Inclusive Security: Digital Security Meets Web Science

Lizzie Coles-Kemp[1]

[1] *Information Security Group, Royal Holloway University of London*

ABSTRACT

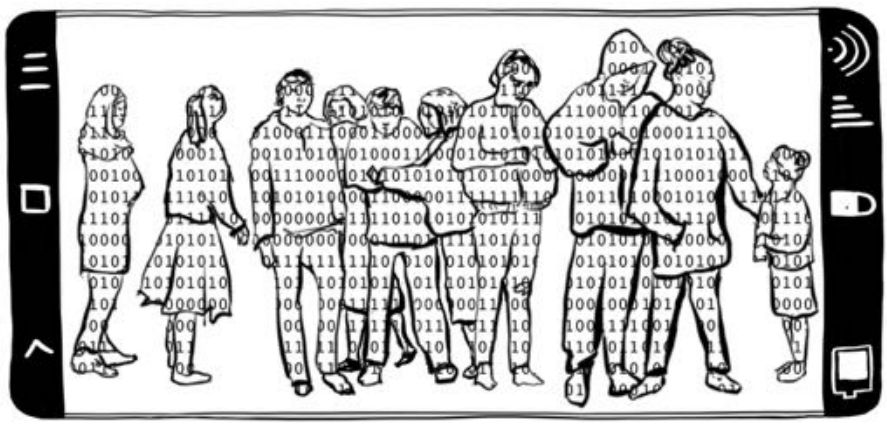
The rationale for designing, implementing and managing security technologies has a notion of "risk" at its core; the risk of compromise to technology or information weighed up against the cost of protecting against such an incursion. However, such approaches have been focused on the protection of technology and information, with the assumption that if this is protected then people are also protected; an assumption that is much harder to maintain in a more open, networked context such as the one that has been enabled by growth of the World Wide Web. Grounded in the interdisciplinary endeavours that characterise Web Science, this monograph presents the case for a more inclusive form of technological security. Such a security places the security of technology in the context of the security of people operating in a web-enabled and digitally-connected society and results in a digital security that responds to the enmeshed nature of technology and society. This monograph uses a wide analytical lens that encompasses the sociotechnical infrastructures, networks of power and the practices that shape our interactions with and through digital technologies to explore this more expansive form of security.

Lizzie Coles-Kemp (2020), "Inclusive Security: Digital Security Meets Web Science", Foundations and Trends® in Web Science: Vol. 7, No. 2, pp 88–241. DOI: 10.1561/1800000030.

The version of record is available at: http://dx.doi.org/10.1561/1800000030

1

Introduction



Digital technologies are woven across our everyday lives

As we become increasingly dependent on digital products in all aspects of our lives, the reliability of that technology increases in importance. Technological security mechanisms, such as passwords and data encryption, are a key way to ensure reliability in the technological delivery by ensuring that the technology performs as expected. Technological security can be thought of as the control of access to technical systems and the control of the use of those systems.

However, the way that digital technologies are woven across the fabric of our everyday lives, and are embedded in all our institutions, means that we need a paradigm for understanding technological security as being part of other forms of security. This monograph introduces the paradigm of digital security that not only encompasses the protection of digital technologies and the data it produces, but also the practices and processes that link those technologies. It also encompasses the political and social processes and practices that shape the meanings, and experiences of the digital protection mechanisms. In a digitally mediated society, security of the state, of society, of individuals and of technologies are bound together through these processes and practices, giving new security meanings to security technologies and policies.

The political dimensions of security technologies are addressed in cybersecurity scholarship. The study of cybersecurity examines technological security as it intersects with national or global interests (Carr and Lesniewska, 2020). Cybersecurity is primarily understood from the perspective of the state (Carr, 2016; Stevens, 2013), global human rights (Carr, 2013; Deibert, 2018) and global governance (Carr, 2015). There is also an acknowledgement that security has a moral force (Nissenbaum, 2005) and that security technology is political, but there have been few studies that examine how people respond to cybersecurity programmes and to the use of security technologies to regulate everyday transactions and practices. Therefore, the term *"digital security"* is introduced in this monograph to reference the security issues and responses that emerge at the intersections between technological security and other forms of security, from the perspective of a person's everyday lived experience. Digital security connects technological security with social and political issues that shape a person's everyday security and examines technological security in terms of the social impacts that it has. Digital security is an inherently interdisciplinary study and practice that focuses on technologies that predominantly rely on access to the World Wide Web. This makes it a type of interdisciplinary study that falls under the remit of Web Science.

Whilst the connection between technological security and social and political forms of security in people's everyday lives has been made in reference to particular groups of technology users (Parkin *et al.*,

2019; Strohmayer *et al.*, 2017; Matthews *et al.*, 2017) or in reference to surveillance technologies (Gürses *et al.*, 2016; Huysmans, 2011), the connection is not made in the more mainstream security technology studies or practices. This monograph seeks to address this gap and the work presented shows why this perspective should be routinely included in technological security analysis and design.

1.1 Background Research

This monograph distils a body of research and study that began with the VOME project – Visualisation and Other Methods of Expression (VOME, 2010). This 3-year project started in 2007 and re-examined how people use digital services and why they share what they share on-line. In line with a Web Science research approach (Berners-Lee *et al.*, 2006, p.71), VOME acknowledged from the outset that the securing of digital services and technology is embedded in a social setting. The VOME project took an embodied position: wanting to understand how people felt and experienced security when using digital technologies. VOME's core research question was: *"What does privacy sound, feel and look like?"*. The project examined people's attitudes towards informational privacy in on-line settings, and we discovered that when examined from an embodied perspective, the sharing and protection of personal security on-line is experienced as a means of protecting the individual, and their kin and friendship network. The VOME project therefore strayed from traditional privacy studies, and instead focused on the intersections between different types of security, and the security feelings and responses that emerge at those intersections. From this start point, subsequent projects examined how information sharing and protection practices evoke feelings of security and how these feelings, in turn, shape those practices.

The project committed to working with the creative arts in a humanities tradition, as well as drawing on the more traditional digital privacy and usable security research to explore these embodied dimensions and pursue this line of enquiry. In following an embodied line of enquiry, the research revealed that how security technology was *intended* to feel, look and work like was not the actual experience of many of the

groups that the project worked with. This was because technological security intersects with other forms of security, and these intersections can engender an embodied sense of insecurity as well as security. For example, if someone is financially insecure, then a complex process of accessing financial services can exacerbate that feeling of insecurity, making the access control processes seem hostile.

Technological security sits at the intersection with other forms of security

People are called upon to prove or verify who they are when setting up a financial service account. This is often a process that requires multiple sources of documentation, not always readily available to the individual or that are costly for the individual to provide. This evidence might be requested using language that can be difficult for the individual to follow and the process might result in a negative outcome if not followed precisely as set-out. For those already feeling insecure or lacking in confidence, the identity verification process can be anxiety-inducing, and result in that individual asking for informal help from their kin and friendship network. This help might be constructive but also might increase the vulnerability of the individual.

Similarly, if someone is feeling anxious and uncertain about their

health, remote access to a health system that is complex and impersonal can amplify those feelings of health insecurity. This can lead to either avoidance of the health service or the altering of data submitted to the health system. Both of these information sharing practices can result in increasing the vulnerability of the individual. The anxiety a person experiences with digital health services can be amplified by limited access to digital connectivity and to data. This can result in an individual having to borrow a device from a family member or friend, or can result in an individual having to rely on someone else to upload their records. Both courses of action can increase an individual's anxiety and extend their vulnerabilities to information misuse or denial of access. If healthcare is not free at the point of access, financial worries can also increase the stress of this situation. The research concluded that security technology often felt alienating, confusing and either threatening or useless to many people. Those negative feelings thus shaped how people used such technology and, in particular, the ways in which they shared and protected information.

Taking an embodied position to examine security aspects of human computer interaction was an unusual starting point for research in this area. The more typical position was to examine the topic from an objective, external perspective, using a positivist research paradigm to focus on the security functionality of the digital technology, and the security of the digital interaction.

An embodied position also revealed a wider view of security in digital settings; it revealed that the security practices people undertake in a digital setting are not limited to the interaction with the technology, but are set in the context of wider interactions with people within their kin and friendship networks. For example, Light and Coles-Kemp (2013) showed that in family settings grandmothers with little or no digital expertise can play a significant role in the information sharing and protection practices of their digitally-confident granddaughters. The study with grandmothers and granddaughters challenged the notion that information sharing and protection practices relevant to digital interaction only take place within the interaction itself. The study showed that the information sharing and protection that takes place *around* the digital interaction can have a significant effect on the information

sharing and protection that takes place within the interaction. The study also showed that working through a social proxy (somebody who carries out information sharing and protection actions on behalf of another person) can engender feelings of confidence in information sharing and protection practices, as well as encourage critical reflection on those practices within the digital interaction itself.

In the finance, health and family examples above, the traditional focus on the security design of the technology, and the focus on the information sharing and protection within the digital interaction, have meant that exploring the significance of what happens in the space around the digital interaction has been ignored. At the same time, the traditional approach has also not taken into account the ways in which technological security intersects with other forms of security, and how an individual responds to those intersections. Finally, the traditional approach has not examined how the political, social and economic context in which people use technologies shapes the meanings of technological controls. As a result, opportunities for security interventions in those wider spaces have been lost, and the conditions for effective use of technological security have not been created. Based on our research, we argue that studying the information sharing and protection practices in the space around the digital interaction, brings to the fore the political, social and economic meanings of technological controls. We also argue that the embodied position from which these practices emerge must also be understood if technological security controls are to be effective and the value of the expertise in creating such technologies is to be realised.

The VOME research therefore identified a number of blind spots within the traditional ways that we understand technological security:

- Security issues in digitally-mediated interactions are not considered from the perspective of those using the technologies. Instead they are typically considered from the perspective of the experts designing and implementing the relevant technologies and consequently often address issues that are only partially relevant to the users of those technologies.

- Security practices are not understood in the wider context of the social, political and economic complexities within which the interactions take place. Consequently, practices are dismissed as non-compliant when they are, in fact, responding to a different security imperative.

- The potential for technologies and services to harm their users, both intentionally and unintentionally, is not considered as part of the security analysis of a digital product, and yet the potential for harm shapes people's digital practices and experiences.

The research further shone a light on the importance of understanding how technological security intersects with other forms of security, and the responses that emerge at those intersections. VOME research yielded three core insights that illuminate these intersections:

- Assessing risk to digitally-mediated networked interactions requires both the assessment of risks to technology, and of the risks networked technology use pose to the users of that technology;

- The understanding of technological risk needs to be set in the context of the wider concerns that networked technology users are experiencing;

- People often focus on the benefits that they gain from using a technology or service, and consider the technological security risks in relation to that benefit.

The VOME research showed that it is important to understand technological security both in relation to the protection of technology and of people so that we can better understand where:

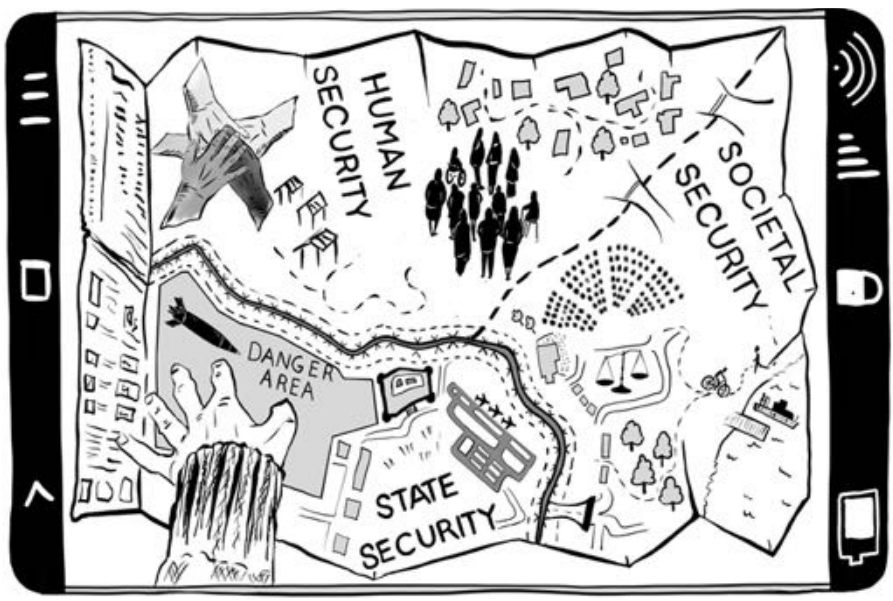
- Security technologies create threats to human computer interaction; and

- Interventions and responses might be made in the spaces around the human computer interaction.

The research has been recognised by the UK's Cyber Security Body of Knowledge (CyBOK, 2019a) as a new area in Cybersecurity Human Factors (CyBOK, 2019b). The practice has also been recognised as part of the UK's National Cyber Security Centre guidance on people-centred security (NCSC, 2019). The guidance titled *You Shape Security* is primarily written for security practitioners: from those who design approaches to technological security within organisations, to those who deploy and manage those approaches.

1.2 Adoption and Development

Following on from VOME, five further projects formed a programme of work grounded on the following position: *for technological security to be effective, a broader digital security must be designed that supports people to both realise the benefits of a digital service and to realise those benefits safely.*



Mapping out a broader digital security

The programme of work has focused on the following research aspirations:

- *Alternative paradigms of technological security*: using the social and political theories of security for inspiration, alternative paradigms for technological security have been investigated and developed.
- *Participatory design and practice for technological security*: using the principles of participatory design and arts-based research practice, methods that generate a wider lens for understanding people-centrred security have been developed and practiced.
- *Inclusion as a form of security*: drawing on thinking and practices related to a conceptualisation of security as a form of empowerment and enablement (and as a collective rather than individualistic issue), digital security structures and practices have been developed using ideas that focus on trust, resilience and collaboration.

The programme of research has developed an inclusive position on digital security that foregrounds benefits for people, and places technological risk in relation to those benefits. The programme of research was further developed through the a UK Research Council funded fellowship, Everyday Safety-Security for Essential Services (ESSfES), and a UK Research Council funded research network that co-ordinates research in social justice in the digital economy (Not-Equal). This network includes a focus on inclusive digital security research under the theme of "Digital Security For All".

1.3 Structure of this Monograph

The monograph starts with a sketch of the main schools of security theory that set out the broader social and political conceptualisations of security into which technological security is deployed. The monograph then briefly sketches technological security and its position on the protection of people, before placing technological security in the wider security theory landscape.

These first three chapters reveal the limitations of traditional security thinking when examining technology use in a digitally-mediated society. In particular, the three chapters show how on the one hand digital technology creates spaces in which people can be empowered to create and shape opportunities, but on the other hand does not provide a means with which to respond to many of the security issues that emerge as a result of that creativity. The next three chapters present a possible way forward in the form of a digital security paradigm that draws on the trust-led, relational, issues-focused work of digital civics, and the broad range of ontological positions from security theory, in order to respond to these limitations.

As a reference, this monograph has the remaining chapters:

- *Security Theory Building Blocks*
  chapter 2: maps out the main schools of thought in political and social theories of security, and reflects on their relevance to technological security.

- *Technological Security and Its Users*
  chapter 3: maps the history of technological security with respect to understanding its intersections with other forms of security.

- *Connecting Technological Security and Security* Theory
  chapter 4: examines how security theory and technological security can be brought further into conversation.

- *Digital Civics, A Practice-Lens and Digital Security*
  chapter 5: introduces a wider lens on human-computer interaction and introduces the notion of practice.

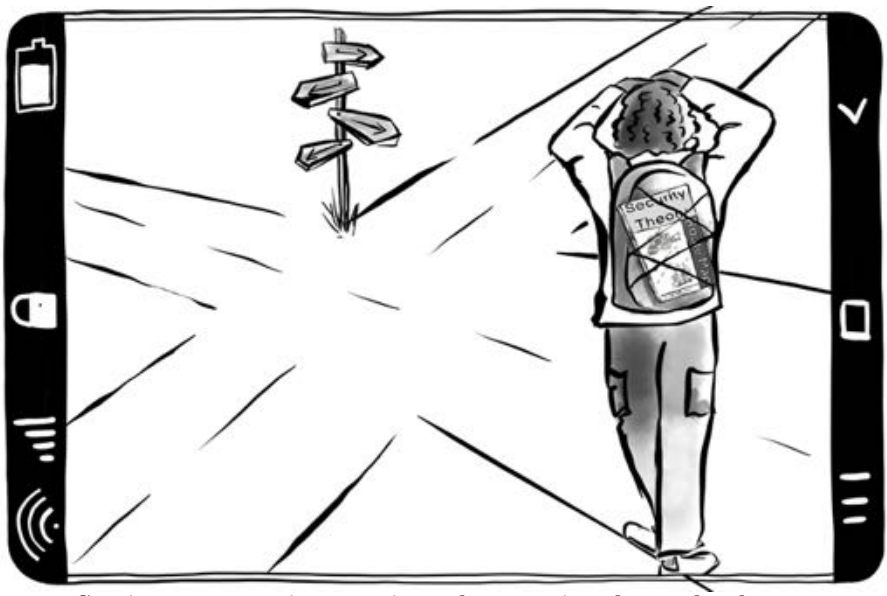
- *Digital Security: Practice and Methods*
  chapter 6: sets out possible approaches to practising and researching digital security.

- *Digital Security From Research to Application*
  chapter 7: sets out three worked examples of digital security and presents key digital security principles.

- *Conclusions and Call to Action*
  chapter 8: summarises the arguments set out in the monograph and issues a call to action.

The intended audience for this monograph is those studying and researching digital design and interaction. The monograph introduces the reader to alternative ways of conceptualising digital technology security. The call to action is to bring together diverse communities of scholarship to develop ideas of inclusive digital security as part of a wider move to build a society that is secure for all.

1.4 Concluding Comments



Setting out on a journey into the security theory landscape

This introduction has set out the case for considering technological security from two positions: from the position of protecting data and technology, and from the position of protecting people in a digitally-mediated society. When considering the latter, we are not solely considering technological security, but where technological security intersects with both other securities and with an individual's embodied sense of

security and insecurity. To denote this wider position, the term "digital security" is being applied to this intersectional form of technological security.

In the next chapter we explore political and social theories of security to set the scene for a wider conversation about digital security, and to provide conceptualisations that might help us to better understand some of these intersections outlined in this introductory chapter.

2

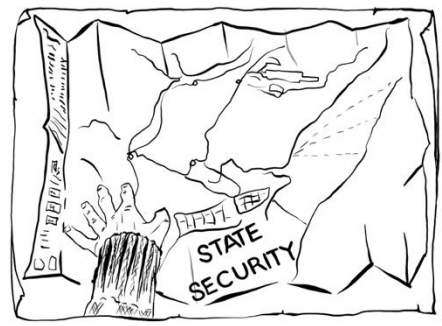
Security Theory Building Blocks

From the VOME project onwards (UKRI, 2020), we discovered that what we understood as technological security was part of a much wider security landscape. We learned that people's information sharing and protection practices were shaped not only by their digital interactions, but also by wider issues relating to people, state and organisational security. We learned that in order to understand the effectiveness of technological security from the perspective of people and institutions, we needed methods and conceptual frameworks that could help us to identify and analyse the intersections of technological security with other forms of security. Repeatedly our studies showed that an individual experienced technological security in the context of economic security, personal security, job security and emotional security. Through our analysis, it became clear that technological security controls can amplify or attenuate issues and concerns in those other areas of security, which in turn increase or decrease an individual's sense of security. We learned that this was, in part, because not only do security technologies protect data and technology, but they also signify the security position and values of the institutions providing the technologies and services.

To understand more about these different security positions and to

see what we could learn from the different schools of social and political theories of security, we began to map the concept of security in the classical canon of security thought (RISCS, 2018). Therefore, rather than start with the fundamental principles of technological security, this monograph starts with a broader overview of security, to better understand security in its different forms.

This chapter is written with technologists and students of sociotechnical security in mind. It is written to highlight that there is a wider canon of security thought than technologists are typically taught, and to introduce some security concepts that are not typically presented in discussions about technological security. It is important to understand that the security positions set out in this canon of security thought can be related to moments in history that have resulted in particular ways of conceptualising vulnerability, strength, values and order. These moments have shaped the values that are prioritised and the trade-offs that are deemed necessary to maintain or restore order and stability.



Security technologists rarely focus on other forms of security

The security theory literature shows that security is rarely considered as an abstract concept (Smith, 2005; Baldwin, 1997), but often explained in terms of how security is achieved or practised. The social and political theories of security set out differing ways of achieving and practising security, and foreground different sites or focus for protection - for example, in the security of states, people and society, as well as the security of the environment, and of digital technology and services. The literature also shows that regardless of the focus, security is also a contested concept (Wolfers, 1952; Baldwin, 1997; Smith, 2005) where different groups privilege different values for protection. Smith (2005) argued that security itself is not a value, but is the protection of a partially ordered set of values. This simply means that different ways of seeing the world have different prioritisations of values. Each position on security foregrounds a different value order for protection.

Different groups privilege different values

As a result, security is also a concept that means different things in different contexts (Smith, 2005), and yet, despite these differences, most forms of security have at their core the twin concepts of power and order. For example, Thucydides, a Greek General and historian, wrote about power and war and in so doing, about security. His works from the 5^{th} century BC present a particularly brutal form of security, one in which strength is presented in terms of the ability to survive and, therefore, the weak perish. Thucydides could be interpreted as putting forward a position on security where internal order and military power were needed for a secure state and therefore, by extension, a secure people. This security position was taken up and appropriated by self-described 'realists' in the 20^{th} century.

The realist security perspective could perhaps be articulated as *whatever an individual or a state cares about, or wants to do, they have to survive first in order to be able to do that.* The point is that such a position prioritises what the state needs to do to survive. Security therefore is seen as an a priori condition to the state attaining the other conditions it might want.

When security is first explicitly theorised in the contemporary era, it is done by elite individuals within state military and foreign policy establishments (Wolfers, 1952; Lippmann *et al.*, 1943). Their conception of security is therefore concentrated on the state and its assets. Such thinking orders values because it implicitly argues the security of the state is preserved by enforcing buy-in to the values that the state promotes, and agreement that as a result, other values will be sacrificed. How the values and the order of those values is arrived at and the means that states use to enforce those values, are political decisions.

This type of security thinking is often described as reductionist as only certain voices are empowered to state which values count and security is reduced to a question of supporting the order of the values or being against the order of the values. Security is thus conceptualised in material terms because such security is primarily shaped by both technologies of security and the territory that is to be protected.

From the 1980s onwards, the realist paradigm was challenged. For example, liberal scholars challenged the privileging of the state in security discussions (Kaldor, 2007). The concept of security was broadened to consider other focus for protection, for example regional, economic, human, societal and environmental security. Nevertheless the notion of security retained the same basic conception of what security was. Constructivist scholars (such as the Copenhagen school (Lipschutz, 1995)) argued that security was not in material form at all, but an effect of power generated through speech acts. By contrast, feminist security scholars such as Hudson (2005) challenged the notion of the state's role in security, and looked to the security roles of the individual and the collective (Doty, 1998). This shift in thinking also saw a move to include the contemplation of security as a form of empowerment and emancipation.

2.1 Navigating Security Scholarship

Political and social theories of security focus on a *referent object*: things whose existence is threatened, and which have a legitimate claim to survival (Buzan *et al.*, 1998). In traditional thinking the referent object is the state. Such theories also include both the *threat actor* (someone or something that can inflict damage on a referent object), and the *security threat* (an event or action that can inflict damage on a referent object).

Security as protection from harms

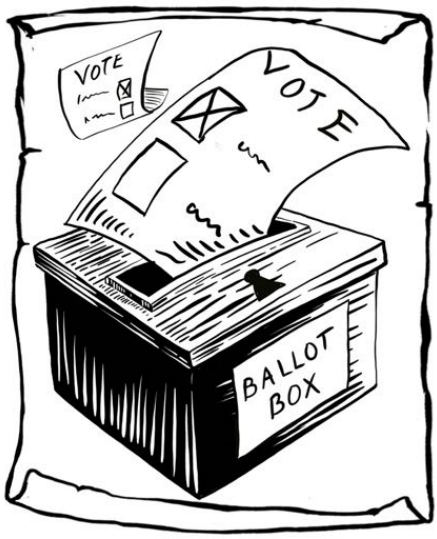
How these elements are mobilised depends on the worldview to which the security theory is committed. This is sometimes referred to as 'ontological commitment' and can be determined from the responses to a number of fundamental security questions. For example, Smith (2005) set the following security questions:

- "Who or what needs to be secured?"
- "What is doing the securing?"
- "Why is the subject being secured?"
- "Who or what is the subject being secured from?"

This list was itself derived from David Baldwin's wider set of questions (Baldwin, 1997):

- "Security for whom?"
- "Security for which values?"
- "How much security?"
- "For what threats?"
- "By what means?"
- "At what cost?"
- "In what time period?"

Baldwin's list contrasts with Smith's list by giving additional focus to how security is done which means that some of the questions include the notion of a trade-off that often occurs when thinking about security as a practice. The idea of a trade-off makes clear that security is achieved at the expense of something else. Baldwin's list also gives less focus to the underlying political reasoning. Instead, Baldwin focuses on the choices that are being made regarding the security practice and the responses to the threat. Such questions provide us with a means of distinguishing between the different forms of security. The questions can also be asked from multiple perspectives to determine the intersections between different forms of security in a given situation.



Security and politics are entwined

The answers to these questions reveal the value order that is being protected by a particular security position. Smith (2005) makes a distinction between *security* and *securing*. Securing is a term linked to the state of being secure, or being safe. It is achieved through an alignment of values and agreement of goals and objectives, as well as through protection of assets (Burdon and Coles-Kemp, 2019). Securing does not always result in achieving the state of being secure because for that state to be achieved, securing has to successfully result in sufficient agreement as to the values that are to be prioritised, and in what order, so that the order is stable and uncontested.

Security is therefore the state of being secure, which Smith (2005) argues is brought about through the attainment of political order. Smith goes on to argue that security is simply a reflection of the relative success or failure to secure. Analysing who or what is doing the securing identifies the implicit social and political processes at work as well as the economic incentives for complying with the political order.

2.2 Security Theory Landscape

Epistemologically, security theories are often placed on a positivist-interpretivist continuum. On one end the realist and liberal theories of security are positivist in the sense that they focus on how power and control is exercised and what security does, not how security is experienced. At the other end of the spectrum, interpretivist theories of security focus on a wider set of security concerns than the protection of the state. The interpretivist theories consider how state control and protection is experienced.

Balzacq (2010, p. 57) argues that *"any approach to security starts with, and rests upon, a specific ontological commitment"*. In this context, ontology is a particular view of what constitutes being, and what entities constitute that being. Each ontological position privileges a particular order of values. Balzacq (2010) argues that security theory can be aligned with different types of ontology, and explains that *"theories can be committed to different kinds of ontology, but two broad categories capture the range of possibilities on offer: materialism and idealism on the one hand, and monism, dualism and pluralism, on the other"*.

