Introduction

> For tribal man space was the uncontrollable mystery.
>
> For technological man it is time that occupies the same role.
>
> (McLuhan 2002: 85)

Security is an inherently temporal proposition. In the modern political philosophical tradition, security is an essential bulwark against the exigencies of an unknowable future. For Thomas Hobbes, whose *Leviathan* (1651) is a foundation of Western political theory, security is the antidote to a situation in which man, 'in the care of future time, hath his heart all day long, gnawed on by feare of death, poverty, or other calamity; and has no repose, nor pause of his anxiety, but in sleep' (Hobbes 1996: 76). Security arises as a central feature of the social contract between people and the state, in which the pursuit and practices of security are invoked to calm the jittery present by the imposition of order on times yet to come. Hobbes states elsewhere that diligence is always required: 'For we cannot tell the good and bad apart, hence even if there were fewer evil men than good men, good, decent people would still be saddled with the constant need to watch, distrust, anticipate and get the better of others, and to protect themselves by all possible means' (Hobbes 1998: 11). Security is an exercise in futurity, a perpetual search for ways to mitigate uncertainty and the potentialities of fear, conflict and violence, even as each living moment fades immediately into the past.

Security is always political, whether we believe security to be epiphenomenal to politics (Booth 2007) or foundational of politics (Dillon 1996). Like security, politics is perennially concerned with time. Every political act is always a 'process in time', oriented towards a particular end, the conception of which 'always implies a future reference, to a state which is either not yet in existence, and which would not come into existence if something were not done about it ... or, if already existent, would not remain unchanged' (Parsons 1949: 45). Expressed through policy, politics 'invariably functions in the future tense'; it is 'hortatory, not historical ... it is designed to "get people to do things" and is therefore

always future-oriented' (Graham 2001: 765). Even if the attainment of its material objectives can only lie ahead of it, politics is also concerned with the past through its constant appeals to history and memory. As a political practice, security is also retrospective, mining the past to frame the narratives of identity and destiny that legitimise and justify its interventions. In looking backwards as well as forwards, the tenses of time are both the friend and the enemy of security: the threat of time and the ungoverned processes of change are the reasons provided for the necessary enactments of security while the imagined times of past and future are cultural resources mobilised in support of these practices.

To note that security and politics are concerned with shaping the future in order to achieve particular ends is unremarkable and perhaps banal, as they are always so oriented. The more important issue is how security intervenes in the structures of time in order to achieve these outcomes. How does security attempt to regulate the future? What resources are mobilised in support of this objective? By what logics does security operate and what worldviews propel security itself, like the objects of its enduring gaze, into the unknowable future? This book addresses these questions through an examination of a particular form of security that has emerged in the late twentieth and early twenty-first centuries – that of cyber security. Cyber security is a response to the perceived risks and threats of the modern, global information-technological infrastructure most commonly glossed as 'the internet'. In broad terms, it is concerned with anyone or anything that communicates through digital, electronic means.

On a randomly chosen day in November 2014 alone, as the final draft of this book was being prepared, there were many cyber security stories in that day's news. *The Washington Post* reported that the Federal Bureau of Investigation (FBI) suspected Chinese government hackers of breaching the computer networks of the US Postal Service, compromising the personal data of 800,000 employees. While the Chinese were infiltrating American networks, US President Obama was in China, urging China once again to halt state-sponsored commercial cyber espionage and intellectual property theft. Elsewhere, security researchers revealed that hackers had siphoned sensitive commercial data from hotel wireless networks over a period of years, compromising the transactions of thousands of international business people. The *Financial Times* of London reported that Germany was to develop a new early warning system to detect foreign cyber attacks on its information technology infrastructures. In India, businesses were cutting cyber security budgets, despite a rise in commercial losses due to information security breaches. And all this without mentioning the continued fallout from Edward Snowden's

revelations about the National Security Agency and the Government Communications Headquarters' (GCHQ's) mass surveillance programmes, practices at the margins of legality, which have become inextricably bound up with cyber security as broadly imagined.

What binds these news stories together is the integration of computer networks, information and security as a fact of global politics and economics, and the unwelcome implications of some of the practices emerging from this conjunction. Cyber security is the suite of practices, processes and policies that have emerged to counter less desirable outgrowths of the global information society. However, it is evident from even the most cursory examination of the rapidly expanding corpus of cyber security literature that there is great fluidity in the definitions and terms employed in the discussion and pursuit of cyber security. These texts furnish the reader with a bewildering array of (often technical) nomenclatures and terminologies, which not uncommonly contradict one another or are to some degree internally inconsistent. Such a situation is probably to be expected, given that cyber security has complex historical and conceptual relationships with a wide range of practices, disciplines and communities, the vocabularies and dialects of which have been transferred and translated into cyber security, not always intact and not always intelligibly. This slightly disorienting inability to settle upon mutually comprehensible language is by no means unique to cyber security, but even as cyber security has risen swiftly up the agendas of governments, businesses, civil society and international organisations, it remains unclear to many quite what cyber security is or entails. One author notes rather mournfully that 'no one can agree precisely what cybersecurity means, or requires' (Bambauer 2012: 587). This situation is further compounded by prefixing terms like 'security' with those 'essential elements in the semantics of the information age' – cyber, digital, information, virtual, internet – which results in an 'arsenal of new expressions' that are used so promiscuously and with so little rigour that 'they can basically mean everything and nothing' (Dunn Cavelty 2008: 14; M.L. Mueller 2010: 159). This may be somewhat incoherent in practice, not to mention inconvenient for the researcher (Denning 2003).

