Introduction

When Bill Gates stepped down as the head of Microsoft in 2008, he said that when he and the late Paul Allen had started the company they had dreamt about putting a computer in every home (Beaumont, 2008). Much has changed since the mid-1970s, when this ambitious vision was set out, but, with 83.2 per cent of households in the developed world now containing a computer, it appears self-evident that the late twentieth and the twenty-first centuries have seen a rapid process of computerisation unfold (ITU, 2018). Alongside the proliferation of affordable computers we have also witnessed the emergence and spread of the internet and the World Wide Web, a development that has brought with it huge increases in interconnectivity at the national and international, public and private levels (Harknett, 2003, p. 18). On this issue there are clear discrepancies between the developed and developing world, with estimated internet usage standing at 80.9 per cent and 45.3 per cent respectively (ITU, 2018). However, the global trend remains one of increased digital connectivity and has subsequently produced significant societal change.

The result of these developments has been swathes of the globe in which networked computer technology is a firmly established feature and where little remains untouched by its influence: consumerism, entertainment, communication, business, everything from managing your finances online to logging exercise via wearable technology. There are near constant reminders of the information age's presence, in our pockets, on our wrists, in our homes, at work, and this ever present feature in our daily lives is only part of the story of the 'computer revolution'. The process of computerisation has produced change at all levels – a dizzying proliferation of technology and platforms has sprawled throughout society, empowering actors and institutions, allowing for greater autonomy and independence but also collaboration and cooperation.

The voice of the individual can be louder than ever, the reach of enterprise wider than ever and the functioning of the State similarly amplified.

A question that has frequently been asked about this transformation is whether it should be viewed in a positive light or not. Despite all of the observable benefits of global connectivity, there remains scepticism around issues such as the (often anonymous) unsavoury or illegal behaviour that this connectivity has empowered, the infringements upon the privacy of individuals in the form of big data collection or systems of mass-surveillance and the spread of misinformation. Put another way, issues of (in)security are not far detached from questions around the societal value of computers and computer networks. How we conceptualise security relies on assumptions *about* security, including deciding whom or what requires securing (Jarvis and Holland, 2015).

However, if we focus momentarily on the most commonly cited referent object (the state) we see how national security strategies consistently reproduce this idea that computerisation is a 'double-edged sword' (Quigley *et al.*, 2015, p. 108), where the tremendous societal and economic benefits it offers must be considered alongside the risks and drawbacks. National cybersecurity strategies the world over reveal the commonality of this perceived trade-off:

> The broad application of information technologies and the rise and development of cyberspace has extremely greatly stimulated economic and social flourishing and progress, but at the same time, has also brought new security risks and challenges. (China Copyright and Media, 2016)

> The UK is one of the world's leading digital nations. Much of our prosperity now depends on our ability to secure our technology, data and networks from the many threats we face. Yet cyber attacks are growing more frequent, sophisticated and damaging when they succeed. So we are taking decisive action to protect both our economy and the privacy of UK citizens. (HM Government (UK), 2016)

> An engine of innovation and wonder, today the Internet connects nearly every person on the planet, helps deliver goods and services all over the globe, and brings ideas and knowledge to those who would otherwise lack access. The United States relies on the Internet and the systems and data of cyberspace for a wide range of critical services. This reliance leaves all of us – individuals, militaries, businesses schools, and government – vulnerable in the face of a real and dangerous cyber threat. (Department of Defense Cyber Strategy (US), 2015)

> The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The domain is transforming our economy and security posture more than ever before, creating opportunities for

> innovations and the means to improve general welfare of the citizens. It is transforming many countries' growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas. However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security. Sensitive data, networks and systems that we now trust can be compromised or impaired, in a fashion that detection or defence can be hard, thus undermining our confidence in a connected economy. (Nigerian Computer Emergency Response Team, 2014)

The vulnerability and risk referenced across all of these excerpts manifests as a diverse series of threats, including rival foreign powers and sub-State actors who utilise a variety of computer-facilitated techniques with the aim of degrading the defensive ability of the State or enhancing their own strategic advantage. Viewed as acts of aggression and threats to national security by familiar foes, the State has responded by expanding the national security agenda to incorporate the domain of 'cybersecurity'. Indeed, while cybersecurity is considered a 'broad' and 'indistinct' term (Carr, 2016, p. 49) upon which 'no one can agree precisely' (Bambauer, 2012, p. 587), it is often conflated with the broader national security agenda (Mueller, 2017, p. 419). Stevens (2016, p. 11) offers one such broad definition that usefully captures two distinct aspects of the concept when he writes that cybersecurity is 'a means not only of protecting and defending society and its essential information infrastructures but also a way of prosecuting national and international policies through information-technological means'.