Many security technologies have their roots in conflict

Balzacq (2010) explains that theories typically sit within a combination of one from each category. For example, whilst there are examples of materialism-monism (Whyte, 2018), the traditional state-centred security theories are typically a combination of materialism-dualism. Implicit to realist security theories is the assumption that some form of conflict over security interests is inevitable. The ability to win conflict and ensure the security of the state is *materialist*, both because it is shaped by access to military power (forms of security technology) and the expert knowledge regarding how to win conflicts and its focus is on the protection of territory.

In this example security is understood as dualist in the sense that there is a gap between the real-world state of these conflicts and our understanding and knowledge of them.

As we move along the positivism-interpretevism continuum, security theories move more towards pluralism because multiple actors are considered and therefore multiple views of the real-world and multiple understandings of what it is to be secure are also considered. At the same time, the focus of security is not to achieve a material form of

security but the realisation of ideals, typically achieved with human interaction (debate, negotiation and other forms of communication) rather than material forms of security.

2.2.1 Security From Different Angles

Security theories offer different angles from which to look at security. We might consider security in terms of a state attacking another state or defending its borders. We might look at security in terms of the relationship between the citizen and the state. We might see security as interwoven relationships between institutions that protect and promote a state's interests. We might diversify what we see as the state's interests and consider, for example, environmental or societal security. We might think of security as a political act. Security from these different angles widens the analytical toolkit of those working with technological security.

In the classical (Western) canon of security thinking, ideas about security have often been born out of conflict, as can be seen with the earlier classical Greek example. These theories focus on notions of military strength, anticipate conflict, and regard the amassing of power through military strength (sometimes in conjunction with political and strategic alliances) as a means of winning a conflict. For example, classical realism has the following principles: accumulation of power; flawed nature of humanity; and continuous struggle to increase their capabilities. Classical realism explains conflicting behaviour through human failings. Wars are explained, for example, as resulting from the behaviours of particular aggressive statesmen, or as a result of domestic political systems that give greedy parochial groups the opportunity to pursue self-serving expansionist foreign policies.

Environmental security considers human impacts on the planet

Gradually, over time, realist theories became tempered by a focus on security through law-regulated international relations. Whilst the state is still foregrounded as the referent object, collaboration, rule of law, collectivity and trade relationships are prioritised as the primary mechanisms of security. In this security position, strength comes from mutual interest and the maintenance of relationships between states.

A social contract sets out security responsibilities

A secure relationship between the citizen and the state is often implicit to a successful security strategy. One means of articulating the relationship between the state and the people is through the concept of a social contract, where the relationship between the individual and the state is maintained. A social contract refers to an allocation of security roles and responsibilities between the individual and the state, whereby the individual is protected by the state, in return for obedience and compliance. Rousseau, Locke and Hobbes are three European philosophers from the 17^{th} and 18^{th} centuries who are often cited when presenting ideas of social contract (albeit contrasting ones). Rousseau believed that progressive civil society is primarily founded on property and ownership, underwritten by a social contract. Locke believed that all are free to do as they wish within the law of nature and of reason, whilst Hobbes argued that people choose to enter a social contract, giving up some of their liberties in order to enjoy peace. This thought experiment is a test for the legitimisation of a state in fulfilling its role as the entity that can guarantee social order, and for comparing different types of states on that basis. These positions are universalist in the sense that they are principles that are applied to all.

Security can also be understood in terms of institutional relationships and political processes. The Copenhagen School (a school of academic thought that emphasises non-military aspects of security) conceptualised security as institutional values and norms where the site of security is both the state and society. It put forward the idea that a framework

for approaching the construction of security is based on *'speech acts'* that designate particular issues or actors as existential threats. This introduced the idea of *'securitisation'*, rhetoric that claims an *'existential threat'* to a particular referent object where this move is accepted by a relevant audience. Security, in this sense, is a site of negotiation between speakers and audiences, albeit one conditioned significantly by the extent to which the speaker enjoys a position of authority within a particular group (Lipschutz, 1995, p. 57).

Using the analytical device of sectors, securitisation theory shines a light on security interactions that, whilst part of a state's security, foreground a more nuanced range of referent objects and reveal different security strategies at work. Sectors are *"seen as analytical devices that are used to shed light on the diverse practices and dynamics of securitization"* (Albert and Buzan, 2011). These sectors are (Nyman, 2013):

- military sector
- environmental sector
- economic sector
- societal sector
- political sector

These different sectors are used in security analysis to highlight the different relationships at work that are used to secure the state. However, sectors are not distinct and remain part of a complex whole. The Copenhagen School also developed the concept of desecuritisation. This is the process whereby issues are recategorised from security to political (Nyman, 2013). Securitising an issue elevates the status of that issue so that it takes on an unchallengable position within the body politic. A successfully securitised issue will attract more resource and is potentially able to circumvent the typical rules and regulations. The ability to move an issue from being regarded as an issue of security to an issue of politics underscores how issues are socially constructed into security issues that mobilise responses, and attract resources to support those responses.

2.2.2 Missing and Hidden Voices

Whilst the broadening of security issues by thinkers such as those within the Copenhagen School made security thinking more relevant to a wider range of stakeholders, there are still questions about the extent to which stakeholders with lesser power or capabilities are represented. Security scholar Hansen (2000) suggests that a tendency for security positions to focus on *'dominant voices'* contributes to further silencing those already marginalised from security debates.

The protection of those stakeholders with less power and those less able to be heard, are recognised through theories of human security and feminist security studies. For example, human security is a concept that identifies the security of human lives as the central objective of national and international security policy (Doty, 1998). Theories of human security contrast with, and grew out of increasing dissatisfaction with, the state-centred concept of security. Human Security can play five roles, namely: *"to provide a shared language to highlight a new focus in investigation; to guide evaluations; to guide positive analysis; to focus attention in policy design; and to motivate action"* (Fukuda-Parr and Messineo, 2012, p. 15).

Human security examines the rights to protection

Human security expands the scope of security analysis and policy in multiple directions: groups and individuals, international systems, institutions, politics, environment, regions, publics, media, forces of nature, and of market. Such a scope also addresses notions of security from a fundamental human rights perspective.

Feminist security theorists extend this position and challenge the marginalisation of voices within society. Feminist security studies draw on scholarship from many disciplines including anthropology, history, literary theory, philosophy and sociology, as well as those trained in peace research, security studies and technology (Wibben, 2010).

Individual branches of feminist security studies form a broad coalition that has four common characteristics (Wibben, 2010):

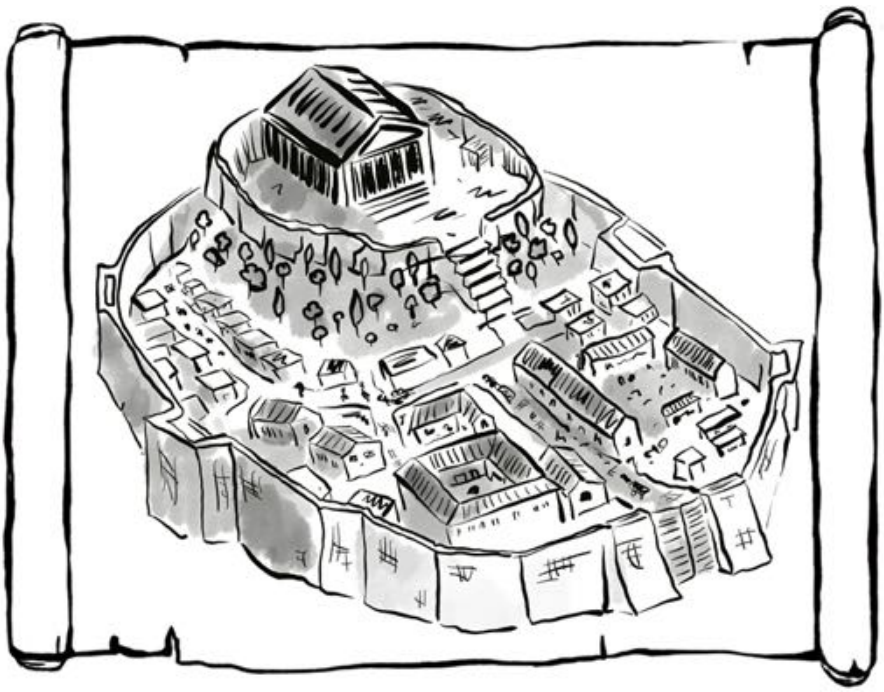
- Ask feminist research questions
- Base their research on women's experiences
- Adopt a (self)-reflexive position
- Have an emancipatory agenda

In contrast to other forms of security studies, feminist security studies deliberately include gender as a central unit of analysis, where gender is understood as a category of analysis that is socially constructed (Wibben, 2010). For example, feminist critical theorists examine prevailing assumptions about both women and men: what it is to be a man or a woman, what is appropriately feminine or masculine behaviour, the roles of women and men within society, the workforce, and the family (Whitworth, 1994, p. 24). This body of work questions security from perspectives that challenge the status quo. This work includes the perspective of marginalised men (Hooper, 2001; Connell, 2005) as well as the position of women. Feminist security studies therefore also debate the power structures that shape feminist security studies. Feminist security thinking is important to the study of security because it offers both critique and the invitation to imagine an alternative basis for a secure world. On the one hand, feminist security theory critiques traditional security positions, and challenges the legitimacy and the universality of

A critical position challenges dominant notions of strength and power

these positions. On the other hand, feminist security theory can also invite people to imagine alternative forms of security, and debate how those forms of security might be enacted.

2.2.3 Security Logic



In practice, a security strategy is composed of several security logics

The purpose of security is in some form or other to protect an object or group of objects from harm, and security theories represent different ontological positions on which objects need to be protected and how. The reasoning processes, together with the rhetorical moves, the forms of evidence and the rationalities used to determine which objects to privilege for protection, can be described as a logic. Doty (1998) characterises these as security logic and argues that many security logics are inextricably linked with the notion of territory. For example, some families of security theory privilege the state as the primary object to be secured, where state is defined as a form of territory. Other families

of security theory privilege society as the group of objects to be secured, but the understanding of society is still linked to the idea of territory. A further grouping privileges the protection of people and through the notion of identity is, often linked back to territory.

For example, Doty (1998) identifies three main security logics: national security logic, societal security logic and human security logic. National security logic is a traditional, state-centred conception of security. It is negative: security is perceived as the absence of an external threat to the national/state territory. Societal security logic also has at its heart the notion of self-other, and is typically linked to a notion of territory, but foregrounds identity politics. Protection in this context is therefore the ability of a society's values and ways of living to continue in spite of change or attack. Human security logic is a human and individual-centred conception of security. It is a positive logic: security perceived as a desired good which enables the pursuit and enjoyment of a good life. It is a logic of inclusion, which transcends state boundaries and binary conceptions of identity.

Accompanying the grouping of privileged objects in a security logic is a power structure, and set of relationships, that enable the object to be secured. An operational code of practice, which encompasses a way of thinking about security, and a way of framing security, is used to bolster the authority of a security logic.

There are other security groupings that one might consider. For example, environmental and planetary security. Environmental security is about relationships between human activity and the planetary biosphere. This looks, for example, at the impacts of overdevelopment, pollution, ecology, water, population, conflict and war, and which proposes a new theory of security on this basis. The United Nations Conference on the Human Environment (1972) initiated a discourse on planetary security that has centred on *"epistemic communities, social movements, governmental departments, and international organisations"* (Buzan *et al.*, 1998, p. 71).

Understanding the impact of a security logic requires analysis from multiple perspectives. As Hudson *et al.* (2013) illustrates in a security analysis of human trafficking, security issues are complex in that multiple perspectives are enmeshed within a security issue, and multiple

theoretical positions are needed to both understand security and to identify which security practices are needed in response. In this example, the analysis reveals that taking a state-based analysis only sheds light on one aspect of the power dynamic, but combining a state-based analysis with a human-security analysis sheds further light on how people are vulnerable to human trafficking.

Disrupting Traditional Security Logic

The way in which security is reasoned is related to what type of security outcome is desired. Some of the families of security theory focus on the protection of objects, whereas others focus on the freedoms gained if threats are removed.

Security often has adversarial connotations

Positive and Negative Security: Negative security is the term used when describing the security reasoning that is used to protect objects. Negative security is an inward-looking force focused on protection and maintaining the status-quo. Negative security is a logic of binaries (Doty, 1998), such as the binary of challenge-resistance or the binary of inside-outside, authorised-unauthorised. This is a reasoning that Hoogensen and Rottem (2004, p. 155) describe as *"attack, parry and riposte"*.

Protective security reasoning often has a negative connotation. For example, security is defined by Gjørv (2012, p. 836) as *"relat[ing] to the treatment of security as a concept we wish to avoid, one that should be invoked as little as possible. We value it negatively, or it is understood to represent a negative value"*. As realist thinking shows us, security is not always about protection; security can be offensive as well as defensive. Even in its defensive form, security can be done in such a way that it is experienced as mean or pernicious. This is because security can be

seen as a series of trade-offs, where security for some is achieved at the expense of insecurity of others. This might also be because the security goals are driven not only by a desire to protect but also a desire to weaken or harm the opponent.

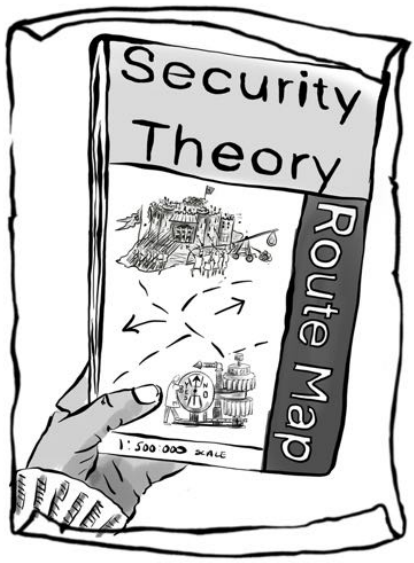
By contrast, positive security is an outward-looking force that is progressive and enables people to move forward and develop their lives. Positive security is *"something that is positively valued, or as something that is good or desired. It is a good which provides the foundation to allow us to pursue our needs and interests and enjoy a full life"* (Gjørv, 2012, p. 836). Positive security brings to light the notion of security as enabler. It provides a language through which to think about the human condition and human contribution to security. Roe (2008) highlights the interplay between negative and positive forms of security, and how security strategies are often a combination of both types of security.

Universal Principles and Contextualised Operation: The reasoning deployed in security theories is universal in nature in the sense that a security theory sets out universal frameworks and principles that apply to everyone. However, the doing of security is largely contextualised and it is in this contextualisation that the opportunity arises for positive and negative security to interoperate. Whilst the security frameworks themselves tend to have either positive or negative security goals, the carrying out of security enables these goals to be nuanced and threaded with protection and enablement.

Security practices take many different forms

Contextualisation is an important means of introducing the security pluralism needed for everyday life. As feminist security scholar, Heidi Hudson, highlights the operationalisation of security can be contextualised if individuals and communities are acknowledged as active participants in the security framework (Hudson, 2005).

2.3 Relating the Theories to the Technological



Technological security represents different security interests

Studies and practices of technological security have been largely separated from the broader discussions of state, individual and societal securities. Technological security is, however, complex and draws on all of the strands of security thinking that we have discussed in this chapter. On the one hand, technological security often represents the interests of powerful institutions, whether that be the state or technology companies or other institutions of power. On the other hand, the security interests that technological security represents can elicit strong responses from the people using the technology and this, in turn, can shape the way the technology is used.

As societies become increasingly digitally-mediated, the state (and other institutions of power) and the individual come into direct conversation with fewer intermediaries. In a sense, technological security is the seam through which many of the security interests of the state and other institutions of power in a digitally-mediated society come into direct conversation with the security of the individual. As a result, technological security should not only focus on a negative security position that focuses on protection from threats, but must also enable access to the benefits that technology offers in such a way that the technology user can be free from fear.

Security theories also raise questions about the way that technological security is designed and deployed. For example:

- "Should the idea of social contract and notion of human rights be included in the way we design and deploy technological security?"

- "Should we consider which values are implicitly being ordered by security technologies when the effectiveness of security technologies are evaluated?"
- "Does a deployment of security technologies change the ordering of values or who is included (or excluded)within that order?"
- "Should we model the impacts of technological security in economic, political and social terms as well as in terms of the technical performance of the security technology itself?"
- "Do the social and political meanings of technological security change if the political security goals are changed?"

Security technologies have social and political meanings

The need for asking these questions that consider the social, political and economic context can be seen in the work of Molotch (2013). This work that highlights the importance of both protection and enablement when he writes about how security technologies must protect against harms, but in such a way that does not undermine people's access to services. Denying people's access to services or necessary support can weaken them to the point where the service no longer has the desired outcome. An example of this is given by Lester *et al.* (2019) in the context of the design of detention centres where, it is argued that designing prisons using technologies that support the prisoner, as well as punish them, enabling the criminal justice system to meet the twin goals of punishment and rehabilitation.

Central to studies in cybersecurity is the understanding that technological security is connected to the security interests of institutions of power. There is a rich body of work that encompasses the global patterns of technology adoption within society and the roles governments play

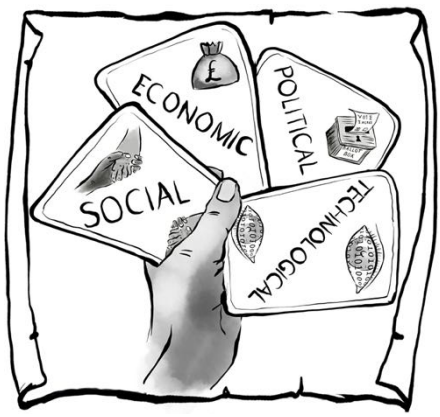
in responding to cybersecurity challenges (Whyte, 2018). This results in several areas of cybersecurity study ranging from mechanisms of cyber conflict and global cybersecurity governance to global resistance movements in cyberspace and the development of new cybersecurity technologies. The focus of cybersecurity studies in this sense examines the development of digital technologies from the perspective of the state and how such technologies change global power structures.

When looking at cybersecurity from the perspective of technological security, cybersecurity might be regarded as the political and social dimensions of technological security (Hansen and Nissenbaum, 2009) which means that risks are both in terms of the risks to technology but also from technology (Deibert and Rohozinski, 2010). Shires (2019) presents technological security as a form of cybersecurity and breaks it down into *three practical worldviews* which are practice-based rather than theory-based. These three worldviews are:

- National cybersecurity: a national perspective that focuses on the networks and technologies within the state's boundaries;
- Commercial cybersecurity: an organisational perspective that focuses on the networks and technologies within both for-profit and not-for-profit organisations;
- Individual cybersecurity: an individual perspective that focuses on the protection of an individual's technology.

Shires (2019) uses Wittgenstein's notion of family resemblance to analyse how these three worldviews relate, and how they differ. This analysis shows that whilst national cybersecurity interprets technological security from the state perspective, and in terms of a conflict regarding control of the internet, also highlights how there is overlap with the economic imperative of organisational cybersecurity, with both perspectives sharing a similar cybersecurity practice. In the categorisation produced by Shires (2019), the focus is on the protection of the assets relating to the organisation, state and individual. However, this analysis might be extended to consider how technological security, when harnessed to a social or political security logic that is intended not only to protect

assets but also exclude some from accessing those assets, can result in the technological security controls being experienced as mean and pernicious. This is particularly salient when considering the experiences of people dependent on digital by default services for essential support, as found in in areas of welfare, health, housing and finance. In the case of digitalised welfare, technological controls are often experienced as mean and pernicious (Coles-Kemp *et al.*, 2020a) because the welfare policy that such controls enact regards welfare claimants as potential misusers of the digital welfare system.



Technological security has social, economic and political dependencies

Regardless of which practical worldview is being deployed, technological security has traditionally focused on negative security because its goal is to ensure that technological systems and services remain available, and are reliable through the regulation of access. Shires (2019) states *"[c]ybersecurity can be defined as the prevention and mitigation of malicious interference with digital devices and networks"*. This means that technological security is focused on the protection of technology and data from threats of unauthorised access, unauthorised modification and unauthorised disclosure. The enablement dimension of security is noticeably absent in such a characterisation, and perhaps there is an implicit assumption that the social, economic and political context into which the technology was deployed would provide the means and the mechanisms to bring about positive security.

However, as digital technologies and services have become embedded into everyday objects as well as our de facto means of accessing essential services, building and maintaining social and bureaucratic relationships - the security issues related to digital technologies are greater than protecting assets and encompass protecting our way of life. This means that we have to think about both positive and negative security issues, who is excluded as well as included by technological security and the

economic, social and political implications of technological security decisions. This shift also means that we have to think about security not only in material terms (i.e. the technologies we can use to protect us), but also in ideal terms (i.e. the ideals that we are striving to achieve). Political and social theories of security highlight that securing in a given situation is achieved by a combination of the technology and social and political processes - a point that is often not clearly made in technological security studies.

2.4 Concluding Comments

This chapter has set out a pallet of security concepts and analytical techniques that enable us to examine some of the different forms of security that technological security intersects with. Social and political theories of security provide different views as to what should be secured, different notions of who or what does the securing, and offer a range of strategies for carrying out these securing processes. These different ways of looking at security problems are important because it is not enough to secure the individual parts of a digital service or technology, we also need to understand how the security of technologies intersect with the security of people if we want truly secure digital products. In the next chapter, we look at how technological security has traditionally recognised the intersections with other securities, and how it responds to them.

The version of record is available at: http://dx.doi.org/10.1561/1800000030

3

Technological Security and Its Users

Security technology fits into a broader set of security logics

In the UK Research Council funded project Families Separated by Prison (UKRI, 2020), we examined how families separated by prison view and engage with the support services provided to them. We learned that to understand the embodied aspects of information sharing and protection practices in this context, we needed to not only understand the security goals of families and the criminal justice sector but also the design of the information control technologies and how these reflect criminal justice policies. Understanding the design of the technological security is as important as understanding the broader security themes that shape the responses to technological security.

Technological security is focused on the protection of data and technology and places an emphasis on the security of the transaction between human and computer or between computer and computer, rather than placing the security of the technology in the wider security context in which it is being used. Technological security was originally a coalition of digital network security, computer security and the security of the data itself. However, as technology and its uses have evolved, these sites of security have also become cloud security, security of edge computing and critical national infrastructure security.

Whilst computers were not originally designed with security in mind, by the 1970s computer security was becoming a focus of research and a concern of practice (Saltzer and Schroeder, 1975; Caine, 1977). Not only was there concern about the vulnerability of data and of computational power but also the implications of computing for the safety and security of the individual (Saltzer and Schroeder, 1975).

Security concerns for both technology and people

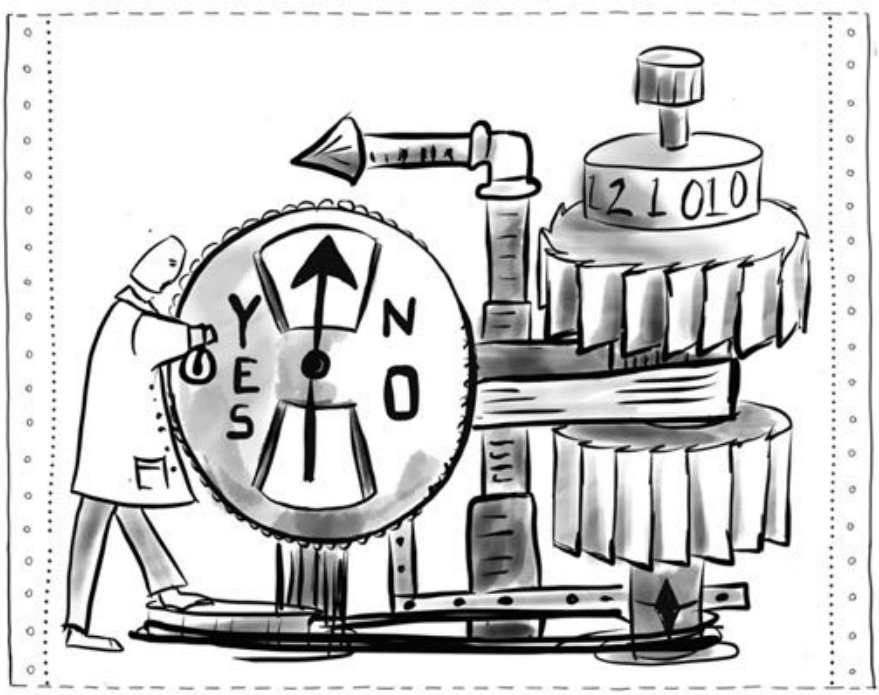
These two concerns are not disconnected but the drive to encourage take up of computer technology and services resulted in a foregrounding of the benefits of technology and a backgrounding of the potential harms. This drive also meant that the benefits were not considered for society as a whole or for where benefits were most needed but for where there would be greatest commercial benefit.

In this chapter the principles of technological security are briefly outlined and the process and challenges of implementing technological security are sketched. The chapter then looks at two developments of practice: security management and usable security. These have the potential to connect technological security with other forms of security and to an individual's embodied sense of security.

3.1 Basic Underpinning Principles

There are three core technological security principles: confidentiality, integrity and availability. Gollmann (1999) defines these terms as:

- *Confidentiality*: prevention of unauthorised disclosure of information.
- *Integrity*: prevention of unauthorised modification of information.
- *Availability*: prevention of unauthorised withholding of information resources.



Security technologies regulate society as well as data

Additional principles might be needed depending on the application, for example principles of authenticity and accountability can be added (Gollmann, 1999). These principles are used to protect technological components, software, applications and digital services. The history of these

principles go back to the start of computer security as a profession and technical practice. Saltzer and Schroeder (1975) wrote a tutorial paper on the protection of information systems. It is one of the first papers to summarise the principles of securing information systems and it lists the categories of security violations as follows:

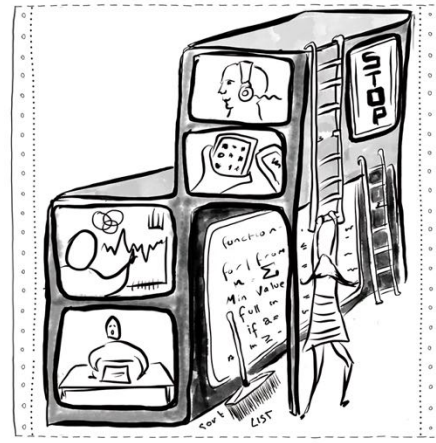
- Unauthorised information release: this category of violation contravenes the confidentiality principles and information is available to those who are not authorised to access it.

- Unauthorised information modification: this category of violation contravenes the integrity principle and information is modified in ways that are not authorised.

- Unauthorised denial of use: this category of violation contravenes the availability principle and information is not available to those who are authorised to access that information.