For our current purposes, cyber security is a broad term connoting the contemporary apotheosis of a much longer relationship between information technology and security. It has its roots in a wide range of allied perspectives and practices that derive from the inter-relationships between information technology and security. Any consideration of cyber security, if it is to avoid accusations of being ahistorical, must recognise that the relationship between information technology and security is 'as old as society itself' (Latham 2003: 1). We need to

understand something of how cyber security has emerged from this relationship and where it sits with respect to the concept of security itself, a task attempted in the following section.

A brief history of cyber security

The digital electronic computer was created in the middle of the twentieth century, and its subsequent spread and implementation have been so remarkable that we turn instinctively to the computer when confronted with the term 'information technology' (Kline 2006). It would be a gross injustice to the historical origins of cyber security to reduce it to the existence of computers alone, but they retain a central material position in the evolving relationship between information technology and security. Prior to the invention of what we would today recognise as a computer, the term often referred to human 'computers', people employed to perform repetitive calculating tasks for the purposes of mathematics, astronomy and other processes that required collective problem-solving through relatively intensive labour (Grier 2005).

In one particularly resonant example, the eighteenth-century British Astronomer Royal Nevil Maskelyne employed a 'network of human computers' to calculate lunar distances and astronomical tables for his annual Nautical Almanac (Grier 2005: 27–33). In an early experiment in redundancy, each set of calculations was sent to two geographically separate computers to perform manually, a task often taking weeks, if not months. The computers passed their finished work to a central 'comparer', who would look for and correct errors and anomalies. If there were no discrepancies between the work of the pairs of computers, this was a sure sign of collusion and Maskelyne had no hesitation in firing the offenders. The redundancy built into his system ensured control not only over the quality of the calculations but also over the character of his employees, demonstrating that even the simplest of information technologies instantiates the politics of control.

'Computer' was still being used in 1942 to refer to persons involved in intensive data processing, although by this stage they had various mechanical calculators – slide rules and other devices – to assist them in their tasks (Ceruzzi 1991). In the mid-1950s, the term would still evoke visions of 'a calculating clerk, or perhaps a mechanical gadget to help you shoot down an aeroplane' (Collin 1993), and the US National Bureau of Standards only stopped referring to employees as computers as late as 1964 (Aloisio 2004: 47). It was only in 1945 that 'computer' began to be associated with machinery as well as people. Persons previously known as computers were to be referred to as 'operators'. A 'computer' would

signify 'a machine capable of carrying out automatically a succession of operations of this kind and of storing the necessary intermediate results' (Stibitz 1945, cited in Ceruzzi 1991: 240); that is, a programmable computer of the kind we would recognise today.

In common with its many analogue information-technological forebears, the origins of the modern digital computer were tightly bound to contemporary conditions of national security. From the Spartan military *scytale* ciphers to *les télégraphes Chappe* of revolutionary France, from Morse code and nineteenth-century electrical telegraphy to battlefield radios, the developmental links between information technologies and national security are many and mutually reinforcing. Scholars debate the exact paths along which 'the computer' developed, but there is little disagreement that early computing experienced a substantial injection of skills, ideas and resources courtesy of World War II. This was consistent with the long-standing military interest in tactical data processing and organisational adaptation and automation. In the military context, the increased information required to manage campaigns in the nineteenth century influenced the creation of general staffs for the purposes of more and better data processing. In turn, this led to ever-greater volumes of information circulating in the military machine and, in the twentieth century, to the adoption of computers to process it (van Creveld 1989: 235–49).

Another key driver was the demands of cryptography, the making and breaking of secret codes. The deciphering of the 'Enigma' codes by Allied cryptographers is regarded by many as a key factor in the eventual defeat of Germany in 1945, and the hardware they developed as among the first, if not the first, digital, electronic and programmable 'computers' (Copeland 2006). The making (encryption) and breaking (cryptanalysis) of secret codes and systems of signs have long been intimately related to the exercise of political power. In the modern world cryptography has become increasingly secularised and computerised and a core competency of militaries and intelligence agencies. That efficient information processors in the form of computers should emerge eventually in the military cryptological context of World War II is therefore not surprising.