Despite the secondary focus of Stevens's definition that includes the pursuit of policy via information technology, cybersecurity is predominantly discussed in relation to a reactive and defensive strategy designed to address vulnerabilities. These vulnerabilities are not abstract, but tangible weaknesses or flaws within the hardware or software of a system that can subsequently be exploited by malicious actors to compromise the integrity, availability or confidentiality of a resource (Dunn Cavelty, 2018, p. 24). Where such vulnerabilities exist, systems can be exploited to allow modification unbeknown to operators, rendered inaccessible to users or accessed without authorisation. Any of these actions compromise the security of the system and can allow for all manner of more specific consequences, from the stealing of sensitive data to the deliberate sabotage of a process (Dunn Cavelty, 2018, p. 24).

Such vulnerabilities are a feature of these systems, the product of their being built, written or operated by fallible humans. They present risks but the potential impact of these risks is compounded and exacerbated when taken alongside the trend discussed above, whereby digital technology and

interconnectivity become so seamlessly and completely threaded into society that these societies are *dependent* upon their smooth functioning (Kizza, 2014, p. 76). 'Cyberspace' has therefore become the focus of a successful securitisation, whereby a raft of new security risks have emerged that have seen governments across the world respond in their capacity as guarantors of security.

These vulnerabilities, and this dependency, have coincided with 'cyber-threats'[1] that are growing in scale and complexity to become increasingly 'asymmetric and global' (HM Government, 2015, p. 19). Efforts to defend 'the digital homeland' have thus required responses on a par with more familiar endeavours such as counter-terrorism (Farmer, 2017). A prominent example of a 'new' security challenge, cybersecurity has quickly moved to the top of national security agendas and has been the subject of significant international attention. However, these developments have not come without differences of opinion and controversy, in particular around a perceived trade-off between security online and privacy, the allocation of particular resources and legislative responses.

In 2020, cybersecurity is very much a part of the national security framework. It is a well-established part of our security imaginaries, and the landscape of discussion and practice herein appears set. Stevens, however, reminds us that there is contestation around what is *meant* by cybersecurity and while this is 'regrettable to some … [it] … also offers opportunities for productive engagements with cybersecurity that interrogate and contest an unsettled field of policy and practice' (Stevens, 2018, p. 1). Dominant discourse is premised upon a particular understanding of cybersecurity (as national security), which has helped structure this field in a way that shares many of the engrained assumptions of realism. However, this is ultimately a contingent knowledge that our investigations can help to expose by revealing the power relations in effect.

This book aims to better understand the construction of this 'cyber security imaginary' (Stevens, 2015), as well as its implications, by exploring private-sector industry expert discourse and the relationships that exist with this source and others. To achieve this I will aim to: first, explore the organisation of dominant cybersecurity knowledge. Second, I will demonstrate the importance of expert knowledge contained within the private sector in the aforementioned construction and finally show how relationships between this source and others have powerful constitutive effects that solidify the conditions of possibility for the extension of a strategy of neoliberal governance.

Motivations, aims, questions and assumptions

Given the desire to better understand how cybersecurity has been framed via the process of social construction, the decision to focus on a particular aspect of the internet security industry[2] may appear less intuitive than other more commonly studied 'sources', such as elite political or popular media discourse. It might also be argued that these are more important or influential in shaping collective consciousness and security practices. I contest these assumptions and explore the importance of industry knowledge on the constitutive process in depth in Chapter 3. However, in this Introduction I provide two main motivations for my decision to focus on the following specific areas.

First, I have focused upon private-sector internet security expertise because doing so pays due regard to the trend towards an increasing privatisation/commercialisation of security (Krahmann, 2003; Leander, 2010) and the proliferation of alternative *expert* discourses that goes beyond the traditional public-sector professionals of politics and security. As this trend continues, so too does private industry's increasing influence and stake in constructing security knowledge, including the constitution of referents and threats. Cybersecurity is no exception to this phenomenon and in the internet security industry we have a wide collection of private firms that generate a specific expert discourse as well as a range of products and services linked to the alleviation of the sorts of threats found within this space. The expert status of these companies, in conjunction with the technified nature of the field (Hansen and Nissenbaum, 2009, p. 1157), leaves this site of discourse uniquely placed to speak to the 'reality' of such threats.