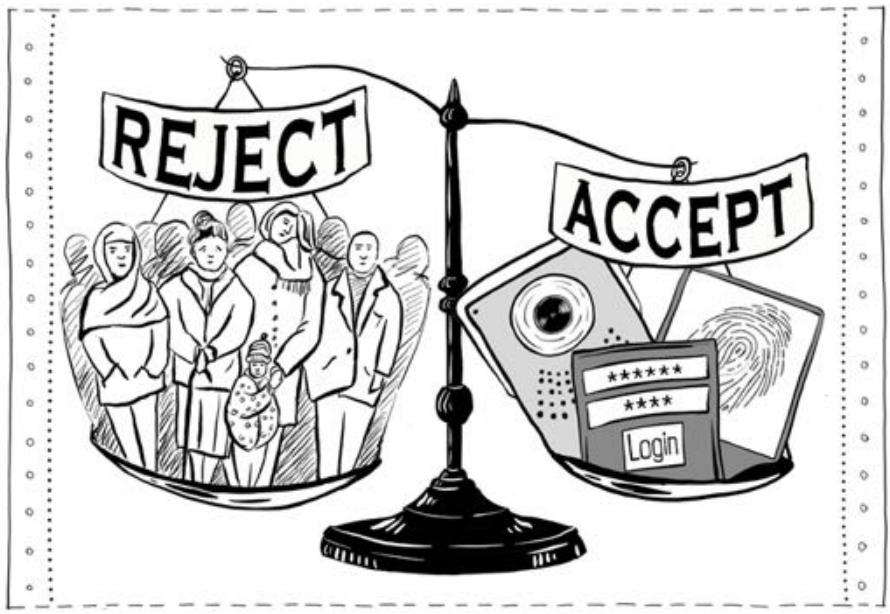
In each case Saltzer and Schroeder point out that these violations do not necessarily require access to information or a programme. For example, they highlight that unauthorised information release can take the form of an attacker observing a pattern of information and inferring meaning from that pattern without having access to the information. Similarly, an attacker might change information but does not necessarily have to see the changes they have made for sabotage to occur. Finally, they make the case that denial of use (commonly referred to as a denial of service attack in the cyber security domain) can happen when an attacker disrupts the processing of information but this can happen without an attacker having access to or modifying the information itself.

After completing this list, Saltzer and Schroeder reflect on the term "unauthorised": *"The term "unauthorized" in the three categories listed above means that release, modification, or denial of use occurs contrary to the desire of the person who controls the information, possibly even contrary to the constraints supposedly enforced by the system"* (Saltzer and Schroeder, 1975, p. 1280). This quotation highlights that technological security terms often have both social and technological meaning.



Security technologies touch many aspects of our lives

The tutorial also brings out the layered nature of technological security, by first addressing security at the very core of a computer system, moving through the application, data processing and communication layers to the layer that interacts with the users of the technology. Saltzer and Schroeder also recognise that technological controls are not always necessary or needed: *"In many cases, it is not necessary to meet the protection needs of the person responsible for the information stored in the computer entirely through computer-aided enforcement"* (Saltzer and Schroeder, 1975, p. 1281). There is an implicit assumption in this statement that the protection needs of people will be met in other ways. Forty-five years later, and in a society where many of our interactions are digitally mediated, this assumption can lead to a gap in protection of the individual. Whilst the technological protection techniques that Saltzer and Schroeder describe are not necessarily current today, and the state of the art of these techniques have since evolved, the design principles that they list are still current today. Saltzer and Schroeder list eight design principles that system and software designers should follow to minimise security flaws and guide the design of a secure system. Significantly, this is one of the first papers of its type to take usability into account. The eighth principle is termed "Psychological acceptability" and the principle specifies that *"the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly"* (Saltzer and Schroeder, 1975, p. 1283). However, it is not only usability that is called for but the recommendation that: *"Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized"* (Saltzer and Schroeder, 1975, p. 1283). This alignment between the mental model of control and its design becomes harder as the communities using technology diversify.



Security technologies impact people

Saltzer and Schroeder also identify two additional design principles which, they claim, do not fit perfectly with computer systems but which need to be considered further. These two principles are:

- *Work factor* - assessing the amount of work an attacker needs to undertake in comparison to the gain they will receive; and
- *Compromise recording* - a tamper-proof means of recording violations and system compromises.

These are both principles that are heavily dependent on the context of use, whilst also highlighting the sociotechnical nature of security. They also highlight the conflicted way that users of technology are conceptualised in technological security. On the one hand, technological security thinking is designed to reduce the problems caused by flawed software coding and system design. On the other hand, security is also achieved by thinking the unthinkable: "What if people cannot be trusted to comply with the goals of the system and what if people try to subvert the system for unauthorised means?". Over time this

thinking has become the norm, the start point being that people cannot be trusted. In so doing, the new unthinkable question became: "what if people are trusted?". As we shall see later on in this chapter, the relationship between trust, people and computing became a key concern of the usable security community and becomes the start point for an alternative technological security paradigm.

3.1.1 Security and Software

Many of the design principles set out by Saltzer and Schroeder still sit at the core of design processes and frameworks for the design of safe and secure software. For example, the introduction of security functionality into code design has been encouraged through the conceptualisation of the Security Design Lifecycle (SDL) introduced by Microsoft in 2006 (Howard and Lipner, 2006), that has now become the SafeCode initiative. SDL has threat modelling processes at its core that enable software developers to identify potential weaknesses and attack vectors in the code, during its design (Shostack, 2008). The goal still remains that security thinking is *"baked into"* the software design process as a part of the software development lifecycle (Geer, 2010; Potter, 2009). In response to the introduction of agile design processes in software development, efforts have been made to make the process of producing safe software more agile and responsive to the software coding practices of developers. However, aligning security thinking with software coding practices can prove problematic. Reasons for this difficulty include a lack of knowledge and interest in the inclusion of security functionality (Weir *et al.*, 2016). In addition, security application programming interfaces (API) are difficult to implement (Nadi *et al.*, 2016) and the processes needed to communicate software flaws are not always easy to implement in the software development lifecycle (Lopez *et al.*, 2012). The UK's Research Institute for Sociotechnical Cyber Security has recognised the challenges of implementing a SDL into the wider software development lifecycle and has sponsored several projects, including "Motivating Jenny to write Secure Software" (OpenUniversity, 2020).

Software code is often developed in teams of coders with different levels of ability and skills (Kitchin and Dodge, 2011), which can make

the production of reliable code complex (Bjarnason and Sharp, 2017). Motivating software development teams is also a complex task, as explained by the canon of literature presented in the literature review of Beecham *et al.* (2008) on the topic. The problems of motivating teams to produce reliable code are further complicated by the economic and business pressures of software projects (Rosenberg, 2008). Consequently, while Saltzer and Schroeder's principles might seem simple, their implementation is challenging as software developers are typically contracted to produce a working product not a secure working product.

It is also noticeable that software development processes such as SDL, typically do not include principles that directly take into account the people for whom the software is being designed. As a result, whilst provision is made for training, Saltzer and Schroeder's provision for psychological acceptability is not directly attended to, as explained by Caputo *et al.* (2016). The lack of focus on the psychological acceptability of security controls leads to security controls being deployed without consideration for their impact on a person's workload, or on the emotional responses that might be triggered by the design of the security controls. This is perhaps because there is an expectation that the security controls not only secure the software code but in securing the code will also secure the people using the software. Without attending to the psychological acceptability principle, the likelihood of poorly designed and implemented security controls that are not universally accessible or beneficial is significantly increased.

3.2 The Art of Management

The deployment and management of the technology is an important complement to secure software design and creates the environment in which security technologies are used. There are also processes that are often tasked with overcoming the security gaps and shortfalls of digital products. The secure deployment and management of digital technologies and services is governed by standards and regulation. There are standards that regulate the design of the cryptographic algorithm all the way to the implementation of security controls in an organisation. Security in general and security of technology in particular are especially

Poorly designed and implemented security controls increase insecurities

prone to the deployment of standards partly to preserve interoperability and partly because security itself is a contested concept. It has been argued that where there is contestation, standards are used to resolve such disputes (Power, 1994).

As digital products and services are deployed in ever wider and more open contexts of use, the potential for conflicts in terms of the security required and how it should manifest itself becomes increasingly more likely.

Such conflicts require arbitration and processes through which consensus can be arrived at and risks of disagreeement and dissent managed. Arbitration in the case of technological security is managed through a series of management processes outlined in security management standards: in particular the international standard, ISO/IEC 27001. Security management is often presented as a continuous process and in early versions of the standardisation of security management, this continuous process was sometimes termed the "Plan, Do, Check, Act" (PDCA) cycle and was applied to individual security management processes of risk assessment, risk management (including risk treatment, risk monitoring and risk communication), audit, incident management, training and awareness and management review.

Security management acts as a form of conflict management

As shown in the following two examples, there are several points in the cycle to identify conflict and to negotiate consensus at these points of conflict. In this respect, the security management processes are more

than a simple bureaucratic exercise. For example, risk assessment can be broken down as follows:

- Plan the scope of the risk assessment, select risk assessment tools.
- Do the risk assessment by identifying assets, the threats and vulnerabilities to the assets and assess the measure of risk of the threat exploiting the vulnerability of a particular asset using selected risk calculation.
- Check the calculations of the risk assessment.
- Act to revise the calculations where necessary.

Similarly, the security audit process can be broken down as follows:

- Plan: Identify the scope of the audit, identify the audit methods and the audit team and set the audit plan.
- Do the audit: Carry out the audit programme.
- Check: Discuss and revise audit findings; Review corrective action.
- Act: Revise audit findings in view of corrective action review.

In addition to processes, security management also uses the notion of a policy to articulate and set security goals, set direction for the use of technological security within an organisation, and provide a benchmark against which security can be assessed. At the core of security management is the principle of compliance, using the technological security as expected and gathering, processing, storing and sharing information in ways that conformed with the security policy.

There are many challenges with such a management approach, not least because gathering evidence that mitigation works is complex, as is determining what mitigation practices work and what constitutes effective mitigation. At the same time, such processes only work as mitigation and protection strategies if there is buy-in to the security goals. Such an approach also assumes that people accept that security risk is, to a degree, individualised. This means that there is a responsibilisation

of technological security in the sense that individuals are expected to carry the responsibility of taking protective action (Renaud *et al.*, 2018; MacEwan, 2017). Renaud *et al.* (2018) argue that responsibilisation should be minimised and a focus should be given to a cyber security approach that is state-led and effectively implements security standards, gathers information on cybercrime and sanctions insecure behaviours.

3.2.1 Security Dialogue

Whilst security management is in many respects another materialist form of security – largely focusing on processes and policies – security management also works at the intersections between technological security and other forms of security dealing with the conflicts that arise in these environments. The main security management activity at these intersections is security dialogue. The dialogue is used to bring together different stakeholders and to undertake different ways of securing to align different worldviews on what an organisation requires from technological security (Burdon and Coles-Kemp, 2019). As a basis for this, some studies have focused on how to build skills related to the construction of dialogue and to cope with dissent and conflict (Ashenden and Lawrence, 2016; Reinfelder *et al.*, 2019). The relevance of security dialogue is revealed in a study on organisational access control (Stevens and Wulf, 2002) where the relationship is illustrated between inter-organisational cooperation and the assets that need most protection and how processes of inter-organisational cooperation have to be able to respond to the tensions that arise over access to key assets.

Security practitioners encourage and enable compliant behaviours within an organisation (Burdon *et al.*, 2016) and this requires a security dialogue that makes security legible to non-experts. The broader sociotechnical security literature has looked at the types of interactions that security practitioners have had with other parts of an organisation. For example, the practices of the security profession have been critiqued as being too technocratic (Stewart and Lacey, 2012) and contributing to a divide between security practitioners and the groups of people with whom they are working (Albrechtsen and Hovden, 2009).

One of the criticisms has been that security practitioners often lack self-reflection and the ability to consider how their own attitudes, behaviours and styles of communication can block engagement with the individuals and groups whose data and technology they are trying to secure (Ashenden and Sasse, 2013). To respond to these challenges, security practitioners themselves have tried to diversify their forms of engagement (Reinfelder *et al.*, 2019).

Security practitioners need to understand people as well as technology

Some of these dialogues take the form of interactions (Burdon *et al.*, 2016) that are often part of formal processes such as risk assessment (Baskerville, 1991), audit, and training and awareness (Albrechtsen and Hovden, 2010). In a bid to improve engagement and understanding of the security concerns of non-specialists, the role of guardians and mentors have been considered (Haney and Lutters, 2017; Becker *et al.*, 2017). Such individuals act as a connector between technological security expertise and non-experts.

In the community setting, this is considered to be a guardian role offering protection to vulnerable individuals such as elderly people (Nicholson *et al.*, 2019). In an organisational environment, this interlocutor is framed more as a champion of security, encouraging a wider take-up of compliant security practices (Gabriel and Furnell, 2011; Becker *et al.*, 2017).

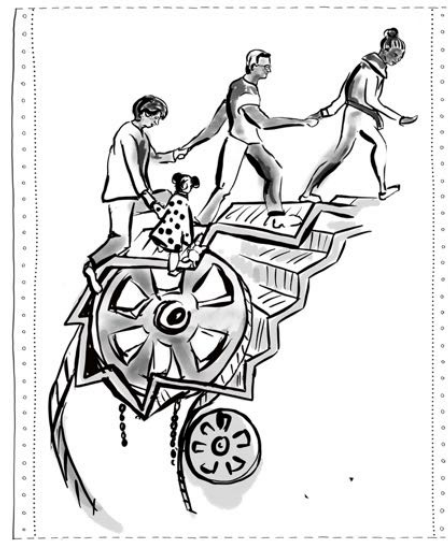
Research shows that security communication in an organisation is primarily focused on the creation of messages that *"sell"* security practices (Ashenden and Lawrence, 2013; Burdon *et al.*, 2016; Chipperfield and Furnell, 2010), particularly by making such messages relatable to particular groups within an organisation (Harbach *et al.*, 2014). There

has therefore been a focus on how to deepen and diversify interactions between security practitioners and other groups within an organisation, both from the practice and research communities (NCSC, 2019; Albrechtsen and Hovden, 2010).

3.3 Usable Security

Security dialogue and management cannot fully compensate for poorly designed security technology. Even if the software and security components are well-designed, they need to be accessible and usable to the intended product user communities. Not only must the security technologies be accessible and usable but so too must the processes that surround them.

The original design principles for safe and secure software largely focus on the internal design of the software. However, Saltzer and Schroeder (1975) also included a principle regarding the usability of secure software. Such a principle has a focus on the people using the security technology and fitting the security technology to people's needs and practices rather than the other way around. Saltzer and Schroeder's paper was one of the first to introduce the notion of usable security (CyBOK, 2019b). It was not until the 1990s that usable security became an acknowledged area of both security practice and scholarship. In the mid-1990s Zurko and Simon (1996) created the term *"user-centred security"* and outlined three categories for user-centred security practice: usability testing for systems development; the development of security models and mechanisms to be used in user-friendly systems; and making the needs of users the primary goal of secure system design and development. Zurko and Si-



Security technology with poor usability can disempower people

mon regarded usable security as a necessity for systems that responded to *"real world problems"* or problems as experienced by people who use systems.

Zurko and Simon highlight one of the cultural conflicts in security scholarship that still affects the study of technological security today: the prioritising of mathematical rigour over other forms of rigour. They phrase this as *"Mathematical rigor was emphasized over usability"* (Zurko and Simon, 1996), but then go on to point out that whilst social systems can be modelled mathematically, such modelling leaves out many aspects of security practice. This observation has been echoed in much subsequent work and as technology has become woven into everyday practice, this observation has been extended to a societal as well as an individual understanding of practice (Bella and Coles-Kemp, 2012).

Adams and Sasse (1999) wrote a paper titled 'Users are Not the Enemy'. The title and framing of the paper challenges the notion that people are the weakest link in security and are responsible for making technology vulnerable to attack. Adams and Sasse argued that non-compliance is caused not by laziness or a lack of interest in technological security but due to the design of the controls or a lack of knowledge by people. They also argue that focusing on the strength of the control rather than the usability of the control can make a technological control less effective because the control will not be complied with. Adams and Sasse's paper presents a study that demonstrates the implications of not considering human factors and provides evidence to support the position in Zurko and Simon (1996).

The lines of argument in Adams' and Sasse's paper were borne out in two areas of usable security research: making security legible for non-experts and designing security controls in line with the needs of people. Both these research themes and concomitant practice areas are significant because they represent the first time that a concerted effort is made to return to Saltzer and Schroeder (1975)'s twin objectives of both protecting technology **and** people.

3.3.1 The Need for Usable Security

Research shows that a *'compliance overhead'* (Beautement *et al.*, 2009) can result from unnecessarily complex security rules that do not support the tasks that people have to carry out. Complex rules can be further exacerbated by poorly designed technologies and compliance regimes. The true cost of this type of security overhead is rarely calculated (Inglesant and Sasse, 2010). This cost of ill-fitting security is difficult to assess, because compliance is not a single behaviour (Blythe *et al.*, 2015) and because there are a multitude of factors that influence compliance. Blythe *et al.* (2015) lists these factors as:

- Self-efficacy, which is an individual's belief about their own ability to perform a security task or exert an influence over it.
- Social influence, which is the extent to which an individual's behaviour is influenced by others.
- Attitude towards the task.
- Perceived susceptibility towards a security threat against which the task is designed to protect.
- Perceived severity of the threat.
- Response efficacy, which is the extent to which a task is regarded as an adequate response to the threat.
- Response cost, which is the time, money and effort required to deploy the task.

There is a long history of including people's needs and requirements in technology design, but including security requirements in design specifications has proved problematic because these were requirements that people did not necessarily feel they needed. The research of Inglesant and Sasse (2010) shows that complex password rules not only impact on an individual's productivity but can also lead to security workarounds. However, whilst the term *workaround* has negative connotations, such practices can equally/also be positive and supportive (Woltjer, 2017).

Technological security is not a one-size fits all approach

However, it is not only the design of controls that can make it difficult to comply with security policy and guidance. MacEwan (2017) describes a *"responsibilisation conundrum"*, where complying with guidance is problematic because the guidance does not relate to an individual's lived experience of the security issues, and does not address the full range of technological security issues that people have to respond to in their everyday lives. In not aligning with an individual's lived experience, not only are relatable cybersecurity issues not always addressed but the controls that are proposed can result in a moral conflict over which course of action to take. Such conflicts can often be found in controls that relate to monitoring and service access where there is a choice between achieving a performance goal or a security goal (but not both). This conflict is further exacerbated by the overhead of additional work and cognition load that security policy and rules can engender (Beautement *et al.*, 2009). This can result in *"security fatigue"* (Furnell and Thomson, 2009; Stanton *et al.*, 2016; Pham *et al.*, 2019), where security task overload and the challenges of processing conflicting security rules further complicate responding to security issues. In response to such

conflicts, an individual may feel forced to break the rules and this, in turn, can lead to a form of moral conflict where stress induced through feelings of guilt result from rule breaking. Interestingly, Pham *et al.* (2019) demonstrate that neither self-efficacy nor additional organisational resources are effective at reducing burnout. The study also showed that simplifying security tasks is also not effective in reducing burnout. In the next section we consider how modelling human-computer interactions might help to further identify challenges with non-compliance.

3.4 Modelling the Security of Human-Computer Interactions

Human computer interaction is complex and as we move into a world of sensor technologies, voice activated software and other forms of pervasive computing, modelling what we understand as the interaction in a particular context is key. The study of usable security brings to the fore the importance of modelling security in the context of human-computer interactions. Identifying where security issues emerge during interaction and where people's practices and interactions both protect and enable interaction are important aspects of security analysis. Such analysis helps to identify both where security technologies are needed and also the degree to which existing controls are effective and appropriate to the interaction.

These models are a means of identifying the intersections between technological security and other forms of security, as well as environmental factors. Different types of security analysis (ranging from the social to the mathematical) require different types of abstraction. Abstraction can be defined as a process of isolating common features or relationships. These abstractions typically take the form of models that present simplified explanations of the interaction. These simplified explanations will always be inaccurate but nevertheless models can have a value as part of security analysis (Box, Draper, *et al.*, 1987).

Currently there are two dominant forms of modelling: modelling of human-computer interaction through different economic lenses, and sociotechnical modelling that draws out the different human-computer interactions in a particular security scenario.

3.4.1 Economics of Security

Making the argument for usable security has increasingly been made in economic rather than social or political terms and modelled as such. In his groundbreaking work Anderson (2001) sets out the argument for examining information security problems through an economic lens. The economic drivers were examined within a technological security context, and in particular investigated how perverse incentives undermine the use of security technologies. Highlighting how behaviourial or organisational factors can encourage or impede the adoption of security controls, this research demonstrates why designing security controls that people use is a difficult and complex task.

Security can be modelled as a series of economic trade-offs

Acquisti (2013) presented how both classical economics and behavioural economics were of value to information security. He points to the economic concept of trade-offs and frames technological security as a trade-off. For example, Herley *et al.* (2009) considers why passwords have not been replaced as a means of authentication despite being a source of stress and difficulty for many people. Herley highlights that whilst the stress may be considerable for individuals, the use of passwords is convenient for the institution providing the service both in terms of their implementation and maintenance.

Beautement *et al.* (2009) tried to address this power imbalance and developed the idea of productive security. They took up the microeconomic argument by looking at the cost to an individual of complying with a security policy. They argued that it was important for an organisation to identify where the friction points were in an organisation's security policy, so that the additional work and the disruption caused by the security policy could be reduced through re-design with technological security becoming more productive as a result.

Behavioural economics has also been the inspiration for a line of inquiry that looks at the possibility of nudging security behaviours and practices. For example, Coventry *et al.* (2014) have looked at different ways to deploy interventions and re-design security technology so that users of that technology are encouraged to engage with the technology in a secure way. However, security behaviours and practices are complex and often require more than nudges. Designing nudges to affect any form of behaviour change has ethical and moral implications as well as questions of efficacy (Mols *et al.*, 2015). It is also possible that designing nudges can affect behaviours negatively (Nicholson *et al.*, 2017). As a result, careful modelling and analysis is needed to identify where security controls need to be placed.

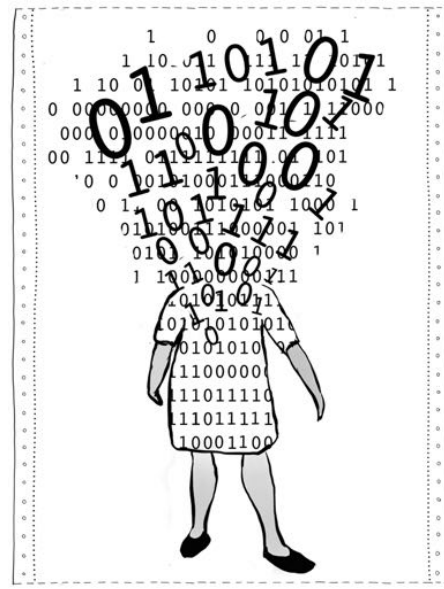
Understanding human interaction and practices through an economic lens has been a dominant force in much of the usable security discussion. However, such a position does not critically evaluate what security means in a particular context and to whom. Furthermore, such a position does not engage with the ways in which security is lived and experienced by different people, or allow for the idea that multiple conceptualisations of security might be in operation at the same time. When Saltzer and Schroeder (1975) referred to different mental models of security, the response has been to try to engender a universal mental model rather than to embrace these different security positions and design technologies that can respond to that plurality.

3.4.2 Sociotechnical Modelling

Usable security is one aspect of technological security scholarship that has begun to acknowledge social and cultural aspects of technological security. Another branch of technological security scholarship to acknowledge these aspects is sociotechnical security modelling. Such models are used to help reason about natural examples of system compromise or attack (Probst *et al.*, 2006). Attaining the most useful level of abstraction (Probst and Hansen, 2008) to understand technological practices as embedded within a social context is one of the challenges of modelling natural phenomena.

In this branch of study, sociotechnical systems are acknowledged as complex systems and often focus on better understanding the interactions between humans and technology (Pieters, 2011). Formal modelling offers a language in which to articulate and analyse the connections between these components. The process of using formal methods requires researchers to carefully unpack the relationships between the technical and the social. Formal methods offer a different language through which to reflect on the social (Bella and Coles-Kemp, 2012). This provides social researchers with an alternative means of deconstructing wider social concepts and a common language through which to compare social and technological security components.

Sociotechnical modelling has been particularly dominant when thinking about *"insider threat"* to technological security. The modelling of technological security is typically understood as attack and defence and people are framed as either undertaking the role of attacker or defender. Technological security also presents another dualism: insider-outsider. The insider is someone who is within the trusted perimeter and who by being inside is themselves trusted. The outsider, someone who is outside the perimeter, is not trusted and the perimeter is designed to keep those individuals outside. The insider threat problem has many definitions (Bishop, 2005b) and insider-outsider is therefore another concept that, whilst it can be designed as a binary in technological terms, is considerably more conflicted and fluid in its social conceptualisation. Sociologist Crinson (2008) has argued that the notion of insider and outsider is based on a sense of trust and trust is not binary in this context but a continuum. It is for this reason that Bishop (2005a) defined the insider problem as a continuum of problems.



Technology shapes people as much as people shape technology

3.4.3 Emergent Forms of Modelling

In the last few years, modelling approaches that draw on the humanities and creative practices have begun to emerge in both security research and practice. One example of this is the creative engagements work (Dunphy *et al.*, 2014) that sets out ways of engaging that produce creative abstractions of security-related scenarios. Such approaches are typically built on narrative methodologies. For example, Vines *et al.* (2012) used a narrative approach with older participants to examine how cheques were used in everyday financial transactions with a view to understanding how digital technology might replace cheques.

Physical modelling techniques using creative materials such as LEGO has been used in different ways to model security-related scenarios. For example, Frey *et al.* (2017) designed a games format that used LEGO as the medium through which to explore potential threats to critical national infrastructure. Hall *et al.* (2015) also offer an alternative example of modelling that uses LEGO to describe scenarios together with a facilitated process to identify security issues and co-design responses.

3.5 Concluding Comments

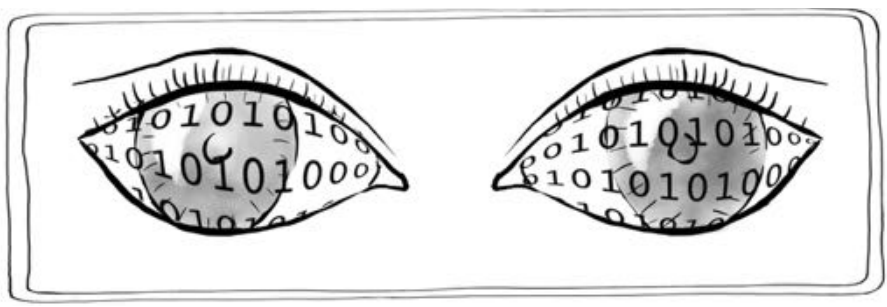
Usable security and security management have broadened technological security and introduced its scholarship and practice to alternative ways of thinking about technological security. However, both usable security and security management stay firmly in the technological security paradigm and focus on how best to support the protection of technology and data in a way that is supportive to the user.

In this next chapter, drawing inspiration from social and political theories of security, we explore how this paradigm might be adjusted to consider the intersections between technological security and other forms of security.

4

Connecting Technological Security and Security Theory

Digitalised welfare is a common theme in many of our projects. When working with marginalised and underserved communities, the digitalisation of welfare is the point at which digital interaction becomes mandated for many people in those communities.



