereignty

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

Assumptions are made by government and technology providers about the power relationships that shape the use of technological security controls, and about the norms under which technology usage occurs. These assumptions are coloured by notions of sovereignty and the importance of not only protecting boundaries (including national borders) in whatever space they manifest themselves (digital or otherwise) but also in demonstrating the exclusive control that legitimizes the existence and the authority of the state. In this article, we present a case study that examined how a community might work together using a digital information sharing platform to respond to the pressures of welfare policy change. Insights gained from this case study cast light on the relationships between the security of the digital infrastructure and the security of the people using that infrastructure *as they perceive it*. Contrary to the typical start point for the security of such a platform, which might best be described as controls to protect the data and the technologies, the community start point was to build networks of trust and collaboration into which the digital sharing technologies could be productively deployed. Our conclusions are that whereas theories of security focus on the relationships between the political, the social, the economic and the technological, the application of cybersecurity controls is often focused on the technical or physical protection of the digital infrastructure, thereby missing the social part of the sociotechnical security system.

The case study leads us to question the sufficiency of the security focus on the protection of the data and the digital technologies, turning to security theory, stemming from Hobbes and also the work of Mark Neocleous (2008), for possible explanations of the apparent gap between the state's use of cybersecurity technologies and the security needs of citizens. Cybersecurity research focuses primarily on the "cyber" part of "cybersecurity", with the unfortunate consequence that the security concerns of the citizen are literally invisible to it. We argue that by locating cybersecurity issues within a broader security literature that takes into account the need to respond to human *insecurities*, new directions emerge for the understanding of the effectiveness of cybersecurity technologies. When, on the other hand, we neglect the citizen-centric view, the security implications of digital service delivery are obscured.

From the case study insights and the subsequent literature review, we conclude that there are three main absences not addressed by the current designs of cybersecurity architectures. We argue that by addressing these absences, the foundations of trust and collaboration can be built which are necessary for effective cybersecurity:

- *Lack of consensus as to whose security is being addressed:* in order for security to work to the public benefit, it is apparent that citizens need to feel secure as a result of its operation. If they do not, then they take security into their own hands, which might increase their local security at the cost of undermining their ability to cooperate with outsiders. Therefore, concentrating on the security and well-being of its citizens is also for the benefit of the state;
- *Lack of evidence of equivalence between the mechanisms that control behaviour:* we argue that when designing a digital service, a control is not independent of the medium used to implement it and a change in medium changes some of the qualities of the control, leading to changes in its effectiveness. For example, when we replace socially-based controls with technology we lose a whole layer of communicative structures when certain options are simply "greyed out" online;
- *One-way legibility:* the state has a need to make the citizen readable by its standardised processes (Scott, 1998) but no corresponding imperative to make itself or its systems legible to the citizen. However, it is apparent that this lack of legibility makes the citizen feel insecure—particularly when the citizen feels that the state views it as the threat.

We first present an inductive consideration of a highly local case study. Whilst such a case study does not of course allow us to generalise the findings, it does compel us to problematise the focus on the security of the technology at the expense of the security of the citizen. We will then consider the contribution that theorising about social, economic and political security can make to the design of cybersecurity technologies.

2. A Community Information Sharing Platform: A Case Study

Our case study took place in the North East of England, in a community suffering the effects of long-term unemployment and degrading social, physical and political infrastructure. Researchers and an arts organisation, Proboscis, worked together to support a community group in the design of an information sharing system that would help their community respond to challenges associated with welfare change.

The community group wanted to develop a system of information sharing that used digital technologies to enhance their capabilities to respond to welfare system changes and provide community support for job seeking, debt management, housing and tenancy advice and benefit claiming. The research team wanted to observe how such a community might design this type of information sharing system as a means to better understand individual and community securities. The research centred on two questions: (i) Which everyday issues become most pressing due to changes in welfare rules and the move to digital welfare delivery? (ii) How might communities work together to alleviate those pressures?