The second motivation is that focusing, as I do, on this industry provides a useful means with which to develop existing cybersecurity research. There are two elements to this: first, despite an increased role within security for the private sector and the emergence of a dedicated internet security industry, there remains a dearth of engagement with these sorts of experts. Instead there has been a tendency to focus on more 'visible political figures' without sufficient consideration given to how their discursive practices 'are facilitated or thwarted by preceding and preparatory linguistic and non-linguistic practices of actors that are not as easily visible, also outside of government' (Dunn Cavelty, 2016, p. 371). This is surprising given the unique claims to epistemic authority that those within this industry have and the ability of these actors to mobilise expert/scientific capital in the production of 'objective' and

'politically neutral' forms of knowledge. Second, while a distinct critical (broadly constructivist) research agenda does certainly exist in relation to cybersecurity (see Chapter 1), it is very much overshadowed by an objectivist and largely realist research project (McCarthy, 2018, p. 5). The research conducted in this book eschews the assumptions underpinning much of this research and argues that by analysing the discourse of internet security companies, we can better understand the intricacies of the constitutive process of knowledge formation that has taken place around cybersecurity. In doing so we can, in this instance, shed light on the importance of these security professionals and develop our understanding of the logics and orthodoxies that are a feature therein as well as the security practices that have been enacted as a result.

Having covered my motivations for focusing on this industry, I will achieve my aims by responding to three sets of overarching questions. First, the book aims to establish the landscape of cybersecurity research to date as a means to situate my own study and determine the significance of the constructions found within this section of private-sector internet security discourse. For example, what assumptions underpin cybersecurity research? Are particular ontological, epistemological, methodological and theoretical commitments more commonplace than others? Is there a discernible homogeneity to what has gone before, or is the landscape characterised by divergence and disagreement? What can be learned from the state of cybersecurity research and where are the gaps in this research that could be usefully pursued to further our understanding?

The book's second aim responds to the question, how is cybersecurity constructed within private-sector internet security discourse? Where, for example, do the companies studied and the experts speaking for them place the focus within this domain? How are they understanding and delimiting 'cybersecurity', 'cyberspace' or 'cyber-threats'? What is their assessment with regards to threat: are they reassured, anxious, alarmed? What themes, tropes and tactics are utilised within this site of discourse to communicate the subject matter? What strategies do they have, if any, to respond to the challenges found within cyberspace? Do these companies speak as a homogenous voice or is there heterogeneity in their understandings and assessments?

Finally, the book aims to answer the 'So what?' question and considers the significance and impact of internet security discourse as part of both the broader inter-subjective process of knowledge construction and the enactment of related security practices. How, if at all, does cybersecurity knowledge in this domain differ from that produced in alternative domains? What is the specific

importance of this expert knowledge in structuring popular or elite understandings of what (in)security and risk look like in cyberspace? How can we determine this? What are the ethical and normative consequences of the answers to these sub-questions?

These questions do not have straightforward answers and require detailed theoretical work if headway is to be made. I outline my own theoretical commitments in relation to several core concepts in Chapter 2 of the book, but it is worth noting here that the argument I gradually outline over the course of the following chapters operates with particular conceptualisations of power, knowledge and security that, I argue, adds value to the cybersecurity debate. I do, however, accept that these conceptualisations do not always lend themselves to the clear prescription/assessment/diagnosis that is a more familiar feature of the majority of cybersecurity and indeed security literature. However, while I am operating outside the conventions of much of the cybersecurity literature, I am certainly not in uncharted theoretical and methodological territory and I seek to clarify this in the latter part of Chapter 1. Nevertheless, although the questions I am setting out to answer, and the arguments I will develop, over the course of the book are purposively rejecting some of the assumptions made by much of the previous research, they do rest on at least two assumptions of my own.

First, is the understanding that 'cybersecurity' and 'cyber-threats' do not exist as objective, material phenomena that are able to be captured in our labels and risk assessments, but, rather, are constructed and constituted via a network of competing knowledge claims (Epstein, 2013). Our definitions, understandings and assessments of cyber-threats – in academia, news media, politics, law, industry and elsewhere – create that which they purport only to describe. Cyber-threats are produced through attempts to establish their meaning and significance, with each knowledge claim itself embedded in deeper intertextualities that are reliant upon the posting of sameness and difference, and situated within a nexus of power relations. Cyber-threats are 'made' through inter-subjective social and discursive practices rather than existing extra-discursively. Rather than approaching cyber-threats as external and objective, this book recognises their contingent and constructed nature and consequently seeks to explore the process of construction, why certain knowledge claims gain prominence and what the implications of these are.