Security technologies are designed with particular assumptions

Digitalised welfare is one of many examples where technological security becomes interwoven into a wider security policy (Coles-Kemp *et al.*, 2020a). Whilst technological security is typically designed, engineered and deployed without explicit reference to social and political theories of security, security technologies nevertheless deploy a security logic that is formed from a particular worldview, and has associated assumptions

about the groups who will use the system, their security needs, and the potential attackers of the system.

Attacks are often seen as inevitable

At an initial glance, technological security seems most clearly aligned with the more traditional forms of security thinking. For example, technological security is often deployed with a mindset that attack will happen and that there needs to be sufficient defence, in the form of security controls, to repel attack. The deployment of technological security takes place using a series of cost vs. benefit trade-offs to determine which controls are deployed and where. The deployment of technological security is also usually conducted through collaboration agreements between parties that will access the technology and is bounded by regulation and law.

Our worldview shapes whom we see as attackers

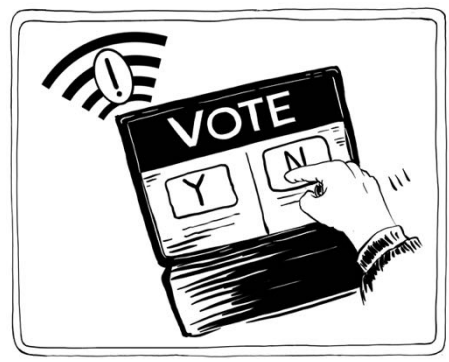
In general, security thinking is ground in a particular way of seeing the world and technological security is no different in this respect. Rogaway (2009) has argued that, for example, cryptographic problems are socially constructed in the sense that they are produced from a particular worldview that prioritises specific types of problems. The social construction of scientific and technological problems is a position of Science and Technology Studies (STS) (Sismondo, 2010, pp. 57–71) which argues that the prioritisation and form of problems is cultural and social. In this chapter we look at some of the different perspectives that shape the meaning of security issues in a digital context.

To recap, as outlined in Chapter 2, Balzacq (2010) argues that *"Theories can be committed to different kinds of ontology, but two broad categories capture the range of possibilities on offer: materialism and idealism on the one hand, and monism, dualism and pluralism, on the other"*. By sketching the conceptual space in this way, we are also able to think about complex technological architectures in different ways (Whyte, 2018; Balzacq and Cavelty, 2016).

Table 4.1: Ontological positions applied to technological security

Ontological pairings	Digital Example
Materialism-dualism	Access control technologies
Idealism-pluralism	Security dialogue

As shown in Table 4.1, it could be argued technological security already deploys some of these ontological pairings. For example, a firewall is a form of *materialism* in the sense that it is both an artefact that represents technological thinking about how to protect a network from an unwanted ingress or egress but it is also a means of defending and protecting territory.



Material forms of security control many aspects of our lives

The firewall represents a form of *dualism* in the sense that its efficacy can only be proven once we have a hypothesis as to what ingress/egress attempts are authorised and unauthorised access, and can determine from what we observe whether an attempt is authorised. It also represents a binary form of thinking by constructing the notion of access as something that is either permitted or denied. By contrast, security dialogue is a form of *idealism* in the sense that the goals of security dialogue are the ideal of making individuals secure in their relationships with each other by building trust and empathy through dialogue. It can also be described as a form of *pluralism* in the sense

that the security outcomes and inputs come from multiple actors and represent different viewpoints and different understandings of what constitutes the real world.

By recognising different possible ontological combinations, a way forward opens up for responding to security issues that emerge at the intersections between technological security and other forms of security. As Table 4.1 also shows, whilst we may think of technological security as materialist-dualist, in the securing spaces that support and enable the technologies – such as those used for security dialogue – alternative ontological combinations are possible. In the following sections we look at some of the ways we might re-shape our security technology thinking to take into account a broader range of ontological security positions.

4.1 Re-shaping Technological Security Thinking

The following are three of the possible ways in which we might re-imagine, re-design or extend technological security, drawing on social and political theories of security as inspiration.

Changing the threat model: Political and social security theories show a broader range of actors and stakeholders than is usually considered in the study and practice of technological security. Additionally, political and social theories of security articulate a broader range of security harms than is typically considered in technological security. Drawing inspiration from this, we might develop threat models that assume the perspective of a different stakeholder, both in terms of addressing the security issues and goals of that stakeholder, or formulate the concept of strength and weakness from another perspective.

Security binary: Threat models are typically constructed as a binary, such as attack and defence, and then under that category a related set of binaries are found: authorised and unauthorised, and malicious and benign. This is a typical position of traditional security thinking. However, by shifting towards a pluralist position, these binaries could be replaced by an acknowledgement of different security outcomes for different stakeholder groups. In responding to this pluralist position, trust, consensus building, conflict identification and resolution become the central tenet, rather than attack and defence.

Artefact or experience: Security technologies take particular material forms and are a product of the science that informs them. Material forms tend to align security technologies with a positivist outlook on security, by linking security technologies to forms of science that reduce security as a concept to the protection of self from others. By including an embodied or experiential position, the technological security focus will also encompass the felt experience of the security technologies, and how security technologies might invoke particular responses from different groups and individuals. To achieve this security technology design might take inspiration from theoretical positions such as ontological security, theories of care and theories of human security. In the following sections we examine three perspectives or worldviews into which we might introduce these re-imaginings.

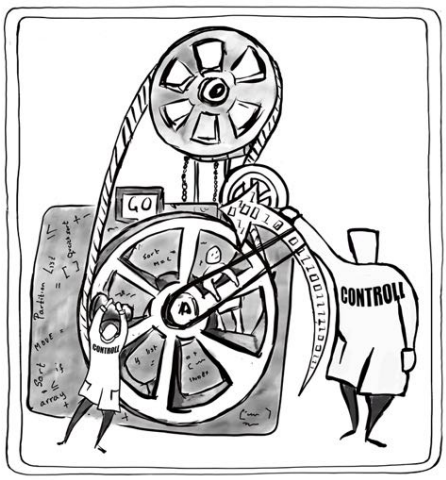
In the following three sections we look at where we might introduce the above opportunities for re-design. We set out three interconnected perspectives that have routinely surfaced in our research. These are:

- Top-down perspective: this takes the position of security technologies being deployed by technology experts to maintain or change a particular order.
- Everyday perspective: this takes the position of security technologies being deployed in a collaboration between technology expert and non-experts in response to security issues that occur in everyday life.
- Internal perspective: this takes the position of the way individuals experience and embody technological security.

4.2 Top-down Perspective – a Default Position

Security technologies have traditionally been designed from the perspective of those regarded as experts in a particular area of technological security. Traditionally, in network and computer security, security technologies are often designed on the basis of an order or a hierarchy of technology users, where the user at the top of the hierarchy has the most power in terms of data and resource access and that power degrades

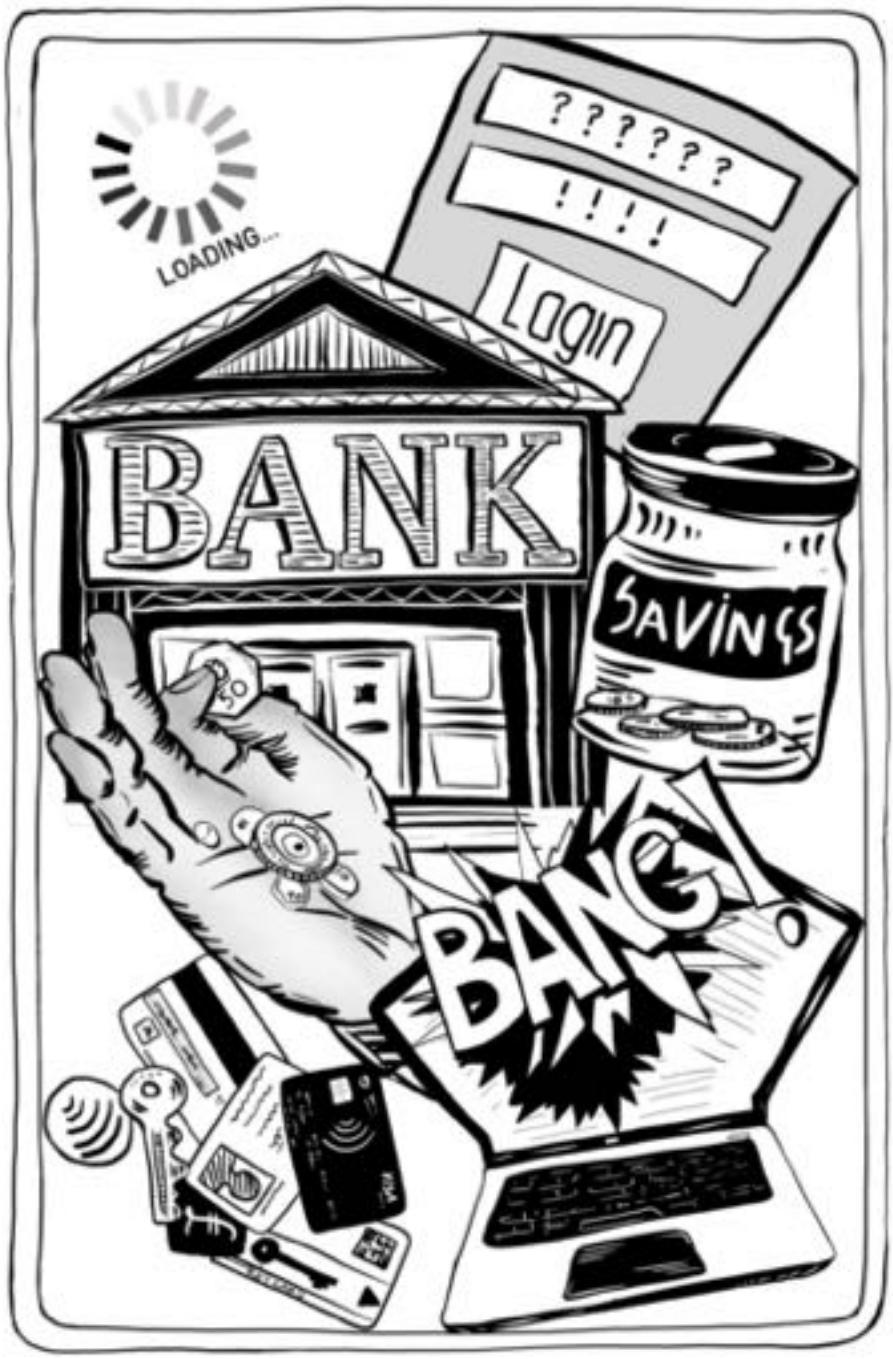
down through the hierarchy. Access is a form of protection, and protection of data, networks and devices is made possible through limiting and controlling access. This access control articulates the terms of a binary of inclusion-exclusion: those who are granted access (included) vs. those who are not granted access (excluded). Whilst there are technological developments that may move control away from a hierarchical structure of control to a more egalitarian one where individual users have sole control over access to data, the fundamental security logic remains the same.



Security technologies are designed by experts

The dominant narrative that surrounds technological security is the prevention of harms, protection of key assets and the use of technology to protect key assets. Whilst the emphasis might be different, there is nevertheless a common focus on protection and defence against threat actors who are seeking to damage or access something of value. The narrative of protection often uses binaries, for example attack-defence, authorised-unauthorised and strong-weak. Doty argued that traditionally, security is a logic of binaries: challenge-resistance, defence-escalation, recognition-defeat (Doty, 1998, p. 80). These binaries can also be found in technological security, and are represented by binaries such as authorised vs. unauthorised, insider vs. outsider and malicious vs. benign. These binaries are used to formulate rules about what constitutes secure and insecure behaviour in a technological setting.

The technological control is used to determine which side of the binary an action or event falls. The strength of the control in technological security is often measured through its ability to control access to the perimeter of the technology, and to control what happens within the boundaries of the technology. The strength of the control is measured both in terms of its resistance to attack, but also in the context of



Security technologies often enable other material forms of security

the strength of the attacker (Carlos *et al.*, 2013; Martina *et al.*, 2015), where the notion of strength is socially-constructed in similar ways to the security problem. Shires (2020) highlights that those enacting technological security and, by extension, the controls themselves, often struggle to determine into which category technological actions should fall (for example the difference between authorised and unauthorised access, because those binaries have a moral basis which is often conflicted and fluid).

The morality of technological security control can be further muddled by the measurement of the control strength in terms of its economic value. This is an economic strength that is measured both through its ability to protect assets where value is measured in economic terms, and in terms of cost of loss, again measured in economic terms if the controls fail. By considering security controls in economic terms, their social and political meaning is often lost. Technological security seldom includes conceptualisations of social impact, morality or ethics and the main processes and approaches to assessing the strength of controls rarely acknowledge these perspectives. As a result, gaps can appear between how a security technology is designed to feel, look and work like, and how it feels, looks and works like for those using it.

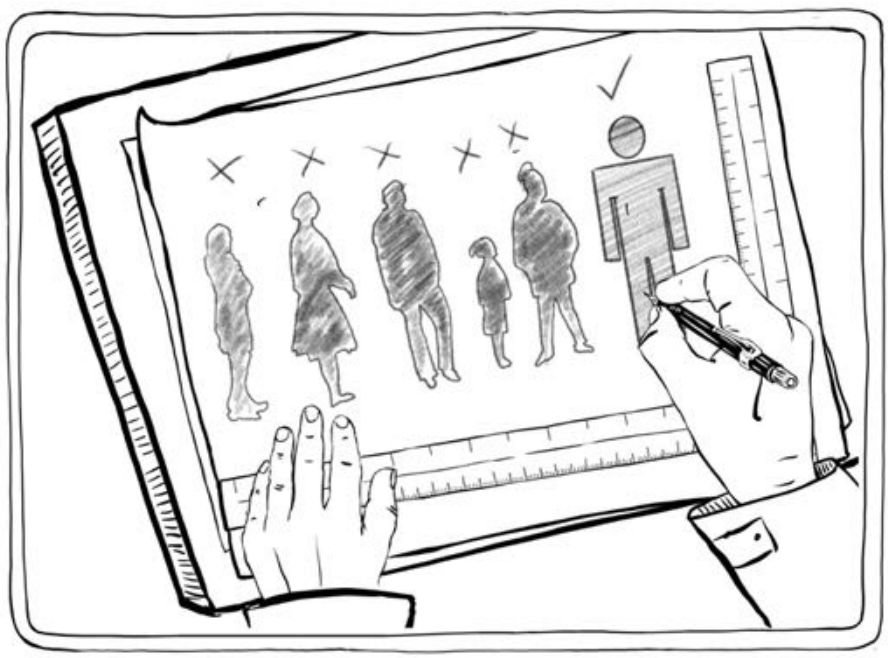
Security is at times a game rather than a moral choice

These gaps and silences can result in adverse social impacts and can have implications for the effectiveness of security controls, given that they offer spaces in which security technologies can be outmanoeuvred and circumvented (Coles-Kemp *et al.*, 2014). In the following section, some of these implications.

4.2.1 Negative Effects of the Top-Down Perspective

Designing security technologies without taking social impact into account can result in the following:

- Language and concepts that focus on the protection of technology rather than people as the end goal.
- Articulate threats that are not regarded as meaningful in a person's life.
- Produce technologies that are difficult to use and require capabilities and resources that people do not have access to.



Security technology design can encode particular biases

The material form of security technology, and the functionality that such technology has, can exclude on grounds of usability, legibility and accessibility. It can also exclude because it expects a particular set of resources and capabilities, including access to technology, access to

knowledge and also access to power to make particular choices about what to access, when and how. The material form can also exclude simply because it is not relevant or useful to the security issues that people face.

However, it is not simply in the design and framing of the security technologies that exclusion occurs. It can also be the case that security technologies enable services that in turn implement a logic of security that excludes. For example, the shift in exclusion through new conditions in the UK's welfare policy revision of 2012 were implemented using digital technologies, the access to which was regulated through technological security controls. The underlying security logic can therefore exclude in the following ways:

- By aiding and abetting the creation of systems that make people feel devalued, threatened or isolated.
- By limiting the social interactions and relationships necessary for creating the trust foundation on which security technologies can be effective.

Exclusion creates resistance and hostility

Security technologies are harnessed and put to work by the security logic underpinning a particular service or technology. This logic can empower, protect and support some groups, but can also disempower, threaten and alienate others. The logic can also offer a form of security that is not meaningful to certain/particular groups of people. These types of exclusions can be overlooked, misunderstood and trivialised when they are not seen or understood by those who design and deploy the logic. For example, access to a digital health service might offer personal choice and freedom to some, but might be bewildering or demand digital skills or infrastructure that some simply do not have.

Exclusion can result in responses that might offer the individual security in the short term, but may not be in either the best interests of either the state or other institutions, or indeed of the individual, in the long term. Such responses to exclusion from digital technologies include (Coles-Kemp *et al.*, 2014):

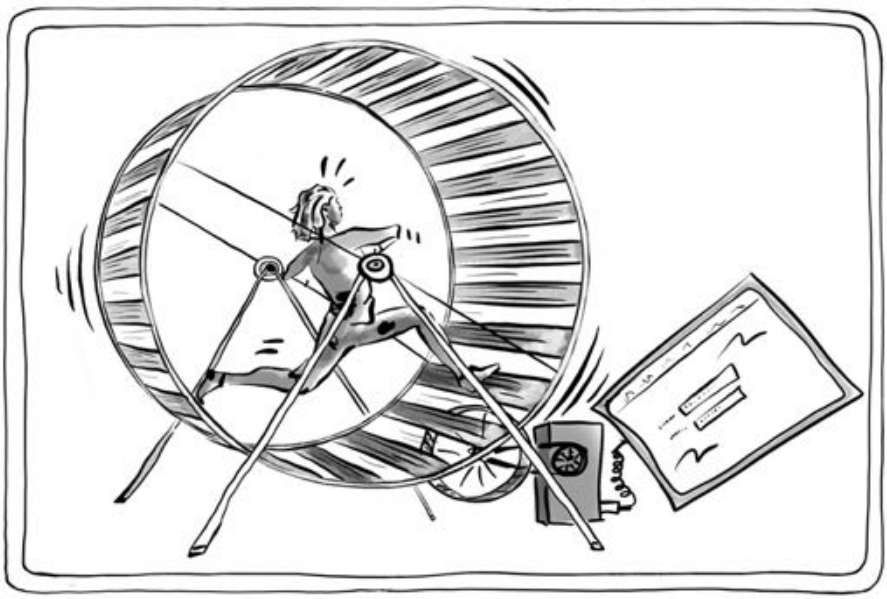
- Finding a guide or a mentor (community worker, boss, colleague, family member) to help them figure out how to tackle the system and services they are struggling with. These might include understanding the benefits of the system, how to navigate the priorities and conditions of service, and learning to trust in the goals and capabilities of the technology. This can lead to challenges for technological security because social proxies and shadow users start to play a part in digital interactions.

- Gaming the system: Twist the system to realise benefits that matter to you. For example withhold or adjust information that you feel might disadvantage you. The more irregularities there are to practices and behaviours, the more volatile the system.

- Opting out and possibly create an alternative system. This, at the very least, depletes the market for the service; but in certain essential services, however, such as housing, education, welfare, employment and healthcare, this can have catastrophic results for the individual, and create a crisis that services have to respond to at a later date.

These responses to exclusion are reasoned from the assumption that the system is designed to exclude, and that the system is in some way hostile to the users of the system. They can also be embodied responses to a sense of being attacked or alienated by the system. These courses of action can have profound impacts on the effectiveness of the technological security.

The research undertaken from the VOME project onwards revealed that people's worldview of security is not top down, but is a view constructed in their everyday lived experience, and from their internal security dialogue. In the following two sections, two alternative security



Security technologies sometimes remove individual choice

views are presented that have their roots in two different ontological positions: everyday security and ontological security.

4.3 Shifting Perspective to the Everyday

The intersections between technological security and embodied forms of security come into view when considering security through the lens of the everyday. Shifting to the perspective of the everyday, the protection and support afforded by technological security is limited, but is supplemented by trust relations and a sense of security from identity.

Digital technologies are an intimate part of our lives

Despite the fact that individuals are increasingly asked to play a part in national security strategies, the views of non-elites are rarely sought by governments (Vaughan-Williams and Stevens, 2016). Instead, security risks are quantified and put into

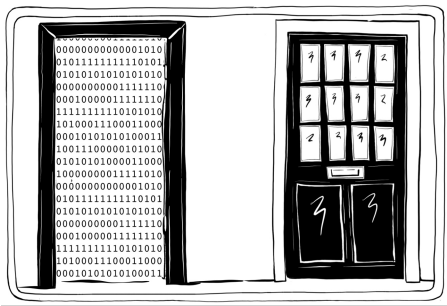
national risk registers (Vaughan-Williams and Stevens, 2016) without considering how people conceptualise threat and [in]security.

At the same time, government narratives around security - and cybersecurity in particular - become increasingly judgemental on issues of non-compliance with government security guidance (MacEwan, 2017). Vaughan-Williams and Stevens (2016) emphasise that when an everyday, non-elite understanding of security comes to the fore, it has the potential to politicise a threat or an issue that has previously been presented as un-biased fact. It does this by highlighting how the issue emerges from power imbalances and from lack of access to resources or other networks of power. This is termed *"everyday security"*. Studies of everyday security have shown (Vaughan-Williams and Stevens, 2016) that the most important site of security to an individual is themselves or their families. These studies show that some non-elite framings of security re-enforce the elite framings. There is often a complex interplay between the two forms (elite and non-elite) of security framing that needs to be understood in order to determine which security controls are likely to be effective as a form of protection, and which elite security framings need to be adjusted.

The binaries upon which much of technological security are grounded are difficult to apply in the complexities of the lived experience of everyday life. Technologies and practices have different meanings in different contexts, and what is deemed secure and insecure emerges from those different meanings. Technological security viewed through the lens of the everyday, lived experience is complex, riddled with contradictions and a constant process of negotiation and exploration. The everyday is not only about the certain practices and issues that are often not typically regarded as political, but it can also be understood in a sensory way. For example, French sociologist, Henri Lefebvre, highlights two conceptualisations of the everyday: one that focuses on the rhythms and cycles of our days and nights and natural world and one that accentuates the routines work and consumption (Lefebvre and Levich, 1987). In this sense, the notion of everyday is linked to the idea of repetitive, mundane practices, and is also embedded in the idea of rhythm and routine which can be used to connect systems in everyday life. Such routines can of course be digitally-mediated and share and

Security technologies mediate many of our day-to-day interactions

protect information. Lefebvre goes on to explain that *"[t]he everyday can therefore be defined as a set of functions which connect and join together systems that might appear to be distinct"* (Lefebvre and Levich, 1987). This perspective makes visible spaces in which previously unseen issues come to the fore and take on political meaning.



Security technologies control access to our private spaces

In international relations, studies of the everyday include the political agency of the non-elites or what are sometimes termed *"the common people"* (Guillaume and Huysmans, 2019). Security issues are framed in terms of the personal (Guillaume and Huysmans, 2019), and as a result factors that are not typically part of any analytical frame - such as gender, resistance, social and political capabilities - are revealed to influence not only the personal but also the international.

One way of conceptualising an everyday perspective is that it looks at an issue horizontally rather than vertically, or top-down (Guillaume and Huysmans, 2019). Aligned to this, Bissell (2013) argues that the everyday can also be understood in spatial terms by conceptualising different types of connections: for example, a linear connection between two points, such as an individual logging into a system, and a web of connections that are made of up of small, routine interactions. In digital terms, the web of connections is an important route to digital access. This lens enables a view on an issue that unfolds through everyday enactments and entanglements, and it is through this unfolding that embodied responses to technology emerge. Security issues when understood from this perspective are fleeting and emergent, and will foreground and background as they form and re-form. This spatial view is particularly important because it reveals the spaces *around* interactions with technology, and it is in these spaces that securing processes and practices, upon which the success of security controls are contingent (Burdon and Coles-Kemp, 2019), take place.

The everyday opens up the need for materialist-pluralist responses where technologies support many types of security, again, some of which might conflict. This perspective offers a much clearer view of how people engage with technology, and how technology aligns or conflicts with everyday life. However, the perspective of the everyday does not fully capture the embodied security experience. To achieve this, we need to bring in an ontological security position.

4.4 Shifting Perspective to the Self

Social routines, identity and trust are important security mechanisms

Much of how individuals respond to everyday security issues is shaped by an embodied and internalised sense of security. Ontological security is the embodied sense of security that influences how security is felt and experienced by an individual. It helps to shape our security practices, and the ways we perceive security threats. As a result it is central to

the way we understand digital security. Everyday security provides the routines and repetition that help to foster an ontological security.

Ontological security manifests itself in the routinisation of life to prevent it from tipping into chaos, enabling individuals to have the confidence to go about their daily activities. This understanding of security as an experience and as a feeling is connected to our understanding of security practice. For example, non-compliant practices are often routinised technological practices designed to cope with complex and unpredictable situations (Singh *et al.*, 2007).

Security is also an embodied experience

Croft (2012), quoted by Croft and Vaughan-Williams (2017), describes ontological security as follows: *"the key elements of an ontological security framework are a biographical continuity, a cocoon of trust relations, self-integrity and dread, all of which apply at the level of the individual, and all of which are constructed intersubjectively"*. Ontological security therefore manifests itself in the everyday practices designed to build and maintain routines that enable an individual to benefit from social forms of security, such as trust relationships, and to cope with complex and uncertain situations. This calls for a broader conceptualisation of trust, one that builds on sociological understandings of trust as a *"social reality"* (Lewis and Weigert, 1985) where trust is established partly through routines (Mollering, 2006).

Ontological security is strengthened not through controls and technologies but through acts of care. Care creates conditions in which trust can be reproduced by recursively enacting social practices across space and time, and it enables people to integrate systems into their everyday lives. Care can be broken down into: recognising a need for care; caring for, *i.e.* taking responsibility to meet that need; care giving, *i.e.* the actual physical work of providing care; and, finally, care receiving, *i.e.* the evaluation of how well the care provided had met the caring need. Nevertheless, issues can still arise *"from conflicting responsibilities rather than from competing rights and requires for its resolution a mode of thinking that is contextual and narrative rather than formal and abstract"* (Tronto, 1993, p. 78). This gives an alternative start point for thinking about security technologies. Care as a start point for a digital security approach is considered by Kocksch *et al.* (2018) when re-framing technological security as careful practices of collaborative tinkering and experimentation. In this paper they argue that IT security is an enmeshed bundle of both care and cure practices, but that the care work is often invisible and badly rewarded, and yet without it, IT security strategies are unlikely to be successful (Burdon and Coles-Kemp, 2019).

It is this contextual and narrative form of security that researchers found when in the field during VOME. It is one that positions a materialist-dualist ontology within a wider, more inclusive and more accessible idealist-pluralist security position.