When designing the case study, researchers wanted to develop an empowering space in which participants could reflect on and design for the types of support that would help them and where the interactions between the research team and participants were transparent. Accordingly, the research design was grounded in participatory design principles (e.g. Coles-Kemp & Ashenden, 2012; Vines, Clarke, Wright, McCarthy, & Olivier, 2013) that encouraged participants to co-design the research questions, to influence the design of the data gathering methods and to actively reflect on and contribute to the presentation of the research findings. Following the community participatory engagement principles set out by Coles-Kemp and Ashenden (2012), the research took place in a community centre which was a familiar space for the participants, the research focus was shaped in partnership with the participants, the data gathering methods were adapted to fit with the participant groups and, to nurture a sense of empowerment and agency, participants were encouraged to consider community responses to the issues identified. Such an anthropologically informed design approach is particularly appropriate for design projects that produce outputs that are to be embedded and sustained within community practices. The case study acted as a provocation for us as researchers by encouraging us to think about security theory in relation to the use of technological cybersecurity controls.

Five focus groups were carried out each with between 4 and 8 participants. In the initial group, the participants were asked to articulate the range of economic, emotional and administrative pressures that they experienced as part of everyday life. Such pressures shed light on the conditions under which interaction with state services might occur and the challenges such pressures present for conformant use of digital state services. In line with participatory design philosophy, the research method used in this initial session was a simple storytelling method which encouraged participants to describe the pressures experienced in different scenarios. The second focus group further deepened the researchers' understanding of these pressures using story telling together with an icon-library to help participants build up a visual and lexical vocabulary of pressures and their responses. For the third focus group, story sheets were developed that were used to systematically capture the pressures, the needs for information sharing and possible community responses. This enabled a wider, more systematic gathering of the issues and ideas for potential community responses and support. The fourth and fifth focus groups used a refined version of this story gathering process until the principles for community support had been developed. The focus groups were recorded, transcripts produced and analysed using thematic analysis before the results were then presented to the wider community for consultation.

2.1. Results and Discussion

The strongest theme to emerge from the data analysis was that of citizen insecurity and precarity. The data illustrated the ways in which the interactions with the welfare systems generated feelings of insecurity for the individual. For example, participants felt that they were not able to question or negotiate with the system and yet experienced heavy penalties for making errors. As one participant pointed out, "If you are underpaid, you don't get it back. If you are overpaid they expect you to pay it back". Participants highlighted that the problems they experienced were due to the complexity of the system and the constant rolling programme of changes. The data from the first focus group showed that participants experienced many such pressures on a day-to-day basis that were exacerbated by the mechanisms used to interact with the system. At the same time, finding ways to work outside the system was also difficult. As another participant commented, "The self-help route is fraught with problems". This insight led us to reflect on how interaction with systems connects to an individual's feelings of security and insecurity that operate at a deeper level than is assumed by the presence (or absence) of technical security controls.

Analysis of the transcripts from the first and second focus groups demonstrated how technology is conceptualised as being interwoven with human social networks and does not operate as a replacement for them. This socio-technological enmeshing connects security technologies to the human networks in which they operate, such that as one participant commented, "It was better when you could see someone face to face. It was better when you could phone for an appointment". Not only was technology not seen as a viable alternative for human interaction, these focus groups highlighted that human networks help to overcome the fear of engaging, as one participant confessed that when reporting to a change in status it, "took me nearly 18 months to phone the Council". This led us to think about in what ways the design of a system that operates within human social networks might increase trust and confidence in working with that system.