Second, and related to the previous assumption, I operate with the belief that the value of research is not found exclusively in its instrumental policy relevance but also in its critical value. To use the Coxian distinction, I therefore

adopt a critical theory approach to the subject matter rather than a problem-solving approach (Cox, 1981). I delve into the cybersecurity literature in Chapter 1 but to generalise for a moment here, the majority of cybersecurity knowledge tends to demonstrate its value by aiming to produce truer definitions, more accurate threat assessments or more effective responses. However, my own work rejects the notion that these sorts of conclusions are what constitute valuable research and instead sees this as unnecessarily circumscribing cybersecurity scholarship. With these assumptions in mind, my exploration of the questions I lay out above aim to make three main contributions of my own to academic cybersecurity knowledge.

First, I aim to add further theoretical depth into the study of cybersecurity, in the first instance, with regard to Foucault's work around power/knowledge, governmentality, the *dispositif* and security and, in the second instance, in relation to the role 'expertise' plays in the process of knowledge construction. By conducting this theoretical application across these two broad areas, I aim to better explain the capillary flow of power within the network that exists between different sources and the effect this has on the formation of a dominant cybersecurity knowledge.

Second, by focusing on the discourse produced by the internet security industry I aim to usefully expand the critical cybersecurity research project into sites of discourse previously unstudied by researchers. This is not to say that the only contribution here is to research a domain that remains previously unstudied, but rather that through studying the discourse of the internet security industry in this context I draw attention to an important regime of truth with a unique constitutive and delimiting function. In so doing, I also aim to contribute to a body of work that has sought to explore how security meaning is made in often-overlooked alternative discursive spaces (Robinson, 2014; Heath-Kelly and Jarvis, 2017).

Finally, I look to demonstrate the broader significance of the empirical work I have conducted and argue for how the tactics and tropes of this discourse resonate outside of the articles, white papers, threat assessments and blogs that make up some of the material considered. I attempt, therefore, to not only link the linguistic particularities of the material I have analysed to the dominant cybersecurity threat framing that exists, but also to show how the security professionals studied here have begun to form communities of mutual recognition with more established security and political professionals as part of a reorganisation of the security *dispositif*. This reorganisation has seen the strengthening of linkages between these different sources to aid in the

sedimentation of a specific cybersecurity knowledge which makes possible security and legislative responses, among other things.

Reflections on method

I elaborate upon methodology and method in more detail prior to the conclusion of Chapter 2, but it is worth reflecting briefly here upon how I have conducted the analysis that in part informs my answers to the questions I have posed thus far. The book concentrates on an analysis of a diverse range of documents published by eighteen internet security companies. These documents are made publicly available via the companies' websites[3] and have been analysed to identify how cybersecurity is understood within this site and what this can tell us about wider cybersecurity knowledge. The companies studied as part of this project are those probably best known for their anti-virus software; notable among these are the likes of Symantec, AVG and McAfee. This, of course, only represents one aspect of a far broader industry, and I have chosen to describe them as internet security companies rather than anti-virus vendors on account of the fact that using the latter term would give a misleading impression of the full range of products and services some of these companies offer; everything from anti-virus to workspace virtualisation (Symantec, 2019).

Other than the fact that they publish regularly on issues of cybersecurity and consist of the sorts of security professionals that I am interested in studying, these particular companies were selected for a range of purposive factors which included: accessibility via the presence of an internal online archive of content; their position in the industry; and language, such that the content was provided in the medium of English. All of the companies included can be considered 'international' insofar as they all make their products available to an international market and often have multiple offices around the globe. There was some considerable diversity when it came to where these companies' main headquarters were based, including: Spain, Germany, the US, Japan, South Korea, the UK, Romania, Russia, India, Canada, Finland, Slovakia, the Czech Republic and the Netherlands.

The material for this study was collected by searching through different archives within each company's website. In certain cases this entailed searching through over a decade of news articles, press releases and blogs; however, the amount of material and the variety of formats differed between companies. No limit was placed on how far backwards in time the search went;

however, the data collected went no further forward than 31 December 2013. Within these parameters the earliest document included in this corpus was published on 29 January 1997 and the latest included was published on 29 December 2013, giving a fifteen-year coverage.