4.5 Concluding Comments

The three perspectives presented in this chapter are interconnected and together they provide explanations as to why technological security is experienced in the ways that it is. From a top down perspective, security provides stability, reliability and consistency in the order and structures that are used to protect states, society and technology. However, when people conduct their lives in a digitally-mediated society, whilst the top down structures of security offer stability, the top down view does not address the challenges when different forms of security interact with each other. To achieve this requires a means of identifying the

intersectional security issues in the context of people's everyday lived experience and of developing contextual and narrative forms of security that can lead the response to those issues. Theories of everyday security and ontological security help to bring these intersections into view, and open up the space for a contextual and narrative form of security that takes place in the social spaces around technological interaction.

In the next chapter, Digital Civics, a branch of Human-Computer Interaction, is examined as one frame through which a contextual and narrative form of security can be unpacked and further developed. This frame is also complemented by the view from the Practice paradigm, to see how a focus on practice shines a light on the intersections between securities, and identifies a broader form of technological security at work in those intersections.

The version of record is available at: http://dx.doi.org/10.1561/1800000030

5

Digital Civics, A Practice-Lens and Digital Security

Our projects have always shone a light on the fact that whilst technological security is focused on the protection of data and technology, this does not necessarily secure the people who use the technology as they go about their everyday lives in a digitally-mediated society (UKRI, 2020). Political and social theories of security introduce many more forms of security, offer a variety of approaches to respond to security issues and present different ways of constructing security problems. Shifting perspective to the everyday lived experience, it becomes clear that the security challenges that people focus on are an enmeshed composition of many forms of secu-

Digital civics connects technology to a wider social context

rity. For example, when working with families separated by prison, we discovered that the question of information access in the context of family support services are often bound up in the wider challenge of managing the relationship with the individual in prison. The groups that we worked with on this project managed and maintained this relationship through the prison visiting journey; the support services and the concomitant information sharing and protection practices were understood as part of the wider challenge of maintaining the security of family relationships.

Community capacity building is at the heart of digital civics

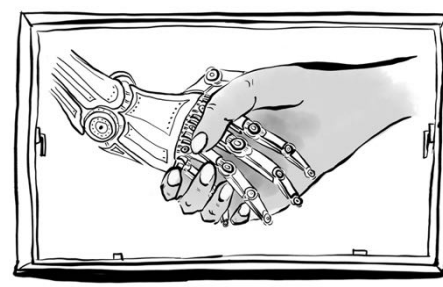
Understanding how people identify and respond to issues in a digitally-mediated setting is core to Human Computer Interaction (HCI). For example, the study of digital civics, a form of HCI with a particular focus on the socio-economic-political processes at work in digital settings, together with the study of practices in and around technology within a setting, help us to better understand why digital technology is used in the ways that it is. In this chapter, we show how a wider lens on technology use illuminates how people use a wide range of sociotechnical resources, networks of power and information sharing and protection practices to respond to security issues in their everyday lives. This wider lens brings a number of the concepts and themes that appear in social and political theories of security into direct conversation with the design of digital services and products. For example the social contract, the protection of the state, digital protection as a human right and marginalised voices are all germane to understanding the different security dimensions of a digitally-mediated

socio-economic-political setting. In connecting technological security to this wider sociotechnical perspective, a digital security paradigm emerges to give a more complete understanding of what it means to both be secure and practice security in a digitally-mediated setting.

The digital civics agenda advocates technologies that support different forms of civic engagement and process (Olivier and Wright, 2015; Taylor *et al.*, 2015; McCarthy and Wright, 2004; Asad *et al.*, 2017; Puussaar *et al.*, 2019). Olivier and Wright (2015) in their introduction to digital civics highlight the importance of designing for citizens rather than for consumers. In making this move from consumers to citizens, Olivier and Wright bring to the fore debates about the impact of digital research and practice on people and also on the place in which they live, work or visit. They use the term *digital civics* to refer to research and practice that uses digital technologies to empower people and set out three key objectives for digital civics:

- Create relational rather than transactional public services.
- Create a model of citizen-led service commissioning.
- Develop long-term engagements with a full range of stakeholders to build relational models of public services.

Whilst the notion of civics and the idea of digital empowerment is not without its challenges, as a body of work digital civics scholarship is one means of recognising how people identify and mobilise responses to security issues in their everyday lives and acknowledging a much broader canvass of security actions.



Digital technologies can support relational services

The digitalisation of government services has become a prominent means of service provision and is increasingly becoming the point at which individual and state meet. Many public services are now digital by default. In the UK, this transformation began in 2012 when the UK Government launched a Digital-by-Default

initiative to bring government departments and several hundred public body under one website, `www.gov.uk` (McLoughlin and Wilson, 2013; HMG, 2012). The aim was to create a single point of access for many of the government services such as registering to vote, applying for driving license, and claiming welfare (HMG, 2019). Initially a strategy framed as one of promoting citizen choice, in the era of austerity, also provided a means of cost savings through the reduction of face to face support and the re-design of services.

Technological security forms an important part of the digital by default story, as it is the main means through which government services identify people accessing services and the means through which access to public resources are controlled. At the same time, such technology also regulates access to services that are important for the safety and well-being of individuals and communities as well as contributing to an individual's economic, social, employment, food and personal securities.

5.1 Technology Through a Political and Social Lens

Digital civics is a cross-disciplinary area of research and practice (Vlachokyriakos *et al.*, 2016) and its focus is technology use as part of civic engagement and civic responses to issues. There are many actors involved in civic engagement and these include organisations, groups and individuals contributing to the response. Digital civics is sometimes cast as a synthesis of studies in community informatics, digital democracy and smart cities (Asad *et al.*, 2017). It is described as having two components: a turn to participatory systems and a focus on relational interaction (Corbett and Le Dantec, 2018a). It also shares a sense of inclusivity and attends to the issues of groups that are typically overlooked in technology design. For example, Schorch *et al.* (2016) examine the issues and possible responses for elderly informal caregivers, a group that is typically not designed for and whilst Müller *et al.* (2012) have attended to the issues experienced by elderly residents in care homes.

Civic responses to issues have the following properties (Le Dantec, 2016):

- civic responses cross many boundaries, blurring the roles of actors;
- projects or products that must meet the expectations of a diverse and fluid range of actors;
- demands at all levels of production, distribution, reception and control.

These complexities add another dimension to security responses. Whilst the engineering and technology design approaches outlined in the previous chapter are still necessary to develop and deploy technologies that are reliable, the technologies are deployed in open systems with the complexities described above. Relational services are services that are based on methods of relationship building and are one means of flexibly responding to these complexities. Open systems are woven together through everyday rhythms and routines and rely on relational services and interactions that re-cast the projects and products in different lights depending on the issues at hand. Relational services encourage positive forms of security grounded in trust and collaboration.

Relationship building re-cast products and services in different lights

Digital civics has a broad agenda that encompasses a number of different areas of scholarly focus. However, woven through the agenda is the theme of supporting, scaffolding and building capacity within communities

to respond to lived issues through the use of technology (Peacock and Al-Shahrabi, n.d.). Following from this, four key areas of scholarly focus in digital civics are:

- Relational design.
- Community engagement.
- Trust.
- Publics.

These different areas of focus are interwoven and whilst a study may focus on, for example, issues of trust, the relational design of processes and community engagement practices will also be present in the study setting and findings. Similarly the idea of publics which is the formation of a multi-stakeholder group of individuals that are connected through trust relationship and that, as a group, identify and respond to issues. In the following sections, these areas of scholarly focus are unpacked.

It is important to note that, like technological security, digital civics blends theory and academic inquiry with practice. As is often the case with security studies, the digital civics community is composed of academic and non-academic stakeholders. As a result, this monograph refers to digital civics as both scholarship *and* practice.

5.1.1 Relational Design

Central to the understanding of digital civics is the shift from transactional service models to relational service models (Vlachokyriakos *et al.*, 2016; Olivier and Wright, 2015). A digital civics perspective contends that it is the relations rather than the transactions that contribute most to civic life (Asad *et al.*, 2017). By configuring service models to focus on relational forms of service, the aim is to change the power relationships between people, communities and the state. Transactional services in the context of digital services foreground an exchange between citizens and state, where governmental agencies and authorities request specific, pre-determined information in return for a public service defined by the government.

In contrast, relational services are those that are based on methods of relationship building that are used to respond to problems defined by the service community (users and providers) as a whole. Muir and Parker (2014) point out that many public services are responding to complex social problems and require both transactional and relational services to meet the needs of people. Relational services are used to determine people's needs and develop the capabilities necessary to benefit from transactional services. In HCI, a relational focus might include, for example, digital tools that can support individuals to envision, campaign for and produce responses to particular issues (Vlachokyriakos *et al.*, 2016). Associated with this focus on a relational approach is an acknowledgement that relational services have different economic models underpinning them and can build a connection between the service and the place in which they are envisioned, produced and deployed.

Relational services reconfigure power relationships

5.1.2 Community Engagement

Allied with a relational approach is the design and execution of community engagement. Community engagement has many modes of execution so that the engagement process is able to adapt and survive the often rapid and unpredictable changes to municipal organisations (Asad *et al.*, 2017). An important aspect of digital civics is therefore to develop methods and processes of engagement that enable communities to set-up and sustain meaningful engagement in order to bring about positive change. To achieve this, community engagement processes need to engender empathy and understanding rather than determine what an engagement is or how it is to be achieved (Asad *et al.*, 2017).

Studies of community engagement have shown that the use of technology is diverse (Lovejoy and Saxton, 2012) and typically uses re-purposed everyday technologies (Lovejoy and Saxton, 2012; Asad *et al.*, 2017; Le Dantec, 2012). For example, Lopez *et al.* (2012) show that non-profits use microblogging technologies such as Twitter to great effect. The work identified that microblogging was used by not-for-profits for three reasons: information sharing, community building, maintenance, and action. The work showed that microblogging was used in four ways for community building and maintenance: giving recognition and thanks, acknowledgement of current events, responses to public reply messages, and public response solicitations. Le Dantec (2012) reveals similar categories in a study of participation and use of an online message board. Such studies also show that community engagement is a means of building social capital which can be defined as *"the value derived from being a member of a society or community"* (Huysman, Wulf, *et al.*, 2004, p. 1) and this social capital helps to build stronger community engagement.

5.1.3 Trust

Relational services and community engagement are a means of engendering and maintaining trust relationships and building social capital. The design of these approaches has to take into account levels of mistrust and develop techniques to operate in spaces where there is an absence of trust (Corbett and Le Dantec, 2018a).

Digital civics foregrounds trust

Trust therefore is a key theme in digital civics research. Digital civics places emphasis on dialogue, empowerment and participation, but distrust often characterises the relationships that these activities are designed to develop (Corbett and Le Dantec, 2018a). Therefore, trust building and trust maintenance in relationships between stakeholders in community engagement is a dominant theme in digital civics research and practice. The focus of this work is to support trust in community engagement. Trust or its absence plays a crucial role in civic engagement (Asad *et al.*, 2017; Crivellaro *et al.*, 2014; Corbett and Le Dantec, 2018a; Harding *et al.*, 2015).

Corbett and Le Dantec (2018a) identified four main strategies for supporting trust building and maintenance in digital civics:

- Historicizing engagement: Barriers to engagement come from events in the past and identifying these experiences is important for understanding a particular trust assessment.
- Focusing on experience: Building trust within the community engagement process can be adversely affected by negative past experiences of engagements.
- Mediating expectations: Creating an expectation that community benefit will be realised, despite uncertainty and challenges helps to build trust.
- Preserving institutional relationships: Personnel churn in institutions and constant organisational restructuring is a key challenge to maintaining trust, and therefore it is important to design ways and means of preserving relationships with those institutions.

Each one of these strategies has a direct impact on how people experience security technologies and provides ways of examining why some people have negative experiences. The implications of mistrust are also

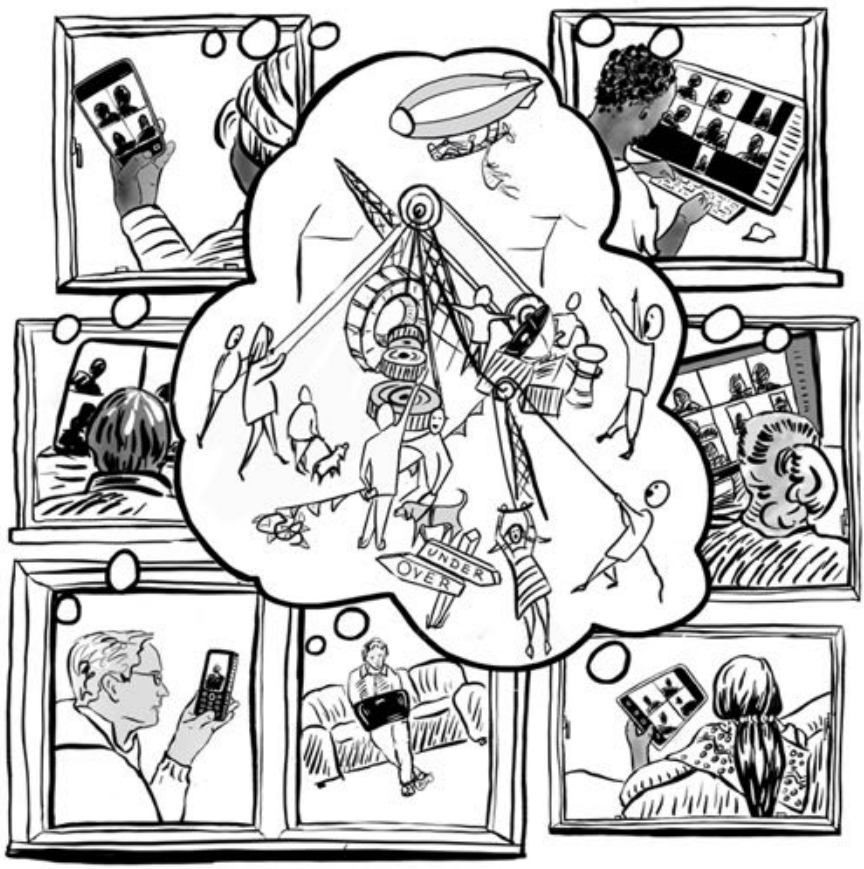
important to highlight because often the challenges that a digital civics approach responds to arise because of pre-existing mistrust conditions. For example, technological controls, such as those used to facilitate digitalised welfare programmes, might serve to highlight the mistrust the state might feel towards the claimant.

5.2 Digital Civics and Publics

The notion of publics is often deployed in digital civics to structure a technological approach in complex environments with multiple stakeholders. Publics are a diverse group of stakeholders bound by common issues (Le Dantec, 2012). The American philosopher John Dewey (Dewey and Rogers, 2012) argued that a public does not pre-exist but is formed when multiple stakeholders identify and express a common concern and then work together to respond that concern. The issues that are identified and responded to cross stakeholder boundaries and involve working together to successfully respond to the issue. HCI scholar Le Dantec (2012) argues that the Deweyan notion of publics is highly relevant to the design of interactive technologies because it involves the identification of issues that affect multiple groups and communities and require collaborative working.

The shift towards the construction of technology through the lens of publics and away from a focus solely on technology as a product is an important one because it puts a focus on the engagement throughout the life cycle of a product, and not only concentrates research and practice on current use but also future use (Le Dantec, 2012). Publics are made up of three elements: attachments, issues, and infrastructure (Le Dantec, 2016). Attachments are a bonding of actors, artefacts and institutions. Attachments are inherently conflicted, for example sharing information vs. hiding information, making information open and accessible vs. regulating access to information. Dependencies and commitments form an attachment and are a means of responding to particular issues. Publics marshal social and technical resources to respond to issues and this marshalling is termed "infrastructuring". When addressing design-in-use, *i.e.* the ways in which a product's meaning and use is adjusted through the process of use, infrastructuring is a key concept. Infrastructuring is

the appropriation of technical and social infrastructures to develop and sustain the response to an issue (Le Dantec, 2012). Through the process of infrastructuring, publics are constituted and refined (Le Dantec, 2012).



Infrastructuring brings together many stakeholders

Digital civics literature often acknowledges that developing and sustaining a response to an issue can be conflicted (Crivellaro *et al.*, 2015), and attachments can be developed through contestation as well as goal and value alignment. The process of infrastructuring is also important in this respect because stakeholders are not fixed and institutional stakeholders often change (Asad *et al.*, 2017). This churn might be in terms of personnel but at the institutional level might also be in terms

of a change in policy direction or in policy constraint. This fluidity and change can result in adjustments to goal and value alignment within stakeholder groups and can lead to contestation and friction between stakeholder groups. Publics are therefore dynamic, living groups that require on-going and adaptable forms of community engagement.

The concept of publics is useful for understanding the wider space in which security issues are responded to. Identifying how attachments are formed, who and what are included in an attachment and the information that flows through an attachment is an important means of understanding how security issues are framed and where security knowledge is created. Security responses will largely take place as part of infrastructuring rather than in the direct interaction between an individual and a digital service as this is where securing processes and activities take place.

5.3 Digital Civics and Security

Issues of security are threaded explicitly and implicitly through the projects linked to the study of digital civics. The digital civics agenda has largely concentrated on issues of safety and security through the lens of trust (Corbett and Le Dantec, 2018b; Le Dantec, 2016). However, the political meanings of security technologies have also been examined by Castro Leal *et al.* (2019) where the ambiguities of technology in a guerilla warfare setting were analysed and collective, social responses to the emergent risks presented.

Whilst security technologies play a vital role in ensuring the reliability of digital technologies and services, trust and resilience are built through the social elements of infrastructuring and in the bonds that are formed between stakeholders to respond to security issues. Digital civics creates a lens through which security practitioners and researchers can both explore and work with these spaces around the technology to develop more contextual and narrative forms of security that supports and includes people in security action.

The lens of publics opens up many more opportunities for the deployment of security interventions, and for the design of security responses that blends different security logics and ontologies. For ex-

ample, an idealist-pluralist framework for security might be introduced into the community engagement processes and the design of the relational services. Equally, if technologies are understood as a constellation of products rather than as individual products, the technologies as a constellation might offer many more ontological combinations.

The digital civics focus on the identification of issues and the formation of responses to those issues, aligns with a social constructionist approach to security that both reorders the security issues and also critically challenges the security issues regarded as legitimately requiring responses.

Digital civics offers multiple security views

By examining technological security through the lens of digital civics, the politics of security, and therefore security technologies, are also foregrounded. This is because at the heart of digital civics is the use of the digital to re-design the relationship between people and the state. With the digitalisation of services and, more fundamentally, the means by which the state communicates both within its borders and outside its borders, technological security as a practice has indeed been reshaped partly because securities that were once distinct and separate are brought together. This gives rise to a new security paradigm, a digital security that through an understanding of security practices connects technological security to a broader range of social and political securities.

Technological security is thus no longer about solely protecting technology designed for a restricted purpose with restricted meaning, but is now called upon to protect both the technology and the people who use that technology in a seemingly infinite number of contexts and for a limitless number of purposes. An approach to security that is technologically mediated and that acknowledges the economic, political and social dimensions of securing, is termed **digital security**, denoting this more expansive form of technological security.

5.3.1 The Practice Paradigm

Implicitly, digital civics places an emphasis on practices of information sharing and protection but these practices are also embedded in the discourses of trust, infrastructuring and publics. However, to understand the securities at work in digitally-mediated situations, a Practice paradigm can be used to examine how information is shared and protected in these settings. Practices are for digital security scholars one of the main hinges through which security technologies are connected to the broader sociotechnical, political and economic complex that is the focus of digital civics thinking.

Kuutti (2013) described practices as relatively stable performances that enable things to get done. There are numerous schools of thought on what constitutes practice but Nicolini (2012) identifies five commonalities of practice theory:

- Practice view on life.
- The critical role of materiality of human bodies and artifacts.
- Roles for both agency and actors that differ to the roles played in traditional theories.
- Understanding knowledge as a capability not simply as something that is transferred from one person to another.
- Centrality of interests and motivation in all human action and they shape and influence the focus of power in those actions.

These ways of understanding practice create a lens through which information sharing and protection practices can be examined. This lens enables security scholars to bring together the materiality of security technologies with the doing of security. It also enables a means of connecting the processes of securing with the materiality of protection. This is because it provides a means of identifying and theorising about the creation of shared goals, orderings of values and the embodied reactions to an access control system. Schmidt (2014) summarises practice as the unity of the capacity to make and act.

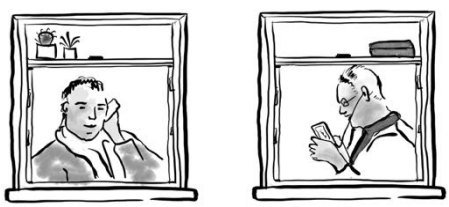
Using a practice lens opens up the surface of analysis. This is because the study of practices emphasise the fabric of action, the knowledge and reasoning that surrounds the action and the context in which it takes place (Castellani 2009). The surface of analysis also situates practice within a temporality. Kuutti and Bannon (2014) put forward that the study opens up the surface of analysis still further by acknowledging:

- Practices are situated in time and space.
- Practices are dependent on the surrounding material and cultural environment.
- Material and cultural environment are woven into the practice.

By harnessing a practice focus to digital civics, a detailed picture emerges of how and why people conceptualise digital security in the way that they do. From this understanding, information sharing and protection actions become something that can be both theorised and engaged with.

5.3.2 Foregrounding Relational Forms of Security

It could be argued that the security goals of technological security controls causes technologists to focus on exclusion, control and mistrust when designing technological systems (Gürses *et al.*, 2016; Coles-Kemp *et al.*, 2018). It could also be argued that technological controls might further exacerbate mistrust. For example, phishing awareness programmes that result in employers phishing their own employees to highlight the dangers of phishing, can result in mistrust of the employer and fear of technological controls in a work setting (Ashenden, 2016).



Positive security is as much about listening as it is about action

Digital civics instead foregrounds responses that are grounded in relational services that build and maintain numerous forms of trust. A relational service focus offers a form of security that is more inclusive and has its roots in notions of care, trust and reciprocity. The relevance

of this re-orientation is discussed by Kocksch *et al.* (2018) in the context of IT security practice, where such professional practices are presented as relational processes and practices.

The digital civics perspective with its focus on enablement is also better aligned with a positive view of security. Roe (2008) presented an overview of the two positions of positive and negative security. In its positive conceptualisation, people live free from fear and enabled to live their everyday lives. In its negative conceptualisation, people are protected from harms. Positive security promotes a relationship with digital technology and services that enables people to successfully go about their day-to-day activities, conditions which are necessary for technological security controls to be effective. Trust is central to the positive conceptualisation of security and is needed so that individuals feel secure in their identities, secure in the relationships that surround them and secure in their environment.

Trust is central to effective technological security

Whilst usable security researchers have long argued that trust is a central component of effective security (Flechais *et al.*, 2005; Riegelsberger *et al.*, 2005; Kirlappos *et al.*, 2014), the focus has primarily been on trust in the technology. Central to this is the understanding that the relationship between trust and confidence, and knowing when to promote either or both, is an important element of interaction design. Kiran and Verbeek (2010) argue that confidence takes the form of people trusting themselves in their ability to use technology and to take part in technologically-mediated interaction. Yet this confidence can be hard to find where advice is conflicted and difficult to follow (Renaud, 2011; Renaud *et al.*, 2018). Sociologist Luhmann (2000) differentiates between the concepts of trust, familiarity and confidence. In this sense, trust is the decision to engage in the face of perceived risk, whereas confidence takes place where actions are executed under the assumption that expectations will be met. Familiarity, on the other hand, results in actions taking place as a form of

routinisation. However, understanding these distinctions in the context of digital interaction is complex and contested as Web Science studies highlight, and therefore trust cannot simply be produced *"by creating the right tools and technologies"* (Berners-Lee *et al.*, 2006, p.89). This is particularly true in the case of security technologies as technological security is the seam through which the security interests of the state and other institutions of power come into direct conversation with the security of the individual.

Therefore, trust in the institutions of power, as well as trust in the providers of the technology and services on behalf of those institutions, play a significant role in whether security technologies are trusted or not. Knowles and Hanson (2018) undertook a study with older adults and concluded that articulating distrust in a technology or system was a shorthand for a wider disagreement with the values represented by that system. In this case, distrust took the form of resisting behaviours and disengagement behaviours as a means of articulating this disagreement with the values represented by the system.

The work of Knowles and Hanson (2018) highlights the importance of recognising the relevance of value alignment when understanding digital practices, including security practices. A trust-led, participatory approach that uses relational services to build and maintain trust, align values of stakeholders with the values of a system and use engagement processes to respond to value clashes are what Smith (2005) describes as securing processes (Burdon and Coles-Kemp, 2019). Securing is also an important aspect of positive security and relies on relational services, which are services that foreground human–to–human interaction (Cipolla, 2009).

5.4 From Technological Security to Digital Security

Digitalisation complicates our understanding of how technological security might work in a digitally-mediated society by simultaneously redefining the social, political and economic structures upon which technological security relies, at the same time as demanding new forms of technological security and new ways of thinking of technological security practice.

The digital civics agenda invites security scholars to use a practice lens to consider security through a relational model that is trust-led, and where issues are not pre-defined but are identified as part of community engagement and where stakeholder groups form clusters around issues. This way of thinking about technology and how it relates to people is very different from the more solution-oriented approach to technological security. The digital civics agenda creates spaces in which stakeholder groups are empowered to identify security issues, and to use their social networks and a blend of social and technological infrastructures to respond to those security issues. This form of issues-led security requires the development and nurturing of trust relationships between stakeholders and the use of social bonds and the development of social capital to resolve some of the security challenges that emerge when responding to civic issues.

Table 5.1: Comparison of technological and digital security

Form of Security	Attribute
Technological Security	Negative-Positive
	Transactional
	Pre-defined
Digital Security	Positive-Negative
	Relational
	Emergent

As Table 5.1 summarises, technological security is led with a negative security (protective) focus, placing a security emphasis on transactional services related to information access and responding to pre-defined security problems. Whereas digital security is led with a positive security (enablement) focus, placing a security emphasis on the relational support provided by social networks and responding to issues that emerge as a result of community engagement. A focus on practices and the complex ways in which practices create complex sociotechnical constellations to respond to security issues generate granular and more complete understandings of what digital security is and how it might be shaped.

5.5 Concluding Comments

Developing a form of security that speaks to both social and technological securities, and where the intersections of these securities are recognised, requires a security mindset that recognises security practices that enable both positive and negative forms of security. Relational processes work along these intersections and respond to issues identified by stakeholder groups that form in response to issues and concerns. Through the lens of practice and the wider sociotechnical perspective of digital civics, a new form of sociotechnical security emerges that is relational, collaborative and ground-up. This is a form of security that draws on social and political theories of security as well as technological security design and practice. This is in fact a digital security that supports the digital civics mission.

In the next chapter, digital security is presented as a practice-based approach that is grounded in the participatory and democratising practices of digital civics.

6

Digital Security: Practice and Methods

Drawing on the engagement and practice principles found in digital civics, this chapter sets out an approach and possible methods that can be used to both practice and research matters of digital security. From the VOME project onwards (UKRI, 2020), we realised that to observe and understand the phenomena relevant to our research questions required a form of research attentive to the context in which security technologies were being used. We also realised that the phenomena that we wanted to reach were not readily observable, and we needed to develop ways of researching that encouraged our participants to guide us to the phenomena, and explore them with us. In developing these approaches, we discovered that we needed to develop a research and engagement approach that moved us towards a more equal distribution of power between researchers and participants, such that both sides could trust each other to explore the unknown.