Analysis of the data from the first two focus groups shows that receiving understandable information about welfare changes from trusted sources was an important means of reducing anxieties, thereby increasing the feeling of security. For these participants, the information you share and how you use it depends on your values and morals as well as your individual circumstances. As one participant said, "it's a lot to do with your priorities". This is an element that digital service design fails to make allowances for—individuals have different priorities in their lives and therefore have different positions on what constitutes security. One participant in the third focus group told the following story of how she had recently lost her job: "The senior that was on, didn't like us because she was me ex's wife. She hated us and grassed us up for everything. But I should have grassed her up first because she was drinking on the job….But you cannot do that". This story highlights that values and morals shape what information is shared, and how it is used. Yet digital services assume an "idealised", "abstract" or "model" individual interacting with systems and such abstractions often lack ecological validity—a "cultural disconnect" in which system designers illegitimately assume that system users share similar characteristics to a dominant social type, able, for example, to manage passwords, absorb complex instructions and adapt easily to change (King & Crewe, 2013). In such models attitudes and behaviours appear predictable and the state assumes that it understands, and can make sense of, its citizens. This insight led us to think about the importance of different types of legibility and how the design of systems needs to be able to adjust to different patterns of information sharing and protection.

2.2. Trust Rather Than Protection: A New Start Point for Security Design

Whilst a Government cybersecurity response is more likely to encompass access control and surveillance, this case study indicates that a community approach is more likely to focus on trust points, crowdsourced trust recommendations and the collaborative use of the community's own resources to dispel abusive behaviour. This understanding of how communities work might well be possessed by those tasked with local delivery of systems, but is typically lacking in the higher echelons of policymakers and system designers, a phenomenon which has been called "operational disconnect" (King & Crewe, 2013).

The types of trust discussed during the study were many and varied, including trust in the quality of the information, trust in the individuals providing the information, trust that the information exchange will help their circumstances and trust that personal details would be kept private. The participants showed that trust in the quality of the information can be engendered through knowledge champions who are seen as having specialist knowledge and are validated through recommendations, through their jobs in related areas, as well as through their track record in providing specialist advice. Trust in the quality of information was further engendered by peer review of information shared within the community.

In the later focus groups, concern for the security and safety of community members who were information providers emerged as a dominant theme. These concerns included liability if the information turned out to be incorrect and concerns for the safety of the provider if they gave information that involved local intelligence about community activities. Of particular concern was information shared about loan sharks and unhelpful or abusive staff who provided state or state-endorsed support. A further concern was the potential for individuals to use the information that was provided to them to defraud the state or other institutions. The third, fourth and fifth focus groups focused on ideas of information sharing to better support each other in responding to the pressures articulated. During this process, several key security concerns were identified: trust in the quality of the information, the safety of the information providers and the potential for manipulation or abuse of the information provided.

These security concerns focus on the close proximal relationships in everyday life. These concerns contrast sharply with the more conventional cybersecurity systems' protection approach that focuses on attackers misusing the system. It suggests an approach to protect citizens who suffer as a result of the lack of information, the flow of false information, the misrouting of information by those who want to abuse the network and the pressures inherent within the context of use. To address these latter concerns, the start point is trust and collaboration rather than a control architecture to protect against attackers and malicious activities.

Our case study insights led us to conclude that a community approach to security might focus on trust points, crowdsourced trust recommendations and the use of the community's own resources to dispel abusive behaviour. From our analysis of focus group data and a comparison of the community response with the typical state approaches to technological control, we focused our attention on the theoretical underpinnings of a security design that speaks to the three absences of security consensus, control equivalence and two-way legibility that we identified above. We conclude that such principles have the potential to encourage a collective notion of cybersecurity and engender positive buy-in and active engagement from citizens, facilitating a genuinely sociotechnical cybersecurity system. We conclude that in the digital by default era, trust between state and citizen is in large part built by developing a cybersecurity model that can (i) adjust to the security needs of the citizen, (ii) that provides a more comprehensive range of security qualities and (iii) is legible to the citizen. We explore these three principles below.