Book organisation

The book begins, in Chapter 1, by providing an in-depth overview of existing cybersecurity knowledge drawn from various disciplines including politics and international relations, law and computer science. The first part of this chapter is structured around the organising themes of definition, threat and response, and provides an important foundation upon which subsequent theoretical and empirical work is based. This chapter identifies a broad homogeneity across this knowledge and demonstrates how it operates within a wider national security framing that reproduces the features, tropes and tactics found therein. However, in the second part of this chapter I also go beyond the 'problem-solving' conventions of cybersecurity knowledge to reveal a smaller body of critical and broadly constructivist research that investigates the same object, but in a manner that eschews the commonplace agenda. By highlighting this work I do two things: first, I situate my own study in a wider academic body of work that sets out to investigate cybersecurity by utilising different ontological, epistemological and methodological assumptions to those typically found in cybersecurity research. Second, by revealing this heterogeneity I project a path forward for my own theoretical and empirical work that recognises the importance of a broader inter-subjective process of knowledge construction which requires engagement with this part of the internet security industry.

Chapter 2 provides the theoretical framework for the book's empirical analysis and clarifies a number of theoretical and conceptual tools that are central to its objectives and contributions. Power and security are two such concepts and the chapter begins by clarifying the conceptualisation of power outlined by Michel Foucault by elaborating upon one of his ideas: power/knowledge. From here the chapter hones in on the 'third modality' of power, that of governmentality, to demonstrate how this functions across society and the role that the security *dispositif* plays in allowing this form of power to function. Prior to embarking on the empirical analysis, this chapter ties together the work on power, governance and security with established work on both 'epistemic communities' and 'security professionals'. I elaborate on these

theorisations to link the productive functioning of power with the role played by particular 'privileged' experts within the *dispositif* to give meaning to the phenomenon of security, sediment certain understandings, prioritise particular responses and foreclose alternative thinking. It is in this section that I most explicitly make the argument for the need to conduct constructivist research into private security industry expertise. Finally, the chapter draws to a close with reflections on methodology and method and addresses some questions that present when conducting a Foucauldian-inspired discourse analysis such as this.

Chapters 3 and 4 represent the book's main empirical contribution and illuminate how various discursive tactics have been deployed to sediment a particular cybersecurity knowledge, imbuing the space itself, as well as the phenomenon, within with particular characteristics that accentuate unease and risk. Chapter 3 begins the empirical analysis by conducting an analysis of 'cyberspace', characterised as the milieu within which (in)security plays out. Here, I reveal the vulnerable underpinnings that are an inherent feature of this space as well as how knowns and unknowns produce a threat that is unknowable in terms of timing and form, but inevitable in terms of its arrival. Chapter 4 continues the analysis, but shifts the focus from the 'space' to the 'threats'. In this chapter I consider how danger and destructiveness are constituted as self-evident features of various nefarious acts executed by a diverse range of actors that present salient and credible threats in the present as well as the future.

In both of these chapters the focus is placed primarily on how this specific expert site of discourse produces a particular and largely apprehensive risk knowledge around computers, networks, the internet, devices, etc. However, the message is not a wholly homogenous one and, indeed, in both of these chapters, efforts are made to identify the scepticism and contestation that exist and that lead experts to question the accuracy or focus of fellow experts' claims, in order for me to reveal a less overt counter-hegemonic discourse. These seeds of scepticism – as well as a dearth of examples of cyber-terrorism or cyber-war, despite over a decade of conversation about their imminence or arrival – present alternative (expert) framings and understandings as well as disrupting the cohesiveness of dominant cybersecurity discourse.

Chapter 5 draws together all these previous threads to reflect on the importance of the internet security industry in the construction of cybersecurity knowledge and the role that relationships between private entities and professionals of politics plays in the sedimentation of cybersecurity as analogous with national security. I begin by highlighting the broad homogeneity that exists

between the expert discourse that I have studied and the 'dominant threat frame' identified by others such as Dunn Cavelty (2008) before theorising as to why this is and what impact it has on a broader process of knowledge construction. To achieve this, I pay particular attention to the position and *raison d'être* of the companies I have studied as well as the formation of communities of mutual recognition that have provided benefits for both the industry and the state. I conclude that the arrival of the 'technological age' poses challenges to the traditional Weberian model of security governance. Subsequently, there has been an expansion and reorganisation of the security *dispositif* to more fully include private expertise as a means of overcoming a sovereignty gap, allowing for the continuation of a strategy of neoliberal governance. In the book's conclusion I summarise the main contributions of my research and reflect upon how similarly motivated constructivist research in this domain could provide scope for further development.