Exploring the unknown together

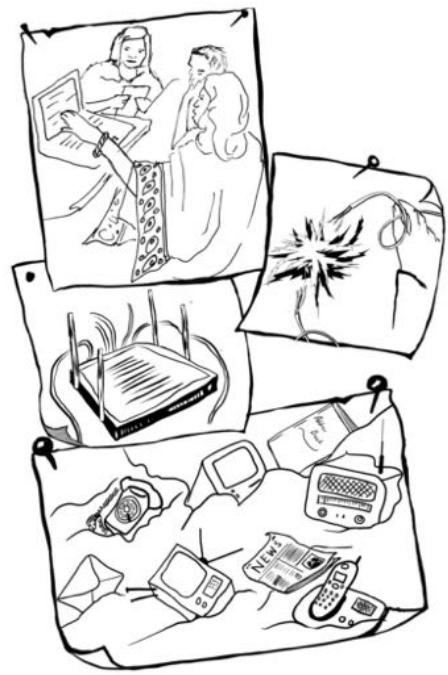
The approach and methods set out in this chapter are grounded in participatory design, design thinking and digital inclusion, and show how using an approach not typically associated with security technology design and practice reveals a different set of issues and ways of practising security. We examine how a practice lens influences the design of an engagement, and show how our methods can be used to illuminate the information sharing and protection practices around and within digitally-mediated interaction.

6.1 Contextual Design

Zurko and Simon (1996) demonstrated that understanding the social aspects of HCI requires alternative research methods, and different types of engagement. This work outlines the importance of contextual design methods that offer a deep dive into people's digital habits and practices. Zurko and Simon (1996) draw from the work of Wixon *et al.* (1990) on contextual design, which examines why traditional scientific methods, often quantitative in nature, drawn from mathematics and the mathematical sciences, *"have failed to provide relevant information for a number of the necessary elements of product development such as: needs analysis, requirements definition and interface design"* (Wixon *et al.*, 1990, p. 329). Wixon *et al.* (1990, p. 331) set out the basis of contextual design being built on a form of contextual inquiry, one that collects data

in partnership with technology users in the context of a person's work. In this context, contextual design is contextual work that incorporates interpretation together with an understanding of technology, to develop an understanding of people's needs as a basis for technology design.

The pioneers of contextual design in HCI argued that design principles needed to be understood from the perspective of the people using the technology (Wixon *et al.*, 1990, p. 334). This argument is equally true for the design of security technology and services, given that it is important to understand how people understand, experience and practice different forms of security in digital contexts (Coles-Kemp and Ashenden, 2012). This requires the use of a range of qualitative research methods which are similar to the context design and inquiry methods cited by the HCI usability pioneers (Zurko and Simon, 1996; Wixon *et al.*, 1990). Dunn Cavelty (2013) identified the importance of considering how the methods of engagement shape the nature of the interaction with research participants and, therefore, the types and qualities of data that are elicited as a result.



Methods of engagement shape the interactions

Contextual technology design often attends to the values of the intended user communities as well as to those of the technology or service provider. Whilst following a value sensitive design approach is relatively uncommon in security technology design, it has been proposed on occasion. For example, Friedman *et al.* (2002) examined how value sensitive design can be used in the design of informed consent controls in the context of browser design. In this article they also argue that informed consent is an important human value, but it can only be realised in an on-line setting if browsers (and other interface technologies)

implement technical mechanisms related to informing and obtaining consent for information gathering and sharing.

Democratic forms of research participation is one of the distinctive features of digital civics practice and scholarship. Participant engagement in academic research is not often prominently featured in research design (Arcury and Quandt, 1999; Chavez *et al.*, 2017). Whilst ethnographic studies have participant engagement techniques deeply embedded into their research design, these studies are often peripheral to the mainstream of many disciplines. Participant engagement is more typically framed in terms of the representativeness of the participant sample, or the demographic selected not in terms of the methods used to achieve engagement or their impact on the quality or types of data collected (Coles-Kemp and Stang, 2019).

The following sections set out some of the options available for technology studies that focus on people and their use of technology rather, than on technology and how people use it. The chapter then moves to set out an approach to enables researchers and practitioners to focus on the digital security needs of people; a creative security approach.

6.1.1 User-Centred Design

Listening is a key research skill

Zurko and Simon (1996) highlight the need for research and engagement methods that work together with people, rather than separate from people. Participation is thus central tenet of contextual design (Wixon *et al.*, 1990). There are various forms of people-centred design, ranging from user-centred design to participatory design.

User-centred design has become a generally accepted approach in technology design (Mattelmäki *et al.*, 2006). User-centred design aims

to understand who the users are, what they do, and what kinds of attitudes they may have. A lot of care and attention has to be given to working with users in the right way, with the right methods, in the right context and at the right time (Wensveen *et al.*, 2000). Mattelmäki *et al.* (2006) argue that there are three ways to engage with user experiences:

- Listen to users.
- Observe what they do.
- Encourage them to express what their aspirations and experiences are.

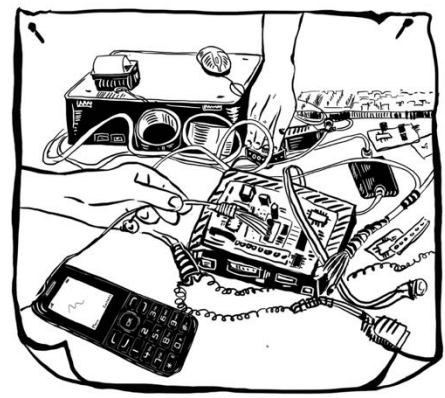
Getting to know users and to understand the potential contexts in which they use technology is often the start point for user-centred design (Wensveen *et al.*, 2000). To do this, traditional qualitative methods from social sciences are often called upon. These may include contextual inquiry, observations, interviews, questionnaires and focus groups (Mattelmäki *et al.*, 2006, p. 28). The more ephemeral the experience - or the more precarious the environment and abstract the concepts - the more careful the design of the engagement. Security is a particularly challenging interaction to capture because security is both interaction with technology, but also a felt experience, and the security meaning of the interaction has to be understood in the context of the felt experience. As a result, observation and discussion have limited success in deriving the whole security experience. For this, we need to look at approaches that create spaces in which people can articulate security as a felt experience, as well as security as an interaction. One such approach is participatory design.

6.1.2 Participatory Design

Whilst usable security has predominantly focused on people-centred design, digital civics has adopted a people-centred approach that focuses on not only the democratisation of technology, but also of the processes used to design technology (not only at the time of initial design, but also in-use).

As Brandt (2006) explains, *"[p]articipatory design implies active involvement of the people designed for and other stakeholders in the design work"*. The author goes on to argue that participation is one of the cornerstones of design. Ehn (2008) argues that by including people who are being designed for in the design work, there is an attempt to anticipate contexts of use that might emerge in people's lived experience before the actual use of the thing that is designed.

Ehn (2008) also refers to *meta design* as design-after-use, where designers and future designers/users envision and anticipate potential design after the initial artefact has been produced. As Vines *et al.* (2013) argues, these two forms of design are often referred to using the one term *participatory design*. The term *design thing* refers to the object of concern in design, the design object and its representatives (the possibilities and concerns that the design object represents) (Ehn, 2008). This term is particularly apt for describing security technologies because the object of concern is a form of security that is not necessarily fully represented by the design object, and which requires an understanding of its *representatives* (for example whilst a file permission might represent access to a file, it can also represent access to a secret or to a document with considerable emotional importance).



Participatory design is the active involvement of people

Both participatory design and meta-design are represented in digital civics; participatory design because it creates spaces of empowerment for potential users of technology to shape technology to respond to the issues and aspirations of their lived experience, and meta-design because it uses the process of infrastructuring to bring together current and future designers and users.

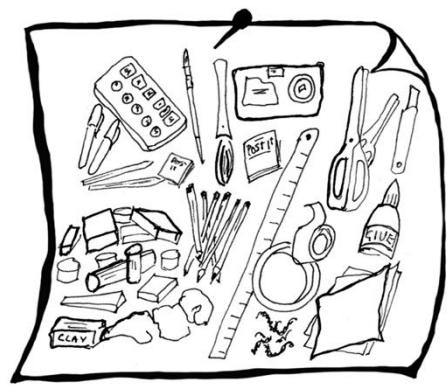
Participatory research has an ever-increasing take-up in HCI research (Vines *et al.*, 2013). It is at the heart of digital civics research and practice because it calls for a democratisation of the technology

design process (Vines *et al.*, 2013). Democratising technology does not only mean increasing the roles, availability and accessibility of technology in everyday life, but also enabling different stakeholder groups to enter into the conversation about where, how and why technology is used (Le Dantec *et al.*, 2010). Participatory design helps to achieve these two democratising goals.

Participatory design democratises research and practice

Participatory design has been a particularly prominent feature of digital civics when examining the impact and design of digital products on the structures, practices and experiences of public life (DiSalvo *et al.*, 2016). Participatory design and, in particular, the innovation of participatory processes and practices, are key to engaging communities who are at the margins of society, and who may appropriate technologies in unanticipated ways (Le Dantec *et al.*, 2010).

It is for this reason that digital civics practice and research often draws on the humanities for inspiration when, for example, designing both the engagement processes and materials (Schofield *et al.*, 2013; Rossitto *et al.*, 2017; Dunphy *et al.*, 2014). For similar reasons, creative citizen technology activities such as hackathons and DIY citizenry activities have also been deployed as forms of participatory engagement (DiSalvo *et al.*, 2014; Shea, 2016).



The humanities inspire participatory research methods

Participatory design is an approach that is able to engage with a wider range of technology users, often able to reach those who are not typically able or willing to engage on the topic. Participatory design

deploys methods and creates spaces in which people are able to reflect on their experiences and articulate their felt experience of working with technologies. However, security technology also represents particular security positions which, in turn, are a defence of a particular order of values. Therefore, it is therefore important that practice and research engagements on the topic of digital security are not only participatory and inclusive, but also use techniques that enable the critical examination of the values that the security technologies represent. This is because the values represented by the security technologies engender particular security responses from those who use the technologies.

6.1.3 Practice Paradigm

The focus of these design approaches often falls on the design of technologies, or of the interactions that happen with these technologies. However, there is typically less attention given to the practices that happen around and between the technologies. This is the focus instead of the *Practice paradigm*. Practices offer the opportunity to unite the capacity to make and the capacity to act (Schmidt, 2014). This is particularly important to digital security because the security of a digital interaction is rarely secured only in that moment, but is instead part of a series of security actions that are bound into knowledge and reason, and cultures and values. The practice focus leads us to examine how technologies fit into our everyday practices (Kuutti and Bannon, 2014). This is a significant insight because digital security technologies fit into everyday practices, and digital security is not only understood as the security technology, and the interactions with that technology, but as part of a web of everyday security practices.

By looking through a practice lens, it is also possible to understand technological security and security interactions from a temporal perspective given that practices are situated in time and space (Kuutti and Bannon, 2014).

The Practice paradigm also acknowledges that practices are dependent on the surrounding material and the cultural environment in which they are situated (Kuutti and Bannon, 2014). The Practice paradigm provides a means of bringing together security technologies with security

theories, by asking practice-related questions that can be answered in different ways from the different theoretical positions. This is because practice enables an individual to adjust general principles and rules to the particular conditions in which the principles and rules are to be enacted (Schmidt, 2014).

The different theoretical positions in the security theory cannon provide a different position from which to determine the following questions that Schmidt (2014) set out when exploring practice:

- "How do they determine the conditions when certain practices are to be used?"
- "How do they derive the most appropriate techniques for use in practices?"
- "How do they decide when to deviate from the rules and form new practices?"
- "How do they deal with breakdowns when practices no longer work?"

Practices are dependent on the surrounding material

The participatory and observational techniques described in this chapter can be focused on patterns of practice as the primary unit of analysis. Participatory, material forms of engagement, such as model building and collage, can be used to uncover how people determine which information and sharing practices to use and when, where, and at what point those patterns of practice need to be changed. Using a practice lens enables researchers to identify the information sharing and protection that happens in-between systems, and is a perspective that links the internal, embodied forms of security with practices of information sharing and protection in everyday life.

This view not only makes visible the reasoning and logic that drive the interactions and use of security technologies, but also the reasoning that shapes those technologies in the first place. The perspective of looking around and between technologies also means that a practice lens is useful for identifying and understanding the interactions between securities and how, through these interactions, a wider security practice fabric is formed.

6.2 Critical Design

Digital civics not only draws on participatory processes in design, but also encourages a critical design approach. This philosophy of critically questioning the role of technology has been adopted as a central tenet in critical design approaches. The essence of what makes design critical has its roots in the Marxist notions of ideology and alienation where *"the basic idea is that dominant social classes maintain their dominance by disseminating a system of myths presenting the status quo as natural and good (this is ideology) which encourages the working class to buy into a system that works against its own interest (this is alienation)"* (Bardzell and Bardzell, 2013).

Bardzell and Bardzell conclude that the following makes design critical:

- *Perspective-shifting and holistic understandings*: critical design helps to encourage multi-perspectival understandings and accounts of a problem, not to offer a singular truth.
- *Theory as speculation*: theories are used to challenge understandings and encourage the consideration of different viewpoints rather than to offer truth.
- *A dialogic methodology*: the focus of a critical design process is not to enter into different types of engagement from which a diverse range of meanings and experiences will emerge.
- *Improvement of the public's cultural competence*: critical design processes encourage people to look beyond the surface and to

question the technologies and rationales that are presented to them.

- *Reflexivity*: critical design processes must understand their limits as well as recognise their involvement in social and political change.

A creative design approach is therefore one that offers security technology design a means of uncovering the tensions and contradictions in what is both wanted and needed from digital security.

Using a critical design approach, we can also call into question what security is being offered, to whom and for what reasons.

Speculation is one potential form of critical design and might be termed *"representations of systems yet to come"* (DiSalvo *et al.*, 2016). The creative arts have been used a key source of inspiration for this redesign, and are often included in such methodological innovation, drawing on techniques such as theatre, film-making and collaging. Such techniques are not only an aesthetic inspiration for the development of research methods to encourage increased participation, but also offer a powerful means of critiquing the implications and impacts of potential digital technology designs.

Social theory scholar Foster (2015, p. 1) explains that *"the arts enable an examination of the everyday in imaginative ways that draw attention to the cruelties and contradictions inherent in neoliberal society"*. The critical dimension extends participatory co-design and principles of contextual design and inquiry by ensuring that the research asks questions of the intentions of both the digital technology design and its deployment. Critical design is therefore an important means of ensuring that the critical security questions of Smith (2005) are central to a security design activity.

Creative arts play a key role in critical design

6.3 Creative Security Engagements

The VOME project developed a creative security approach to digital security inquiry (Dunphy *et al.*, 2014), which offered a means of understanding security technologies as technologies embedded within a social context.

Engaging with people in everyday spaces

It became clear from the outset of the VOME project that the standard user-centred design approaches of interviews, observation, surveys and focus groups had a limited success with the groups that VOME was working with. VOME initially started out by working with a user-centred approach, but in order to reach marginalised and under-served communities, the engagement processes had to be rethought, and the basis on which engagement took place had to be democratised.

Redesigning the engagement on this basis meant that the balance of power shifted from the researchers towards the participant groups that the researchers were working with. As a result, a participatory engagement process and design ethos was adopted by the project. The shifting of the balance of power towards the groups VOME was working with was important for the building of trust, and also to ensure that security was being addressed in terms of the issues that resonated with those groups.

6.3.1 Creative Security Philosophy

At its core, a creative security approach is a critical design engagement that draws on participatory and user-centred methods, in order to examine practices of information sharing and protection. Such practices include the making of security technologies, as well as the actions of

sharing and protection. Its focus is not the human computer interaction or the design of security technologies, but the actions that take place in the space around and between the interaction and the security technologies. By working through a Practice paradigm, we were able to connect the security practices, interactions and technologies to the overarching security narrative that shaped a particular context. Miettinen *et al.* (2009) observed that the study of practice is not only about the present, but also about how the practice in the present relates to the past and to larger institutional complexes.

A critical position, along with a participatory design approach, emerged as a result of the move towards democratising both the engagement process and the notion of technological, and subsequently digital, security. A critical approach examines technology and process starting from the question: *"security for whom?"*. Critical security design encourages practices and research that interrogate the assumptions, beliefs and values underpinning security technology practice and design, with a view to responding to emergent security problems in an innovative way. The focus of critical design in the context of digital security it to look below the surface of security problems and their technological responses and to critically challenge what is being asked of security and why. In answering this, we can also identify who the real beneficiaries are and how they benefit. This also means that we can identify who is dis-benefitted and at what cost to societal, individual, technological and state security.

Critical security design inquiries designed for VOME took a number of forms, including:

- Examining problems in security designs produced in the past.
- Co-development of technologies and responses for current security problems.
- Speculative design technologies for future and emergent security problems.

Creative security methods (Coles-Kemp, 2018) are designed to enable the development of an understanding of the broader context in which

information protection, sharing and production takes place. In particular, the methods are designed to draw out the broader issues and objectives that frame particular flows or systems of information. The participant-led methods of engagement are deliberately broad and open-ended so that participants can create a picture of their world, and in so-doing, develop an understanding of the issues that relate to the production, protection, sharing and curation of information in a particular context.

The focus of creative security methods is to promote dialogue, collaboration, listening, innovation and collective action in response to issues of information sharing and protection. The methods come from a tradition of participatory engagement that encourages active participation, encourages the identification of common interests (rather than re-enforcing differences between people), and promotes design responses that reflect and encourage the strengths of a particular environment. Creative security methods encourage people to reflect on their environment, the emotions they feel when sharing and protecting information, the constraints they experience, the pressures that they undergo, as well as the actions and the tasks that they perform when generating and sharing information. The methods encourage the use of colour, imagery, shapes, textures and sound, as well as text, to reflect upon and articulate the situations in which information is generated and shared.

Different methods are used to elicit security narratives

6.3.2 Creative Security Methods and Principles

There is no prescribed set of methods that are used as part of creative security engagements; any method that encourages creative thinking and discussion about an aspect of security could be classified as a

creative security method. The practice of creative security has revealed time and time again that the materials that are used and the way in which they are used must be appropriate and meaningful to the group using them.

There are, however, a number of methods that we have used in the course of our work that have proved particularly successful engagement and data gathering methods. These methods are described in the following paragraphs.

Ceding control to participants is fundamental to the approach

Collaborative wall collage: uses the form of the wall collage and it was first developed for creative security engagement on the VOME project by (Coles-Kemp and Stang, 2019). Open questions, statements and stimulus material are used to encourage participants to produce their own responses to a particular theme. The responses are both written and pictorial, and can also be audial. The responses are created as a wall collage where participants, not researchers or security practitioners, produce the content and have full editing rights. The output is a meta-narrative from a group of people about a particular security topic.

Current experience comic strip: uses a form of storyboarding combined with the use of pre-prepared icons and the technique of doodling. It was first developed for creative security engagement by Makayla Lewis on the CySeCa project (Lewis, Coles-Kemp, *et al.*, 2014). Open questions and statements are used to encourage participants to think about and communicate everyday experiences in a particular aspect of security. Participants are provided with icon sets as well as art material with which to illustrate their responses. The output is an individual narrative about a particular security topic.

Physical modelling: this is a narrative method that uses physical modelling as the main medium for storytelling. It was first developed

for creative security engagement by Claude Heath on the TREsPASS project (Hall *et al.*, 2015). Open questions and statements are used to encourage groups of participants to build an everyday security narrative in a physical modelling tool such as LEGO. As part of the model building process participants are encouraged to discuss and reflect upon the security issues and the potential security responses. The output is a group narrative about a particular security topic.

To try to keep the approach as open and supportive as possible, creative security engagements are grounded in four participative principles:

- Cede control to the participants to create a form of engagement where participants are able to negotiate the terms on which the research takes place.
- Make visible all collected data by participants, displaying the data in open spaces, so that participants both develop a sense of ownership of the data, and have access to the data to make subsequent changes.
- Carry out the research and engagement in a space that participants routinely frequent in their everyday activities.
- Engender a participative environment that encourages participants to envision positive change to a particular aspect of their everyday working environment.

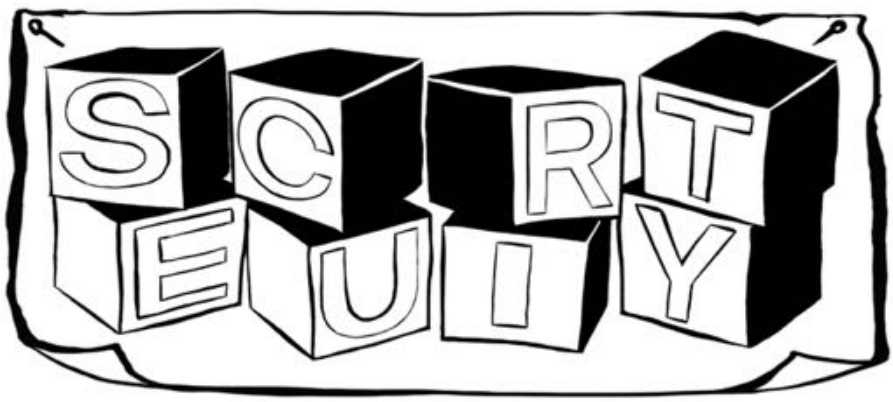
These principles have been found to shift the power towards the groups taking part and away from the practitioners or researchers (Coles-Kemp and Ashenden, 2012). Designing these principles into each engagement encourages spaces where people are able to share their experiences of everyday security concerns, build trust both in each other, develop their own understandings of what security means, and where people feel able to be part of changes that resolve security concerns not just for individuals but for groups of people.

As can be seen, the creative security engagement approach has many parallels with the approaches used in digital civics, and contributes to

the wider canon of participatory design engagement that draws from the creative arts.

6.4 Using Security Theories as Design Inspiration

A creative security approach can be used to develop an understanding of the context of use, and the securities at work, in a given situation. They also provide an approach in which people can collaborate to identify the security issues that are important in their everyday lives. Crucially, such an approach also identifies the much broader canvas of sociotechnical networks that combine to secure people in a digital context. For example, Coles-Kemp and Jensen (2019) demonstrate how access to digitalised refugee resettlement services is primarily a question of the benefits that can be realised through accessing these services, and that access is both enabled and protected through wider access to a network of social and technical resources.



Playful challenging of design assumptions

Creative security engagements produce narratives of security which contain different forms of security – both social and technical. Understanding wider social and political theories of security provides a broader set of analytical tools with which to unpack the security narrative and experiment with different security strategies. For example, competing security goals of different stakeholders might be identified, multiple lived experiences or real worlds might be identified, contrasting notions of strength and vulnerability might come to the fore, and different security

perspectives might be revealed if the narrative is told by the state, society or the individual.

Creative security tools can also be used in a more speculative manner, by using security theories as a provocation to challenge the narrative of security technology design, to examine its security impacts in current usage, and to imagine alternative futures with different security outcomes. Our methods are playful and creative to encourage experimental thinking about security possibilities and futures.

One approach to helping security technology designers to shift perspective is to use social and political theories of security to change the "start point" or assumptions about the design. For example, a scenario might be viewed from the perspective of:

- Different security logics where a scenario might be viewed using both positive and negative security positions, or from the perspective of a different site of security, and by swapping a universalist for a contextualised security position (or vice versa).
- Different types of security thinking could be embodied in design personas so that security technology designers, for example, could adopt a persona that embodied a realist position, and another one could adopt a persona that embodied a feminist security position.
- Different security strategies with their roots in different theory positions: for example an attack-defence strategy or a collaborative strategy.

These different, theory inspired techniques, could be used to build and re-build scenarios to assess which security strategy and design approach to deploy in a given scenario, for the best effect. An approach that encourages experimentation in this way can use other provocations, and bring in other ways of seeing and thinking, to encourage and welcome new forms of security thought and practice.

6.5 Concluding Comments

This chapter has presented a participatory, inclusive approach to identifying digital security issues, and co-designing responses to them. The

approach enables the identification of the different securing processes as well as the security technology. It also brings clearly into view the sociotechnical networks in which elements of the digital security practice take place. The next chapter sets out three worked examples that represent a digital security approach.

7

Digital Security From Research to Application

Security technologies have to protect both people and technology

A digital security approach does not replace or ignore technological security principles. Those principles are essential to the reliable, secure technology upon which we all depend. However, digital civics scholarship and a Practice paradigm offer a means of understanding technological security as being a part of a wider digital security design - one that *resonates* with the people it is protecting, *responds* to their security issues and, through negotiation and participation, and *resolves* security issues. A digital security approach therefore has the twin goals of protect *and* enable at its core.

In the projects that we have worked on (UKRI, 2020), every participant that we have worked with not only wants protection from digital harms but also wants to use digital technology in a way that is free from fear and that enables them to achieve their goals. To create digital

environments in which these goals are met requires not only reliable, secure technology, but also an understanding of the meanings of those technologies for individuals and the patterns of information sharing and protection practices that form around those meanings.

This chapter illustrates a digital security approach through the following three studies: digital security and service design, digital security for all and digital security and professional security practice.

People want to be both protected from harms and free from fear

Digital Security and Service Design: in this study, stakeholders worked together through a creative security engagement to identify the security issues that were relevant for a micro-payments service. LEGO was used to model the micro payments service situated within intended sites of use. By modelling the wider context of use, issues of financial, ontological and organisational security came into view, and responses were identified that responded to security at the intersections between these securities and technological security. The approach enabled participants to explore the potential webs of practice that might form in and around the micro payments service. This case study makes visible how the intended technological controls within the micro payments service relate to the security logic and practices of household security, financial institution security and service provider security (and the practices that form to connect these different securities).

Digital Security For All: in this study, a group of welfare claimants took part in a story telling activity within a focus group to examine how security practices might form around a digital welfare service. The study shows how when the conditions of a welfare policy are enforced

through security technologies and the face to face support is removed, the result can be a security policy that feels both harsh and unfair. This in turn can lead to practices of resistance. The study also shows that an effective way to respond to such resistance is not to increase the technological security of the service but to use relational services and interactions to develop positive security around the service. This case study makes visible how technological controls within the digital welfare service relate to the wider security logic of social security and of state security and the practices that form to resist these connections.

Digital Security And Professional Security Practice: in this study, LEGO modelling is used to explore different approaches to controlling the information generated by Internet of Things (IoT) monitoring in the workplace. The LEGO modelling surfaced a risk-driven control approach and a trust-driven issues-based approach. Using Smith's four critical security questions we identify the ways in which these two approaches can be contrasted (Smith, 2005). This study shows that effective security practices require consensus as to what the security issues are and how they should be responded to. The study also shows the importance of agreeing the value and use of technology before embarking on security responses to those technologies.

In each case study, we set out the use of security technologies within the wider security landscape, examined the information sharing and protection practices that are illuminated and reflected on how the wider perspective helps us to see a more nuanced and multi-layered security.