3. The First Absence: The Security of the Citizen

The insights from the case study reflect that security requirements are often conflicting, culturally and morally constructed and both individualistic and communal. To explore how a cybersecurity model might better reflect this, we need to look at the roots of modern conceptualisations of sovereignty. The modern security community theorises sovereignty of cyberspace along the lines of the pioneering conceptualisation of Thomas Hobbes (1588–1679), which still underpins both liberal and conservative theorising of the nature of the state. In particular, Hobbes suggested that sovereignty, to be effective and legitimate, needed to take a particular form, and fulfil particular functions: it was contractual, and co-constructed with (though not co-constituted by) the citizens. People would rationally seek wider protection than they could provide for themselves by surrendering their rights of self-protection to a more powerful sovereign which could protect a community from outsiders and the members of the community from each other, therefore promoting cooperation, trust and other forms of social behaviour. It follows that, if people feel unprotected by the state, then it is reasonable and rational for them to seek protection elsewhere. "The end of obedience is protection" (Hobbes, 1996, p. 152), and therefore if obedience to the state does not give you protection, (i) protection needs to be found elsewhere, and (ii) the duty of obedience evaporates.

We argue that as the state withdraws from in-person contact to digitally-mediated interaction and as digital technology facilitates the types of communication and collaboration that can make possible the diversification of wealth production and gives citizens the option to move between modes of wealth production and social orders, the security relationship between the citizen and the state needs to be re-negotiated. Such re-negotiation is necessary in the first place because the assets that citizens wish to be secured may not be the same as those identified by the state (or large organisations). Secondly, citizens may value particular types of behaviour or interaction which may be hindered or even prevented by security measures, and which may therefore prompt the use of workarounds which undermine those measures even in their own terms. Because of the co-constructed nature of Hobbesian sovereignty, these are serious problems, because citizens' acceptance of the legitimacy of the sovereign (i.e. in the modern world, the state) depends crucially on their own perceptions that it serves their security needs. It follows that if the sovereign opts to define the types of security it will provide on the winner-takes-all model, it must either persuade citizens that these are the types of security they value, or sacrifice legitimacy. If it fails to engage with the citizenry upon matters of security, then it has to expect the citizenry to have an antagonistic attitude, resulting in the only option being to rule by force, treating its own citizens as the enemy. The insights from the case study indicate that an alternative means of overcoming this potential for antagonistic outcome is to situate Digital by Default (DBD) services within existing networks and embed the services through a more robust security control equivalence and through system legibility, thus both increasing trust and creating spaces in which conflicts and differences can be resolved.

4. The Second Absence: Equivalent Methods of Control

The case study data indicate many frustrations with the control mechanisms deployed in the various state systems. For the citizenry to align with the state's model of security, the controls have to afford security to the citizen. Yeung (2011) talks about the bond of trust between the state and the community it governs pointing out that, "small erosions may lead to its long-term degradation" (p. 25). One of the reasons that trust may erode is that the principles of control and the related principles of security remain the same but the mechanisms for operationalising them differ. Digital controls do not necessarily carry the same signals of trustworthiness, legitimacy, openness to negotiation, and ability to reconcile different interpretations of security within a single transaction as socially-grounded forms of the same control principle.

Lessig's (1999) socioeconomic theory of behaviour constraint argues that regulation (in the widest sense) can happen through four mechanisms—the law, social norms, economic incentives and architecture. Taking this view, digital technology and sovereignty have been game-changers for the state. Previously, the state had monopoly control only over the law, and so that was its main interface for citizen control. Now, it can alter the *architecture* of its interactions with the citizen in order to make certain behaviours more likely while ruling others out (and it can also gather the data to evaluate and refine its strategies in real time). It follows that it can achieve its goals stealthily by adjusting the architecture of interaction, rather than by commanding and punishing; this is the basis of 'nudge' philosophy (Thaler & Sunstein, 2008).

This theory has much plausibility, but it has intentionally or otherwise led to the fallacious corollary, that, because control can be exercised through any one of these four mechanisms, the mechanisms are *interchangeable* for a given piece of control (Hildebrandt, 2015). In other words, if some type of behaviour is prevented through, say, a legal restriction, the control mechanism can be changed to, say, a constraint on the digital architecture, while leaving everything else untouched. Indeed, one of the myths underpinning the DBD strategy for citizen-state interaction is that the easiest way to do this is through techno-regulation which Yeung defines as a reliance on embedding regulation in technology design rather than relying on the law to regulate. Yet this is fallacious for two reasons that are relevant to our own inquiry.

First, the four mechanisms have very different properties. Techno-regulation uses the architecture of systems to enforce control. Yeung (2011) suggests that, "it is the action-forcing character of techno-regulation that makes it a particularly powerful form of control" (p. 4) and goes on to make the point that this way of regulating human activity in cyberspace has negative "implications for liberty, autonomy and responsibility". Compare the use of law to constrain behaviour with the use of architecture. Law has three properties that digital architecture does not have. Firstly, one can disobey the law. There are consequences if one does, but one can (and people often do). This is an important source of freedom—consider civil disobedience—which is not replicated by a technical architecture. Secondly, law can be challenged within the law; one can take one's case to higher courts. Architecture does not admit legitimate challenge (although it can be illegitimately hacked). Thirdly, law needs a certain legitimacy to operate—it is at least in part created, in a democracy, by a legislature that can be voted out by the citizens it binds. Software (even open source), on the other hand, is created by small expert cliques accountable to no-one but themselves. Economic incentives can also be subsumed by the architecture of a digital system. In our case study, participants gave examples of how failure to engage with the system on its own terms resulted in financial punishment by being underpaid or overpaid and then expected to pay it back.

The case study indicates that citizens can choose not to engage with these incentives and may well prefer informal economic activities that are outside the control of the state and bypass the digital system. Some of the social norms that sit around these informal economic activities emerge from our focus group community. Not only does each of these constraint mechanisms have different properties but the state is more likely to focus on hard controls such as the law, architecture of the system and economic incentives rather than attempt to tackle social norms and yet this mechanism emerged from the case study as the most important factor in developing trust and security through protection of the community and its members. In other words, when we switch focus from the security of digital or financial assets to the kinds of security that matter to the citizen, we see that the hard constraints are more likely to produce insecurity than security, and consequently that the ideal of a co-constructed sociotechnical security architecture in this context fractures into a set of government controls designed to counter community resistance.

The second reason is that the nature of the constraints in question is more complex than Lessig's simple picture suggests. Perhaps most importantly, pre-DBD, the citizen might have spent time talking to a representative of the state who almost unconsciously performed the vital communicative function of explaining the assumed responsibilities of the citizen. This is a very rich interaction of the citizen with not only a monolithic state, but its human representatives and also various other actors in the same society. The digital architecture wishes most of this away, and replaces it with an input/output function where the claimant identifies himself in terms meaningless to him, but that the state recognises (e.g. a biometric or a password), and then transfers resources once it has verified entitlement. No conversation, explanation or human interaction is needed from the architecture's point of view. This is not merely a change in interaction style but a removal of fundamental and necessary qualities of security control. By contrast, the case study reflects the importance of communication, interaction and the negotiation of responsibilities that are preconditions to the successful operation of a system.

5. The Third Absence: Legibility of the State to the Citizen

The illegibility of the state systems appears as a clear source of mistrust for our focus group participants. The technologies of cybersecurity are built on a particular type of mathematical abstraction away from the everyday, "embodied situated experience" (Cohen, 2007, p. 213) of individuals, reducing visibility of the fluidity that digital technologies both enable and encourage (Bauman, 2013). However, reducing its visibility does not remove it. Scott (1998) has described the processes by which the state reduces complexity, by rendering its citizens and their lifeworlds legible to administrative order. This goes against typical living practices that are legible for citizens, that are local, interested, contextual and historically specific (Scott, 1998) and that make sense in the particular circumstances of citizens' lives. For the state to intervene effectively, either to appropriate resources, to control behaviour, or to manipulate behaviour, it has to abstract away from all these factors to produce national, homogeneous, uniform standards. State simplification produces descriptions of communities that are usually: (i) related only to the state's interests (in taxing, providing services, providing security, etc.), (ii) written facts, numerical or verbal, (iii) static facts, snapshots rather than ongoing processes, (iv) aggregate facts about groups and averages, rather than about individuals per se, and (v) standardised, based on categories that bracket citizens together, no matter how unique their circumstances (Scott, 1998).