7.1 Digital Security and Service Design

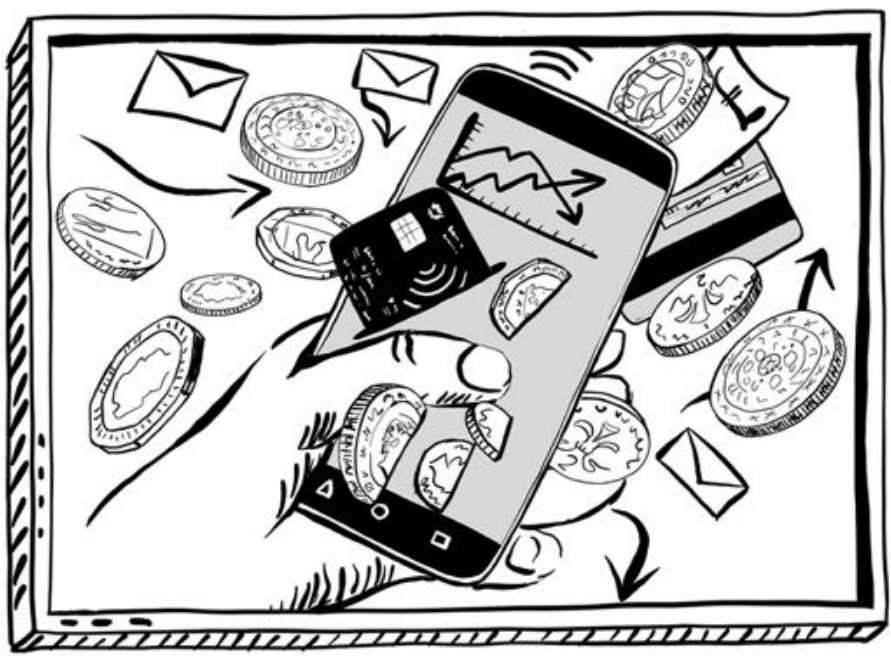
In this case study, we look at a digital security approach to service design. This work was originally published in 2015 (Hall *et al.*, 2015) as a critical review of the way in which visualisation is used in technological security practice.

7.1.1 Technological Security and the Wider Security Landscape

This case study is situated in a Small to Medium Enterprise (SME) that specialises in the delivery of micro-payments services to small

businesses and households. The micro-payments service was designed use via Internet Protocol Television (IPTV). The goal of the study was to identify which security controls were needed in the IPTV service, how those controls would benefit the people using the service whilst still meeting the regulatory requirements, and questioned under what social, economic and political conditions those controls would be effective.

Micro-payments are a useful means of financial management for many households, particularly for those in lower socio-economic groups. By combining micro-payments with technology such as a television that is commonly found in a household, micro-payment technology becomes more accessible. IPTV has a wide user-community demographic, and the micro-payments service was particularly aimed at users without access to, or distrustful of, computers and other smart devices. Given the intended breadth of the user community, the service had to be usable and accessible as well as secure.



For many micropayments are an everyday event

In this context of managing household finances, the people using the service might be vulnerable to abuse of the system that might be carried

out by other members of the community or from their own carers and family. In this security landscape a number of different securities come to the fore: security built on power and trust relations within households, the importance of financial security to power and trust relations within a household, and the relationship between the security view of the regulators and the meanings of the security controls within a household setting.

7.1.2 Physical Modelling and the Wider Surface Area

This study used a collaborative modelling approach based on participatory design principles in order to gather the views of different stakeholder groups. Participants were asked to model in LEGO central actors and the infrastructures that were made and used to access micro-payment services.

Creating a physical model that included the wider context of use enabled a much broader discussion about the context in which the service could be used. For example, modelling the service in this way enabled a discussion about how the intended user community was remote in many ways from those providing the service. The physical modelling showed how the service provider was both physically distant and also distant in terms of how they experienced very different pressures and stresses to the ones likely to be experienced by many of the intended service users.

The physical modelling also illuminated the extent of the sociotechnical infrastructure necessary to provide a micro-payment service that was inclusive. In addition to the provision of technical and service infrastructure, the modelling showed how third sector organisations and community groups were important both to signpost families to the service and to support families in setting up the service and using it. Debt-support organisations and consumer rights groups were also highlighted in the model as important aspects of the infrastructure needed to support families in managing their finances and this support would have a direct impact on service use. The model also showed the different information flows across this infrastructure and discussions were had as to how those information flows might be controlled.

Pressures surrounding the context of use became visible

The physical modelling showed the potential power relations both within families and within the neighbourhood and the types of information that was used to create and sustain those power relations. The modelling highlighted how technical know-how might reside with younger members of the household. The locus of technical know-how in a family network might conflict with the need to control access to information. It was discussed how the context of use was also shaped by the pressures in which the different actors resided. For example, financial pressures caused by unexpected bills might result in more stressed interactions with the micro-payment service and less attention being paid to security controls. Another example was given of how the television was likely to be in a communal area and it might be difficult for bill payers to have the necessary calm to make the payments. These fluctuations and disruptions were all identified as points of vulnerability for the micro-payment service user.

7.1.3 Reflections

The physical modelling exercise revealed the full design of the micro-payment service and the sociotechnical infrastructures that interoper-

ated to form the service. It revealed that what had been regarded as a micro-payment service was in fact made up of a number of services that were held together by a sociotechnical infrastructure composed of technology, network connections and community groups. The modelling exercise also created a space in which people could discuss the different power relationships that might be at work and how these relationships were shaped by cultural practices, the pressure landscapes in which the different actors resided and the technical capabilities that actors might have.

Once the extent of the service was made clear, the extent of the possible security challenges also emerged. Examining the models of the possible sites of service use, it also became clear how the environment might contribute to the threats that service users could face. For example, carrying out micro-payments in a communal living area introduces threats related to coercion by another family member, masquerading of legitimate users as the login process might be observed, and accidental errors caused by accessing the service in a stressful, chaotic environment.

The threat landscape becomes clearer

The physical modelling exercise also revealed which values the service was developed from and how those designing and delivering the services understood the intended user community. This resulted in a greater focus on building and developing trust with the intended user communities and a greater focus on the support infrastructure for those communities. This meant that the security that was foregrounded was the security of social relations and the financial security of that household. This in turn meant that the technological controls had the focus of ensuring availability of the service and of enabling access.

7.2 Digital Security For All

The work presented in this case study was first published in 2014 (Coles-Kemp *et al.*, 2014). The focus of the study is the implications of digitalised welfare. The original study revealed how technological security controls in digitalised welfare were viewed by one group of participants and how people respond when they perceive those controls to be hostile to their individual security.

The study demonstrates the importance of designing a digital security for all, and ensuring that the underlying political and social system as well as the technological controls afford security to the intended users of that system.

7.2.1 Technological Security and the Wider Security Landscape

This was a small case study that was situated in an economically deprived area of the North East of England where unemployment is significantly higher than the UK's national average. The focus of the case study was to explore how the introduction of digital welfare services might change attitudes towards information sharing and interaction with representatives of the welfare services. At the time of the research, Universal Credit (the UK's digital-by-default welfare system) had not been rolled out but welfare claimants were having to use various on-line services as part of the welfare claiming process. In particular, welfare claimants had to use on-line processes to log job seeking activities and demonstrate compliance with the welfare claiming policy.

This case study connects the security of individuals with the social security policy deployed through digital services and the protection of the digital service.

7.2.2 Speculation and Practice

A small group of five participants discussed the impact of the digitalisation of welfare services. Three participants were long-term unemployed, two participants were working in the third sector and two of these participants received a disability living allowance. The participants were members of a community group that provided digital welfare support.

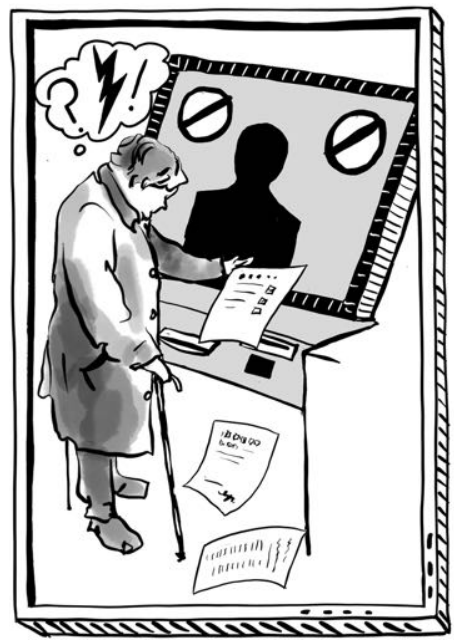
The participants walked through how they gain access to digital services. In walking through how they access services, they used storytelling to speculate about the types of resistance practices that might emerge if people felt that the welfare services were unfair. During the walkthrough, the participants also talked about how they felt when accessing these services and the types of control that they believed they had.

Digital access can be complex

The participants in the focus group told speculative stories of future digital welfare use that showed little respect for the registration, identification and verification processes enforced through technological security. Twisting the technological security controls to achieve unauthorised or illicit outcomes was sometimes presented as an act of empowerment, sometimes an act of coercion and typically as an act driven by financial need. The participants gave detailed examples of how they would expect to be able to twist the system, where twisting meant breaking or bending the welfare rules. It is striking that the participants demonstrated a rich body of knowledge of how an individual might subvert these processes and showed no respect for the technological implementations of these processes. By contrast, the respect that was shown emerged when talking about the face-to-face contact with welfare officers, which was a form of interaction that participants felt they were less able to subvert.

7.2.3 Reflections

From a digital security perspective, this study underscores the relationship between security practices, security issues and the stakeholder groups. The stakeholder group (welfare claimants) who took part in this study perceived the digital welfare system as being a source of potential harm. The result was a series of practices, called twists, that people might invoke to counter the insecurities exacerbated by digital welfare.



Digital by default can be alienating

The stories that the participants told showed how these twists are in part resistance practices that are pushing back on welfare systems that are regarded as hostile. The analysis of the participants' narratives also indicate that standard end-user system security techniques of identification, verification, monitoring and surveillance do not result in compliant behaviour from a user community that contests the values and the goals of the underpinning service logic. This raises the important question of how to make these security controls more effective in such a scenario and, in particular, how to adjust the sociotechnical infrastructure and social network that emerge around such services.

A potential point of security intervention, therefore, lies in the social relationships that form around and between such digital services. The participants' narratives also underscore how technology and technological controls are enmeshed within social relationships. Adversarial systems, as the participants felt digital welfare systems to be, often result from poor relationships between the stakeholder groups and this exacerbates adversarial security practices. The participants' narratives showed that security is repaired when stakeholder groups work together to re-position the values and the goals of the system, and to develop strategies that develop positive security to minimise the harms that can result from interacting with the digital welfare system. This outcome foregrounds the point that when a digital security lens is used, the responses to security problems arising from the use of digital services may well lie away from the technology use and in the relations into which the use of services is situated.

7.3 Digital Security And Professional Security Practice

This case study was first published in 2020 (Coles-Kemp *et al.*, 2020b) and it presented a study of two alternative approaches to identifying and responding to the security issues that emerge from IoT monitoring in the workplace. The study demonstrates the limits of technological security and how a wider position is needed to respond to the security issues that emerge at the intersections between technological security and the security of people. The study also illustrates the limits of a protection-led approach to security, and the possible benefits of blending a protection-focused approach with an enablement-focused approach to security.

7.3.1 Technological Security and the Wider Security Landscape

The context for this study was IoT monitoring in the workplace. This is a context in which the security of people and the security of technology are physically and technologically interwoven (Pierce, 2019).

The study presents two very different types of security practice in the context of IoT monitoring in the workplace; one type of practice was performed by security practitioners and the other by healthcare service providers. The case study presented each group with an imagined scenario of IoT monitoring. In the case of the security practitioners, the use of IoT to monitor staff was the given scenario. In the case of the healthcare service providers, the use of IoT by patients to self-manage health conditions was the given scenario. In this study, we wanted to compare the approaches of both professional practice communities might have towards this scenario and to explore what forms of digital security might work in professional security practice.

A physical modelling approach was chosen as the main engagement method. Each practitioner group used LEGO to model and discuss their IoT in the workplace scenarios. The data was gathered, processed and stored under ethical approval from the academic institution. Data was generated in the form of physical models, annotations made by individual participants, facilitator observations, notes of collaborative outcomes from the brainstorming, and final group-feedback contributions.

The data trails from monitoring technologies are extensive

7.3.2 Establishing the Basis of Controls

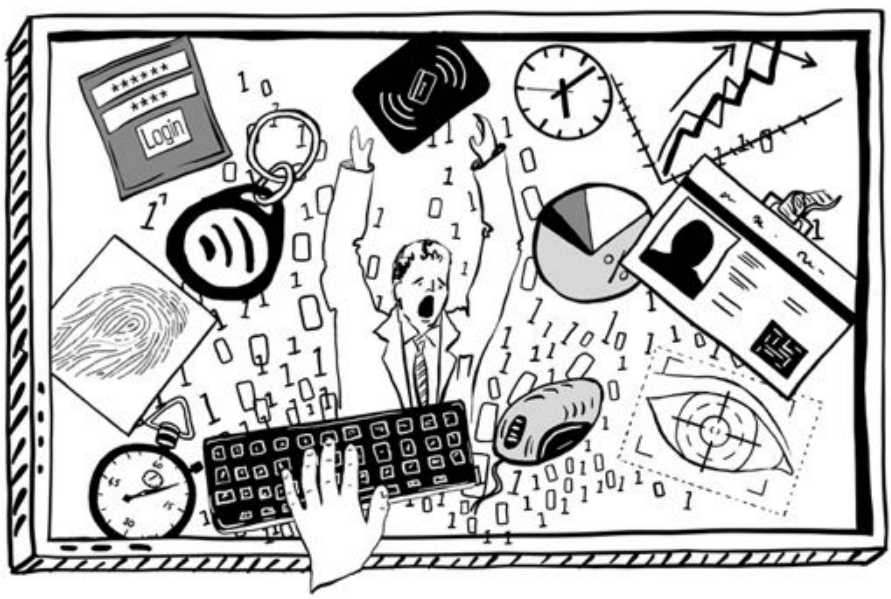
The analysis showed the challenges that embedded technologies pose for protection-focused technological security thinking. When information production and circulation moves away from fixed points and becomes embedded as part of day to day interactions, an approach based on security perimeters is less effective. The following themes were identified from the analysis:

- Security Issues: Much of the response from the security practitioners focused on the inherent threat of not being in control. This manifested itself in a sense of being overwhelmed with the volume of data, and also of not being able to create a protected and stable perimeter around the technology itself. This security issue arises from a mismatch between security strategy and security threats and highlights how vulnerabilities emerge when trust diminishes in the capabilities of experts to manage a technology.
- "Who Secures?": Both groups questioned the extent to which technology could provide security in this setting. Both groups concluded that the technological responses were only a part of any answer to this question, and that social interaction plays an equally important and necessary securing function. This theme sheds further light on why "workarounds" might appear in order to mitigate deficits in security technology capabilities, and highlights the importance of social interaction and relational services in securing these contexts.
- Benefits and Disbenefits: Both groups identified that establishing, agreeing and communicating the benefits of IoT monitoring were important processes to establish the relevant security goals. It is through these interactions, some of which take the form of relational services, that alternative conceptualisations of security are both identified and reconciled.

The secondary analysis performed through Smith's four critical security questions (Smith, 2005) revealed different referent objects in each study: the security practitioners focused on threats to the organisation

and threats to themselves, whereas the healthcare service providers focused on threats to the individual using the IoT monitoring device and threats to the community of device users. The analysis performed using these four questions also revealed a difference in opinion as to who or what was doing the securing. Whilst the security practitioners focused on technology as doing the securing (whilst recognising the limitations), the healthcare service providers focused on trust-led collective and social action as the primary means of securing the use of IoT monitoring.

7.3.3 Reflections



Technological controls have limited power

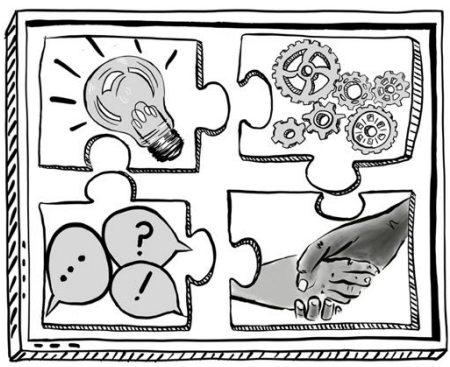
Each group of practitioners viewed the security issues in different ways. The security practitioners largely saw the environment as being too complex for the security technologies to defend, whereas the healthcare service providers saw the issues more as a lack of transparency and accountability resulting from the complexity of the environment. In response to this, the healthcare service providers argued for a multi-stakeholder response in order to make the information flows from the IoT devices more legible to those being monitored and to those doing

the monitoring.

Both groups doubted the effectiveness of technology to respond to the issues that were thrown up and, in different ways. Both groups indicated that technologies and practices that helped people to relate the technology use to their practices and tasks would increase the trust in the way information was being produced and circulated. This in turn would help the identification of risks because it would be clearer which aspects of the technology they could rely on. Both groups recognised that the IoT monitoring technologies could both benefit and harm people in the workplace and that there needs to be debate and agreement to decide how these technologies are being used.

This case study shows the limitations of a solely technological approach to security. The response from the healthcare professionals focuses on a dialogic, multi-stakeholder, trust-led approach. This represents an emphasis on the securing processes and seeks to build consensus on the purpose of IoT monitoring and the parts each person plays to achieve that agreed outcome. In order to cope with the ambiguity of the IoT monitoring technology, both groups agreed that there needs to be debate and discussion. This again throws a spotlight on the securing processes.

7.4 Digital Security as a Practice



Resonate, resolve, reciprocate

Each of the three case studies show the importance of a people-centred, issues-driven approach that mobilises sociotechnical security responses. Each case study also throws light on one more intersections between technological security and another security. By setting out the wider security landscape, it becomes possible to simultaneously see the social and political security logics at work, how the technological security interacts with this logic, and the information sharing and protection practices that emerge as a result of

this interaction.

These case studies show that a digital security practice can be characterised with the following three principles: resonate, resolve, reciprocate. The principles are set out in the table below and each promote a more inclusive form of security. The principles are a recognition of the fact that we are mutually dependent on each other to protect our digital interactions. They are also a recognition of the fact that security controls that do not respond to the security issues that people experience will not be engaged with and potentially will increase insecurities, not decrease them.

Table 7.1: Digital security principles

Principle	Explanation
Resonate	An approach that people recognise as offering security
Resolve	An approach that resolves or reduces security issues
Reciprocate	An approach where the security of one party also improves the security of another

The principles in Table 7.1 play out in the three case studies in this chapter as follows:

In *Digital Security and Service Design* we see the value of participatory consultation when designing a service and the importance of identifying security issues that *resonate* with the intended audience of the service. We can also see that many of the security issues that are identified sit at the intersection between technological security and other forms of security. Therefore to *resolve* these issues requires that the technological security is part of a wider sociotechnical network of relational support. The security in this network is intended to *reciprocate* where both service providers and the intended user communities work together to identify and resolve issues for the protection of each other.

By contrast, the *Digital Security for All* study shows how both insecurities increase and resistance to security controls emerges when

the approach to technological security does not resonate with or resolve the security issues of the service user. This case study also illustrates what happens when the wider social and political security logic is not felt to be reciprocal and that security is felt to be one-way (towards the service provider) and hostile towards the individual.

Finally, *Digital Security and Professional Security Practice* illustrates the limitations of technological security to resolve human security issues that arise from technology use. It also demonstrates how an issues-led inclusive approach that uses collaboration and a strong sociotechnical network to co-produce this response results in responses that are more likely to resonate and resolve the security issues that people experience from IoT monitoring technologies.

7.5 Concluding Comments

The three case studies demonstrate the significance of the original VOME insights:

- assessing risk to digitally-mediated networked interactions requires both the assessment of risks to technology and of the risks networked technology use pose to the users of that technology;
- the understanding of technological security risk needs to be set in the context of the wider concerns that networked technology users are experiencing;
- people often focus on the benefits that they gain from using a technology or service and consider the technological security risks in relation to that benefit.

Using approaches that illuminated not only the technologies but the people using those technologies and spaces in and around those interactions, the case studies identify where:

- interventions and responses might be made in the spaces around the human computer interaction;
- security technologies create rather than resolve threats to human computer interaction.

In the final chapter, a call to action is set out that is intended to move forward digital security from being a series of case studies to being an area of study and practice in its own right.

8

Conclusions and Call to Action

Digital security acknowledges the importance of technological security and the security of human computer interactions, but it sets those forms of security into a security paradigm that places digital products and its security in the wider social, cultural, economic and political setting.

In this monograph, digital security has been set out as:

- A paradigm that connects technological protection to the wider social and political security logics.
- A paradigm that focuses on the practices that form in and around digital products and their security technologies.
- A paradigm that produces understandings about particular patterns of security responses to security technologies and policies.

This wider security perspective is needed in order to build meaningful forms of digital protection because technological security has become one of the main seams through which the security interests of the state and other institutions of power come into direct conversation with the security of the individual. On the one hand, technological security is turned towards the task of ensuring that data and technology are

reliable and stable in our digital products and services. On the other hand, technological security signifies the values of the institutions that deploy the technologies and enforce their logic of security which, in turn, interacts with the security of the individual. It is an inescapable fact that technological security is embedded in the social and political security conversations about which values to protect and why (but also which values to not protect). Digital security acknowledges the importance of such conversations and recognises the social impacts security technologies might have.

Digital technology has transformed society and changed the lived experience of the majority. As a result, our relationships with the world, with each other and with ourselves have been transformed through digital products and services. Productivity and efficiency and how we can do more, create more and produce more with ever scarcer resources have been the dominant narratives that have driven this digital transformation. Technological security has been put at the forefront of our digitalised approach to regulating access to resources, controlling access to processes of production, and determining who gets access to what is produced and when.

In this drive to get more from less, it has been taken for granted that the trust relations that bind society together will scale up to keep pace with our digital expansion. When computer and network security was first designed, it was not the intention that the principles used to protect data and technology would become the principles used to build and maintain trust relations between people. We contend that technological security cannot do this alone and needs to be placed into a broader form of digital security to be effective in this front-line role. Such a security places the security of technology in the context of the security of people living day-to-day in a web-enabled and digitally-connected society. It is a digital security that is sufficiently flexible to respond to the security tensions between stakeholders. Using a trust-led, relational approach to identifying and responding to those tensions means a broader, more inclusive digital security emerges; one in which traditional forms of technological security are embedded into forms of narrative and contextual security that both enable people to live free from fear and protected from harms.

Technological security is located within a broader digital security

8.1 Call for Recognition and Action

This monograph concludes with a call to recognise both the political and social power of security technologies and reflect this recognition in the claims made about the effectiveness of security technologies. We therefore call for the recognition of:

- The social and political forms of security that security technologies represent, and the ways that these forms shape the effects that security technologies have on individuals, groups and society.
- The ways in which digital exclusion takes many forms and has the potential to harm not only those who are excluded but society as a whole.

Once this is recognised, we call on those practising and researching forms of digital security to take the following actions:

- Identify the security concerns of all stakeholders in a given situation and critically examine the power relations and political imperatives that give rise to those concerns.
- Embrace and promote civic initiatives to develop different forms of digital security and recognise the legitimacy of those approaches in the ontology in which they have been designed.
- Promote and support a culture of respect for scholars and practitioners who engage with different forms of digital security - the validity of digital security should be determined by the effects it has and the contribution it makes to scholarship, not by the ontological tradition that it stems from.

Security scholars and practitioners working with the digital stand at a crossroads. We can either continue to place a focus on a security paradigm that has protection shaped by a logic of exclusion and control at its core or we can seek and acknowledge a form of security that puts the responsibility to both protect *and* enable a secure society for all at its core. If we continue to concentrate on a paradigm of security through

exclusion and use this paradigm as the primary means of securing a digitally-mediated society, we shall continue to contribute to cycles of conflict and tension that are only set to increase as resources become ever scarcer. If instead we place a focus on a paradigm of security through inclusion that locates technological protection within a more expansive and flexible logic of security, we can reshape our outlook and in so doing contribute to a reformation of security norms and practices that are grounded in principles of inclusion, trust and reciprocity.

Standing at a crossroads and the choice of direction is ours

Acknowledgements

I am extremely grateful to the many participants, collaborators and funders without whom this research would not have been possible. I would also like to thank Will, Nick, Oliver, Nicola, Kieron and the two reviewers who read the manuscript and gave comments and feedback. This monograph was made possible through the collaboration and support of Alice Angus and Thiago Zagatti – both of whom showed extraordinary levels of patience and care as the monograph was slowly transformed from a heap of words into a manuscript. Alice's artwork draws out the complex and contradictory details of everyday life. Every line in her drawings writes back in the feelings and experiences of technological security use that academic writing so often struggles to articulate. And finally, thanks and affection go to Peter for his encouragement and for gently reminding me you can only ever do your best and then leave it there. Thank you to everyone for your support and contributions! Despite all this wonderful help, any errors are, as always, my own.

Artwork by Alice Angus. Artwork is ©Alice Angus 2020.

Lizzie's writing and Alice's artwork in this manuscript were funded by EPSRC Fellowship: Everyday Safety-Security for Everyday Services (EP/N02561X/1).

References

Acquisti, A. (2013). "Complementary perspectives on privacy and security: Economics". *IEEE Security & Privacy*. 11(2): 93–95.

Adams, A. and M. A. Sasse. (1999). "Users are not the enemy". *Communications of the ACM*. 42(12): 41–46.

Albert, M. and B. Buzan. (2011). "Securitization, sectors and functional differentiation". *Security dialogue*. 42(4-5): 413–425.

Albrechtsen, E. and J. Hovden. (2009). "The information security digital divide between information security managers and users". *Computers & Security*. 28(6): 476–490.

Albrechtsen, E. and J. Hovden. (2010). "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study". *Computers & Security*. 29(4): 432–445.

Anderson, R. (2001). "Why information security is hard-an economic perspective". In: IEEE. Seventeenth Annual Computer Security Applications Conference. 358–365.

Arcury, T. A. and S. A. Quandt. (1999). "Participant recruitment for qualitative research: A site-based approach to community research in complex societies". *Human Organization*. 58(2): 128.

Asad, M., C. A. Le Dantec, B. Nielsen, and K. Diedrick. (2017). "Creating a Sociotechnical API: Designing City-Scale Community Engagement". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM. 2295–2306.

Ashenden, D. (2016). "Your employees: the front line in cyber security".

Ashenden, D. and D. Lawrence. (2013). "Can we sell security like soap?: a new approach to behaviour change". In: *Proceedings of the 2013 New Security Paradigms Workshop*. ACM. 87–94.

Ashenden, D. and D. Lawrence. (2016). "Security dialogues: Building better relationships between security and business". *IEEE Security & Privacy*. 14(3): 82–87.

Ashenden, D. and A. Sasse. (2013). "CISOs and organisational culture: Their own worst enemy?" *Computers & Security*. 39: 396–405.