In the end, such an understanding engenders incentives for people to abridge their own practice in order to be legible by the state—for instance, an unemployed person on welfare might be better off working casually in the informal economy, but the state recognises only the possibility of formal employment or enforced idleness. Its rules are crafted on this assumption, giving the welfare claimant the choice of forfeiting payments or foregoing informal work. If she forfeits her welfare entitlement, the social safety net is removed from under her, but if she claims welfare and foregoes informal employment she is unable to use her contacts and local knowledge (her social capital) to help support her and her dependents, and work that would benefit the local community is left undone. The state, with its imperative to abstract and simplify, ends up with individuals simplifying their own behaviour deliberately to become legible to the state.

Note also that some commitment to transparency (e.g. the provision of open data) may be necessary for legibility, but cannot be sufficient. Government transparency can only help when what is revealed to citizens is legible to them. A data set in the Resource Description Framework from data.gov.uk will not in itself accomplish this. As our case study insights indicate, rich engagement, and a willingness to discuss and explain, will be of far greater value.

6. Discussion and Conclusion

Sovereignty is the ability of a state to maintain the exclusive power and authority to govern itself, for example by maintaining control of, and managing, citizens within, its borders. Neocleous (2008) argues that social security is an important aspect of this imperative for the state. An effective cybersecurity deployment is essential if the state is to maintain its exclusive authority and a secure DBD policy further bolsters this. Franzese (2009) suggests that sovereignty in cyberspace depends on a state receiving external recognition of its authority and ability to, "exert some measure of control over its own cyberspace" (p. 9), and such authority is under heavy challenge at the time of writing. In the UK, the importance of such recognition to the establishment of sovereignty is encapsulated in the Government aspiration to make the UK the safest place to do business online (UK Government, 2016). Achieving this aim establishes sovereignty in two ways, firstly, through other countries and global businesses engaging in online business with the UK thereby demonstrating their confidence in the control UK Government has over its cyberspace and secondly, through delivering secure Government services to its citizens, again demonstrating that the Government has the ability to manage its citizens in cyberspace.

Sovereign capability in cyberspace is complex and contested and the projection of sovereignty is demonstrated, at least in part, through state activities around cybersecurity. As Lessig (1999) points out, "real-space sovereigns" (p. 198) will respond to the threat of cyberspace by attempting to ensure that their regulatory power encompasses virtual spaces, and, by framing cyberspace as a spatial domain analogous to land, sea and air (Murphy, 2010), will conceptualise the control and management of cyberspace through cybersecurity. This Westphalian model is traditionally framed as being threatened by hacking causing the disruption of democratic processes by foreign powers, and by attempts to copy or take control of data assets of UK businesses and individuals. However, our case study gives us cause to reflect that civil disobedience stemming from the undermining of the social contract between citizen and state is also a potential significant threat to domestic sovereignty. In the era of DBD, civil disobedience can result in non-compliance with cybersecurity controls and rejection of social policies and programmes as the citizen feels forced to focus on their own security at the expense of making positive and creative contributions to the state.

Neocleous (2008) makes a powerful argument for social security to be considered an integral part of a nation's security policy as its function is the maintenance of social and economic order. If considered from this perspective, cybersecurity technologies of passwords, file permissions, encryption and firewalls are digital means of fulfilling this mission of order and containment. These security technologies are core to DBD and embody a particular security philosophy. The case study participants, however, focus on a different security mission, of mutual support and information sharing. This mission addresses the challenges of human insecurities rather than the frailties of a system of order and rendering legible. These security missions are not mutually exclusive, but each responds to a different type of insecurity.

In the context of Neocleous' argument about domestic containment (2008), DBD makes cyberspace central to the question of domestic sovereignty and this makes cybersecurity and its control framework a central part of domestic policy initiatives. The current security model for DBD focuses on the protection of the data and the technology with the assumption that this will also provide security for the citizen. By contrast, our case study shows that the start point for an individual's security is not protection but trust.

Acknowledgements

We'd like to thank the participants who gave their time, creativity and energy to the work of the focus groups. We'd like to thank Proboscis for their support and creative input to the case study. Coles-Kemp's contribution was funded by EPSRC grant ESSfES: Everyday Safety-Security for Everyday Services (grant number EP/N02561X/1). O'Hara's contribution was partially funded by EPSRC grant SOCIAM: The Theory and Practice of Social Machines (grant no. EP/J017728/2).

Conflict of Interests

The authors declare no conflict of interests.

References

Bauman, Z. (2013). *Liquid modernity*. New Jersey, NJ: John Wiley & Sons.

Cohen, J. E. (2007). Cyberspace as/and space. *Columbia Law Review*, *107*, 210–256.

Coles-Kemp, L., & Ashenden, D. (2012). Community-centric engagement: Lessons learned from privacy awareness intervention design. In S. Faily, I. Fléchais, & L. Coles-Kemp (Eds.), *Proceedings of HCI 2012 the 26th BCS conference on human computer interaction* (pp. 1–4). Retrieved from https://ewic.bcs.org/content/ConWebDoc/48813

Franzese, P. W. (2009). Sovereignty in cyberspace: Can it exist? *Air Force Law Review*, *64*, 1–42.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Cheltenham: Edward Elgar Publishing.

Hobbes, T. (1996). *Leviathan*. Cambridge: Cambridge University Press.

King, A., & Crewe, I. (2013). *The blunders of our governments*. London: Oneworld Publications.

Lessig, L. (1999). *Code: And other laws of cyberspace*. New York, NY: Basic Books.

Murphy, M. (2010, July 1). Cyberwar: War in the fifth domain. *Economist*. Retrieved from http://www.economist.com/node/16478792

Neocleous, M. (2008). *Critique of security*. Edinburgh: Edinburgh University Press.

Scott, J. C. (1998). *Seeing like a State: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.

Thaler, R. H., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New York, NY: Penguin.

UK Government. (2016). *UK National cyber security strategy 2016–2021*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Vines, J., Clarke, R., Wright, P., McCarthy, J., & Olivier, P. (2013). Configuring participation: On how we involve people in design. In S. Bødker, S. Brewster, P. Baudisch, M. Beaudouin-Lafon, & W. E. Mackay (Eds.), *Proceedings of the SIGCHI ACM conference on human factors in computing systems* (pp. 429–438). Paris: ACM.

Yeung, K., (2011). Can we employ design-based regulation while avoiding brave new world? *Law, Innovation and Technology*, *3*(1), 1–29.

About the Authors

Lizzie Coles-Kemp is Professor of Information Security at Royal Holloway University of London. She is a qualitative researcher who uses creative engagement methods to explore everyday practices of information production, protection, circulation, curation and consumption within and between communities. Lizzie's focus is the intersections between relational security practices and technological security and she specialises in public and community service design and consumption. She is currently an EPSRC research fellow with a research programme in everyday security.

Debi Ashenden is Professor of Cyber Security in the School of Computing at the University of Portsmouth. She is also the Programme Director for Protective Security & Risk at the Centre for Research & Evidence for Security Threats (CREST). Debi's research interests are in the social and behavioural aspects of cyber security—particularly in finding ways of "patching with people" rather than technology. She focuses on building security dialogues between communities.

Kieron O'Hara is an associate professor in electronics and computer science at the University of Southampton, and visiting professor in law at the University of Winchester. His interests are the political implications of technology, particularly the World Wide Web, AI and big data, with a focus on privacy, trust, openness and ethics. His book *The Anonymisation Decision-Making Framework* (co-written with Mark Elliot, Elaine Mackey and Caroline Tudor) is a practical guide to data anonymisation.