Baldwin, D. A. (1997). "The concept of security". *Review of international studies*. 23(1): 5–26.

Balzacq, T. (2010). "Constructivism and securitization studies". In: *The Routledge handbook of security studies*. Routledge. 56–72.

Balzacq, T. and M. D. Cavelty. (2016). "A theory of actor-network for cyber-security". *European Journal of International Security*. 1(2): 176–198.

Bardzell, J. and S. Bardzell. (2013). "What is critical about critical design?" In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM. 3297–3306.

Baskerville, R. (1991). "Risk analysis: an interpretive feasibility tool in justifying information systems security". *European Journal of Information Systems*. 1(2): 121–130.

Beautement, A., M. A. Sasse, and M. Wonham. (2009). "The compliance budget: managing security behaviour in organisations". In: *Proceedings of the 2008 New Security Paradigms Workshop*. ACM. 47–58.

Becker, I., S. Parkin, and M. A. Sasse. (2017). "Finding security champions in blends of organisational culture". *Proc. USEC*. 11.

Beecham, S., N. Baddoo, T. Hall, H. Robinson, and H. Sharp. (2008). "Motivation in Software Engineering: A systematic literature review". *Information and software technology*. 50(9-10): 860–878.

Bella, G. and L. Coles-Kemp. (2012). "Layered analysis of security ceremonies". In: *IFIP International Information Security Conference*. Springer. 273–286.

Berners-Lee, T., W. Hall, and J. A. Hendler. (2006). *A framework for web science*. Now Publishers Inc.

Bishop, M. (2005a). "Position: " insider" is relative". In: *Proceedings of the 2005 workshop on New security paradigms*. 77–78.

Bishop, M. (2005b). "The insider problem revisited". In: *Proceedings of the 2005 workshop on New security paradigms*. 75–76.

Bissell, D. (2013). "Pointless mobilities: rethinking proximity through the loops of neighbourhood". *Mobilities*. 8(3): 349–367.

Bjarnason, E. and H. Sharp. (2017). "The role of distances in requirements communication: a case study". *Requirements Engineering*. 22(1): 1–26.

Blythe, J. M., L. Coventry, and L. Little. (2015). "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors". In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 103–122.

Box, G. E., N. R. Draper, *et al.* (1987). *Empirical model-building and response surfaces*. Vol. 424. Wiley New York.

Brandt, E. (2006). "Designing exploratory design games: a framework for participation in Participatory Design?" In: *Proceedings of the ninth conference on Participatory design: Expanding boundaries in design-Volume 1*. 57–66.

Burdon, M. and L. Coles-Kemp. (2019). "The significance of securing as a critical component of information security: An Australian narrative". *Computers & Security*. 87: 101601.

Burdon, M., J. Siganto, and L. Coles-Kemp. (2016). "The regulatory challenges of Australian information security practice". *Computer Law & Security Review*. 32(4): 623–633.

Buzan, B., O. Wæver, O. Wæver, and J. De Wilde. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Caine, B. (1977). "Computers and the Right to Be Let Alone-A Civil Libertarian View". *Vill. L. Rev.* 22: 1181.

Caputo, D. D., S. L. Pfleeger, M. A. Sasse, P. Ammann, J. Offutt, and L. Deng. (2016). "Barriers to usable security? Three organizational case studies". *IEEE Security & Privacy*. 14(5): 22–32.

Carlos, M. C., J. E. Martina, G. Price, and R. F. Custódio. (2013). "An updated threat model for security ceremonies". In: *Proceedings of the 28th annual ACM symposium on applied computing*. 1836–1843.

Carr, M. (2013). "Internet freedom, human rights and power". *Australian Journal of International Affairs*. 67(5): 621–637.

Carr, M. (2015). "Power plays in global internet governance". *Millennium*. 43(2): 640–659.

Carr, M. (2016). "Public–private partnerships in national cyber-security strategies". *International Affairs*. 92(1): 43–62.

Carr, M. and F. Lesniewska. (2020). "Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance". *International Relations*. 34(3): 391–412.

Castro Leal, D. de, M. Krüger, K. Misaki, D. Randall, and V. Wulf. (2019). "Guerilla Warfare and the Use of New (and some old) Technology: Lessons from FARC's Armed Struggle in Colombia". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

Chavez, M., B. A. Cotner, and W. Hathaway. (2017). "Building Rapport during Applied Research Recruitment". *Anthropology News*. 58(3): e271–e275.

Chipperfield, C. and S. Furnell. (2010). "From security policy to practice: Sending the right messages". *Computer Fraud & Security*. 2010(3): 13–19.

Cipolla, C. (2009). "Relational services and conviviality". *Designing Services with Innovative Methods. Helsinki, University of Art and Design and Kuopio Academy of Design*: 232–245.

Coles-Kemp, L. (2018). "Practising Creative Securities". https://bookleteer.com/collection.html?id=28.

Coles-Kemp, L. and A. Ashenden. (2012). "Community-centric engagement: lessons learned from privacy awareness intervention design". In: *The 26th BCS Conference on Human Computer Interaction 26*. 1–4.

Coles-Kemp, L., D. Ashenden, A. Morris, and J. Yuille. (2020a). "Digital welfare: designing for more nuanced forms of access". *Policy Design and Practice*: 1–12.

Coles-Kemp, L., D. Ashenden, and K. O'Hara. (2018). "Why should I?: Cybersecurity, the security of the state and the insecurity of the citizen". *Politics and Governance*.

Coles-Kemp, L. and R. B. Jensen. (2019). "Accessing a New Land: Designing for a Social Conceptualisation of Access". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

Coles-Kemp, L., R. B. Jensen, and C. P. Heath. (2020b). "Too Much Information: Questioning Security in a Post-Digital Society". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

Coles-Kemp, L. and F. Stang. (2019). "Making Digital Technology Research Human: Learning from Clowning as a Social Research Intervention". English. *Rivista Italiana di Studi sull'Umorismo (RISU)*. 2(1): 35–45. ISSN: 2611-0970.

Coles-Kemp, L., A. Zugenmaier, and M. Lewis. (2014). "Watching You Watching Me: The Art of Playing the Panopticon". *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*: 147.

Connell, R. W. (2005). *Masculinities*. Polity.

Corbett, E. and C. A. Le Dantec. (2018a). "Exploring trust in digital civics". In: *Proceedings of the 2018 Designing Interactive Systems Conference*. 9–20.

Corbett, E. and C. A. Le Dantec. (2018b). "Going the Distance: Trust Work for Citizen Participation". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM. 312.

Coventry, L., P. Briggs, D. Jeske, and A. van Moorsel. (2014). "Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment". In: *International conference of design, user experience, and usability*. Springer. 229–239.

Crinson, I. (2008). "Assessing the 'insider–outsider threat'duality in the context of the development of public–private partnerships delivering 'choice'in healthcare services: A sociomaterial critique". *Information Security Technical Report*. 13(4): 202–206.

Crivellaro, C., R. Comber, J. Bowers, P. C. Wright, and P. Olivier. (2014). "A pool of dreams: facebook, politics and the emergence of a social movement". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3573–3582.

Crivellaro, C., R. Comber, M. Dade-Robertson, S. J. Bowen, P. C. Wright, and P. Olivier. (2015). "Contesting the city: Enacting the political through digitally supported urban walks". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2853–2862.

Croft, S. (2012). "Constructing ontological insecurity: the insecuritization of Britain's Muslims". *Contemporary security policy*. 33(2): 219–235.

Croft, S. and N. Vaughan-Williams. (2017). "Fit for purpose? Fitting ontological security studies 'into' the discipline of International Relations: Towards a vernacular turn". *Cooperation and conflict*. 52(1): 12–30.

CyBOK. (2019a). "Cyber Security Body of Knowledge". https://www.cybok.org/.

CyBOK. (2019b). "Human Factors KA". https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf.

Deibert, R. J. (2018). "Toward a human-centric approach to cybersecurity". *Ethics & International Affairs*. 32(4): 411–424.

Deibert, R. J. and R. Rohozinski. (2010). "Risking security: Policies and paradoxes of cyberspace security". *International Political Sociology*. 4(1): 15–32.

Dewey, J. and M. L. Rogers. (2012). *The public and its problems: An essay in political inquiry*. Penn State Press.

DiSalvo, C., M. Gregg, and T. Lodato. (2014). "Building belonging". *interactions*. 21(4): 58–61.

DiSalvo, C., T. Jenkins, and T. Lodato. (2016). "Designing speculative civics". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 4979–4990.

Doty, R. L. (1998). "Immigration and the Politics of Security". *Security Studies*. 8(2-3): 71–93.

Dunn Cavelty, M. (2013). "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse". *International Studies Review*. 15(1): 105–122.

Dunphy, P., J. Vines, L. Coles-Kemp, R. Clarke, V. Vlachokyriakos, P. Wright, J. McCarthy, and P. Olivier. (2014). "Understanding the experience-centeredness of privacy and security technologies". In: *Proceedings of the 2014 New Security Paradigms Workshop*. ACM. 83–94.

Ehn, P. (2008). "Participation in design things". In: *Proceedings Participatory Design Conference 2008*. ACM.

Flechais, I., J. Riegelsberger, and M. A. Sasse. (2005). "Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems". In: *Proceedings of the 2005 workshop on New security paradigms*. ACM. 33–41.

Foster, V. (2015). *Collaborative arts-based research for social justice*. Routledge.

Frey, S., A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi. (2017). "The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game". *IEEE Transactions on Software Engineering*. 45(5): 521–536.

Friedman, B., D. C. Howe, and E. Felten. (2002). "Informed consent in the Mozilla browser: Implementing value-sensitive design". In: *Proceedings of the 35th annual hawaii international conference on system sciences*. IEEE. 10–pp.

Fukuda-Parr, S. and C. Messineo. (2012). "Human Security: A critical review of the literature". *Centre for Research on Peace and Development (CRPD) Working Paper*. 11.

Furnell, S. and K.-L. Thomson. (2009). "Recognising and addressing 'security fatigue'". *Computer Fraud & Security*. 2009(11): 7–11.

Gabriel, T. and S. Furnell. (2011). "Selecting security champions". *Computer Fraud & Security*. 2011(8): 8–12.

Geer, D. (2010). "Are companies actually using secure development life cycles?" *Computer*. 43(6): 12–16.

Gjørv, G. H. (2012). "Security by Any Other Name: Negative Security, Positive Security, and a Multi-Actor Security Approach". *Review of International Studies*. 38(4): 835–859.

Gollmann, D. (1999). *Computer Security*. Wiley.

Guillaume, X. and J. Huysmans. (2019). "The concept of 'the everyday': Ephemeral politics and the abundance of life". *Cooperation and Conflict*. 54(2): 278–296.

Gürses, S., A. Kundnani, and J. Van Hoboken. (2016). "Crypto and empire: the contradictions of counter-surveillance advocacy". *Media, Culture & Society*. 38(4): 576–590.

Hall, P., C. Heath, L. Coles-Kemp, and A. Tanner. (2015). "Examining the contribution of critical visualisation to information security". In: *Proceedings of the 2015 New Security Paradigms Workshop*. 59–72.

Haney, J. M. and W. G. Lutters. (2017). "Skills and Characteristics of Successful Cybersecurity Advocates." In: *SOUPS*.

Hansen, L. (2000). "The Little Mermaid's silent security dilemma and the absence of gender in the Copenhagen School". *Millennium*. 29(2): 285–306.

Hansen, L. and H. Nissenbaum. (2009). "Digital disaster, cyber security, and the Copenhagen School". *International studies quarterly*. 53(4): 1155–1175.

Harbach, M., M. Hettig, S. Weber, and M. Smith. (2014). "Using personal examples to improve risk communication for security & privacy decisions". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM. 2647–2656.

Harding, M., B. Knowles, N. Davies, and M. Rouncefield. (2015). "HCI, civic engagement & trust". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2833–2842.

Herley, C., P. C. Van Oorschot, and A. S. Patrick. (2009). "Passwords: If we're so smart, why are we still using them?" In: *International Conference on Financial Cryptography and Data Security*. Springer. 230–237.

HMG. (2012). "Government Digital Strategy". https://www.gov.uk/government/publications/government-digital-strategy.

HMG. (2019). "The Cross Government Transformation". https://www.gov.uk/government/collections/the-cross-government-transformation-programme.

Hoogensen, G. and S. V. Rottem. (2004). "Gender Identity and the Subject of Security". *Security Dialogue*. 35(2): 155–171.

Hooper, C. (2001). *Manly states: Masculinities, international relations, and gender politics*. Columbia University Press.

Howard, M. and S. Lipner. (2006). *The security development lifecycle*. Vol. 8. Microsoft Press Redmond.

Hudson, H. (2005). "'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security". *Security Dialogue*. 36(2): 155–174.

Hudson, N. F., A. Kreidenweis, and C. Carpenter. (2013). "Human security". In: *Critical approaches to security*. Routledge. 24–36.

Huysman, M., V. Wulf, *et al.* (2004). *Social capital and information technology*. Mit Press.

Huysmans, J. (2011). "What's in an act? On security speech acts and little security nothings". *Security dialogue*. 42(4-5): 371–383.

Inglesant, P. G. and M. A. Sasse. (2010). "The true cost of unusable password policies: password use in the wild". In: ACM.

Kaldor, M. (2007). *Human security*. Polity.

Kiran, A. H. and P.-P. Verbeek. (2010). "Trusting our selves to technology". *Knowledge, Technology & Policy*. 23(3-4): 409–427.

Kirlappos, I., S. Parkin, and M. A. Sasse. (2014). "Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security". In:

Kitchin, R. and M. Dodge. (2011). *Code/space: Software and everyday life*. Mit Press.

Knowles, B. and V. L. Hanson. (2018). "Older adults' deployment of 'distrust'". *ACM Transactions on Computer-Human Interaction (TOCHI)*. 25(4): 1–25.

Kocksch, L., M. Korn, A. Poller, and S. Wagenknecht. (2018). "Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices". *Proceedings of the ACM on Human-Computer Interaction*. 2(CSCW): 1–20.

Kuutti, K. (2013). "'Practice turn'and CSCW identity". *ECSCW 2013 Adjunct Proceedings*: 39–44.

Kuutti, K. and L. J. Bannon. (2014). "The turn to practice in HCI: towards a research agenda". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3543–3552.

Le Dantec, C. (2012). "Participation and publics: supporting community engagement". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1351–1360.

Le Dantec, C. A. (2016). *Designing publics*. MIT Press.

Le Dantec, C. A., J. E. Christensen, M. Bailey, R. G. Farrell, J. B. Ellis, C. M. Danis, W. A. Kellogg, and W. K. Edwards. (2010). "A tale of two publics: Democratizing design at the margins". In: *Proceedings of the 8th acm conference on designing interactive systems*. 11–20.

Lefebvre, H. and C. Levich. (1987). "The everyday and everydayness". *Yale French Studies*. (73): 7–11.

Lester, H. D., G. B. McKay, and E. A. Lester. (2019). "Sociotechnical systems for high rise detention". In: *Transdisciplinary Engineering for Complex Socio-technical Systems: Proceedings of the 26th ISTE International Conference on Transdisciplinary Engineering, July 30–August 1, 2019*. Vol. 10. IOS Press. 319.

Lewis, J. D. and A. Weigert. (1985). "Trust as a social reality". *Social forces*. 63(4): 967–985.

Lewis, M., L. Coles-Kemp, *et al.* (2014). "A tactile visual library to support user experience storytelling". *DS 81: Proceedings of NordDesign 2014, Espoo, Finland 27-29th August 2014*: 386–395.

Light, A. and L. Coles-Kemp. (2013). "Granddaughter beware! an intergenerational case study of managing trust issues in the use of Facebook". In: *International Conference on Trust and Trustworthy Computing*. Springer. 196–204.

Lippmann, W. *et al.* (1943). "US foreign policy: Shield of the republic".

Lipschutz, R. D. (1995). *On security*. Columbia University Press.

Lopez, T., M. Petre, and B. Nuseibeh. (2012). "Getting at ephemeral flaws". In: *Proceedings of the 5th International Workshop on Cooperative and Human Aspects of Software Engineering*. IEEE Press. 90–92.

Lovejoy, K. and G. D. Saxton. (2012). "Information, community, and action: How nonprofit organizations use social media". *Journal of computer-mediated communication*. 17(3): 337–353.

Luhmann, N. (2000). "Familiarity, confidence, trust: Problems and alternatives". *Trust: Making and breaking cooperative relations*. 6: 94–107.

MacEwan, N. F. (2017). "Responsibilisation, rules and rule-following concerning cyber security: findings from small business case studies in the UK". *PhD thesis*. University of Southampton.

Martina, J. E., E. Dos Santos, M. C. Carlos, G. Price, and R. F. Custódio. (2015). "An adaptive threat model for security ceremonies". *International Journal of Information Security*. 14(2): 103–121.

Mattelmäki, T. *et al.* (2006). *Design probes*. Aalto University.

Matthews, T., K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo. (2017). "Stories from survivors: Privacy & security practices when coping with intimate partner abuse". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2189–2201.

McCarthy, J. and P. Wright. (2004). "Technology as experience". *interactions*. 11(5): 42–43.

McLoughlin, I. and R. Wilson. (2013). *Digital government at work: a social informatics perspective*. OUP Oxford.

Miettinen, R., D. Samra-Fredericks, and D. Yanow. (2009). "Re-turn to practice: An introductory essay". *Organization studies*. 30(12): 1309–1327.

Mollering, G. (2006). *Trust: Reason, routine, reflexivity*. Emerald Group Publishing.

Molotch, H. (2013). "Everyday security: Default to decency". *IEEE Security & Privacy*. 11(6): 84–87.

Mols, F., S. A. Haslam, J. Jetten, and N. K. Steffens. (2015). "Why a nudge is not enough: A social identity critique of governance by stealth". *European Journal of Political Research*. 54(1): 81–98.

Muir, R. and I. Parker. (2014). *Many to many: How the relational state will transform public services*. IPPR.

Müller, C., C. Neufeldt, D. Randall, and V. Wulf. (2012). "ICT-development in residential care settings: sensitizing design to the life circumstances of the residents of a care home". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2639–2648.

Nadi, S., S. Krüger, M. Mezini, and E. Bodden. (2016). "Jumping through hoops: Why do Java developers struggle with cryptography APIs?" In: *Proceedings of the 38th International Conference on Software Engineering*. ACM. 935–946.

NCSC. (2019). "You Shape Security". https://www.ncsc.gov.uk/collection/you-shape-security.

Nicholson, J., L. Coventry, and P. Briggs. (2017). "Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection". In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 285–298.

Nicholson, J., L. Coventry, and P. Briggs. (2019). "If It's Important It Will Be A Headline: Cybersecurity Information Seeking in Older Adults". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. 349.

Nicolini, D. (2012). *Practice theory, work, and organization: An introduction*. OUP Oxford.

Nissenbaum, H. (2005). "Where computer security meets national security". *Ethics and Information Technology*. 7(2): 61–73.

Nyman, J. (2013). "Securitization theory". In: *Critical approaches to security*. Routledge. 51–62.

Olivier, P. and P. Wright. (2015). "Digital civics: Taking a local turn". *interactions*. 22(4): 61–63.

OpenUniversity. (2020). "Motivating Jenny". https://www.motivatingjenny.org.

Parkin, S., T. Patel, I. Lopez-Neira, and L. Tanczer. (2019). "Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse". In: *Proceedings of the New Security Paradigms Workshop*. 1–15.

Peacock, S. and D. Al-Shahrabi. "HCI, Digital Civics and the Refugee Crisis: Challenges at the Intersection of the Field".

Pham, H. C., L. Brennan, and S. Furnell. (2019). "Information security burnout: Identification of sources and mitigating factors from security demands and resources". *Journal of Information Security and Applications*. 46: 96–107.

Pierce, J. (2019). "Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. 45.

Pieters, W. (2011). "Representing humans in system security models: An actor-network approach." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 2(1): 75–92.

Potter, B. (2009). "Microsoft SDL threat modelling tool". *Network Security*. 2009(1): 15–18.

Power, M. (1994). *The audit explosion*. No. 7. Demos.

Probst, C. W. and R. R. Hansen. (2008). "An extensible analysable system model". *Information security technical report*. 13(4): 235–246.

Probst, C. W., R. R. Hansen, and F. Nielson. (2006). "Where can an insider attack?" In: *International Workshop on Formal Aspects in Security and Trust*. Springer. 127–142.

Puussaar, A., I. G. Johnson, K. Montague, P. James, and P. Wright. (2019). "Making Open Data Work for Civic Advocacy". *CSCW Paper, In Press*.

Reinfelder, L., R. Landwirth, and Z. Benenson. (2019). "Security Managers Are Not The Enemy Either". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM. 433.

Renaud, K. (2011). "Blaming noncompliance is too convenient: What really causes information breaches?" *IEEE Security & Privacy*. 10(3): 57–63.

Renaud, K., S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron. (2018). "Is the responsibilization of the cyber security risk reasonable and judicious?" *computers & security*. 78: 198–211.

Riegelsberger, J., M. A. Sasse, and J. D. McCarthy. (2005). "The mechanics of trust: A framework for research and design". *International Journal of Human-Computer Studies*. 62(3): 381–422.

RISCS. (2018). "Annual Report 2018". https://www.riscs.org.uk/wp-content/uploads/2019/03/2018-RISCS-Annual-Report.pdf.

Roe, P. (2008). "The 'value' of positive security". *Review of international studies*. 34(4): 777–794.

Rogaway, P. (2009). "Practice-oriented provable security and the social construction of cryptography". *Unpublished essay*.

Rosenberg, S. (2008). *Dreaming in Code: Two Dozen Programmers, Three Years, 4,732 Bugs, and One Quest for Transcendent Software*. Three Rivers Press. ISBN: 9781400082476.

Rossitto, C., M. Normark, and L. Barkhuus. (2017). "Interactive Performance as a Means of Civic Dialogue". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM. 4850–4862.

Saltzer, J. H. and M. D. Schroeder. (1975). "The protection of information in computer systems". *Proceedings of the IEEE*. 63(9): 1278–1308.

Schmidt, K. (2014). "The concept of 'practice': What's the point?" In: *COOP 2014-Proceedings of the 11th International Conference on the Design of Cooperative Systems, 27-30 May 2014, Nice (France)*. Springer. 427–444.

Schofield, T., J. Vines, T. Higham, E. Carter, M. Atken, and A. Golding. (2013). "Trigger shift: participatory design of an augmented theatrical performance with young people". In: *Proceedings of the 9th ACM Conference on Creativity & Cognition*. ACM. 203–212.

Schorch, M., L. Wan, D. W. Randall, and V. Wulf. (2016). "Designing for those who are overlooked: Insider perspectives on care practices and cooperative work of elderly informal caregivers". In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. 787–799.

Shea, P. (2016). "Civic practices, design, and makerspaces". *Negotiating digital citizenship: Control, contest and culture*: 231–246.

Shires, J. (2019). "Family Resemblance or Family Argument? Three Perspectives on Cybersecurity and their Interactions". *St Antony's International Review*. 15(1): 18–36.

Shires, J. (2020). "Cyber-noir: Cybersecurity and popular culture". *Contemporary Security Policy*. 41(1): 82–107.

Shostack, A. (2008). "Experiences Threat Modeling at Microsoft." In: *MODSEC@ MoDELS*.

Singh, S., A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. (2007). "Password sharing: implications for security design based on social practice". In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM. 895–904.

Sismondo, S. (2010). *An introduction to science and technology studies*. Vol. 1. Wiley-Blackwell Chichester.

Smith, G. M. (2005). "Into Cerberus' Lair: Bringing the Idea of Security to Light". *The British Journal of Politics & International Relations*. 7(4): 485–507.

Stanton, B., M. F. Theofanos, S. S. Prettyman, and S. Furman. (2016). "Security fatigue". *IT Professional*. 18(5): 26–32.

Stevens, G. and V. Wulf. (2002). "A new dimension in access control: Studying maintenance engineering across organizational boundaries". In: *Proceedings of the 2002 ACM conference on Computer supported cooperative work*. 196–205.

Stevens, T. (2013). *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Taylor & Francis.

Stewart, G. and D. Lacey. (2012). "Death by a thousand facts: Criticising the technocratic approach to information security awareness". *Information Management & Computer Security*. 20(1): 29–38.

Strohmayer, A., M. Laing, and R. Comber. (2017). "Technologies and social justice outcomes in sex work charities: fighting stigma, saving lives". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3352–3364.

Taylor, A. S., S. Lindley, T. Regan, D. Sweeney, V. Vlachokyriakos, L. Grainger, and J. Lingel. (2015). "Data-in-place: Thinking through the relations between data and community". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM. 2863–2872.

Tronto, J. C. (1993). *Moral boundaries: A political argument for an ethic of care*. Psychology Press.

UKRI. (2020). "UKRI Grants". https://gtr.ukri.org/person/7CBB849B-4C10-46F9-9B14-F00670C59A10.

Vaughan-Williams, N. and D. Stevens. (2016). "Vernacular theories of everyday (in) security: The disruptive potential of non-elite knowledge". *Security Dialogue*. 47(1): 40–58.

Vines, J., M. Blythe, P. Dunphy, V. Vlachokyriakos, I. Teece, A. Monk, and P. Olivier. (2012). "Cheque mates: participatory design of digital payments with eighty somethings". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1189–1198.

Vines, J., R. Clarke, P. Wright, J. McCarthy, and P. Olivier. (2013). "Configuring participation: on how we involve people in design". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 429–438.

Vlachokyriakos, V., C. Crivellaro, C. A. Le Dantec, E. Gordon, P. Wright, and P. Olivier. (2016). "Digital civics: Citizen empowerment with and through technology". In: *Proceedings of the 2016 CHI conference extended abstracts on human factors in computing systems*. ACM. 1096–1099.

VOME. (2010). "VOME Website". http://vome.uk/.

Weir, C., A. Rashid, and J. Noble. (2016). "Reaching the masses: A new subdiscipline of app programmer education". In: *Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering*. ACM. 936–939.

Wensveen, S., K. Overbeeke, and T. Djajadiningrat. (2000). "Touch me, hit me and I know how you feel: a design approach to emotionally rich interaction". In: *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques*. ACM. 48–52.

Whitworth, S. (1994). *Feminism and international relations: towards a political economy of gender in interstate and non-governmental institutions*. Springer.

Whyte, C. (2018). "Crossing the digital divide: Monism, dualism and the reason collective action is critical for cyber theory production". *Politics and Governance*. 6(2): 73.

Wibben, A. T. (2010). "Feminist security studies". In: *The Routledge Handbook of Security Studies*. Routledge. 84–94.

Wixon, D., K. Holtzblatt, and S. Knox. (1990). "Contextual design: an emergent view of system design". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Citeseer. 329–336.

Wolfers, A. (1952). "" National security" as an ambiguous symbol". *Political science quarterly*. 67(4): 481–502.

Woltjer, R. (2017). "Workarounds and trade-offs in information security–an exploratory study". *Information & Computer Security*. 25(4): 402–420.

Zurko, M. E. and R. T. Simon. (1996). "User-centered security". In: *NSPW*. Vol. 96. Citeseer. 27–33.