After the war, government agencies, academic institutions and corporations took advantage of the mathematical capabilities of this new breed of machines and employed them for high-volume computational tasks. In this era of large-scale data processing, the relationship between computers and security was redefined from one contingent on the use of computers in pursuit of national security to a range of new security issues arising from the use and architecture of computing technologies themselves. The predominant view of information technologies until this time

had been one of military 'force enabler rather than a source of vulnerability' (Dunn Cavelty 2008: 41). These vulnerabilities were not perceived as security issues as such (although see Shannon 1949), but the types of multi-user systems deployed brought non-specialists into computing systems and with them a host of new and identifiable 'security' problems. In particular, 'time-sharing' practices developed in the 1960s and 1970s drove awareness of and research into computer security. These systems allowed multiple users to access computing resources concurrently, during which time any user's programs and data were held in central memory and hypothetically accessible by any other (Ceruzzi 2003: 154–8). Due to the possibilities of malicious behaviour, systems began to need protection from their users, and users from each other.

Universities could perhaps live with these possibilities, but the military could not, and the US defence sector was instrumental in developing new computer security theories and protocols, predicated on the notion that all programs and, by association, all users were potentially 'hostile' agents (Mackenzie and Pottinger 1997). System and data security would be maintained either by controlling access to computing resources based on levels of privilege granted to users by system administrators or by encrypting data. Sets of overarching design principles for modelling secure information systems were developed, whose contemporary influence persists. This period also saw the emergence of data protection legislation and international attempts to harmonise this legislation, like the Organisation for Economic Co-operation and Development (OECD) Guidelines on Trans-Border Data Flows and the Protection of Privacy. It was during this period that the first national and international computer security conferences were established, some of which continue today.

Additional security issues arose in relation to the accidental loss or deliberate disclosure of confidential data, particularly as many databases were administered by insurance companies, banks, airlines and other organisations with access to personal biographic, demographic and financial data. Public disquiet is illustrated by reactions to the use of computers for census purposes. The US Bureau of the Census was an early sponsor of computing research and development and used the famous UNIVAC machine in the 1950 census (McPherson and Alexander 1951). By 1970, public concerns about computer databases, specifically the possibility that access to confidential data might be granted to a range of government and private entities, were so great that Bureau employees dubbed the 1970 census the 'census of controversy' (Alterman 1969: 248–61). Privacy and confidentiality issues intermingled with worries over the scope and authority of the census as a whole, although in the event there was little impact on levels of public cooperation (Eckler 1972: 195–205). By contrast, the 1971

Netherlands census faced a high degree of public resistance and non-participation. This led to the cancellation of all further censuses and the generation of population counts by more traditional methods (Prewitt 2004). In the United Kingdom and elsewhere, the censuses of 1970–71 produced 'protests of a kind not hitherto encountered by census-takers' (Bulmer 1979: ix). Government responses were expressed as security measures and protocols designed not only to safeguard the confidentiality and privacy of personal data but also to counter the insecurity felt by citizens with respect to this newly computerised environment (e.g. Burnham 1983).

The growth in personal computing which characterised the 1980s further challenged these ambitions. The formal security verification and certification methods developed for earlier closed computing systems had less applicability in the more diverse technological milieux of distributed computer networks (MacKenzie and Pottinger 1997: 56). Companies and institutions deployed hundreds of thousands of personal computing terminals, while local data storage and manipulation bypassed the centralised security controls of mainframes and their specialised staff. Inexperienced first-time users were charged implicitly with security responsibilities; confidential data were stored, exchanged and lost – often via the recent innovation of portable 'floppy' disks – and the general availability of unsecured data proved a diverse and complex 'nightmare' for computer professionals (Highland 1983; Murray 1984). In the wake of these developments, legislation was introduced to deter criminal use of computer networks in the United States, through the *Computer Fraud and Abuse Act* (1986), and in the United Kingdom, through the *Computer Misuse Act* (1990).

Issues of network (in)security intensified further as national-level networks linked together geographically separated computing resources and these networks were in turn connected on a global scale. The advent of the internet brought with it new security issues and new ways of creating mischief in and through computer networks. The first computer 'worm' emerged in 1989, followed by a recognisable industrial 'computer security' sector. The first viruses began to infect millions of personal computers and email systems in the 1990s, leading to the development of anti-virus software. Worms, viruses and other forms of malicious software (malware) were usually indiscriminate but 'cyber attacks' became more targeted in the 2000s, with the first major breaches of credit card databases for criminal gain and a growing realisation of the impact on businesses of these incidents for customer trust and brand reputation.

In recent years, 'cyber security' has emerged as a security regime concerned ostensibly with the protection of infrastructural information

systems. The technologically advanced countries of North America, Europe and the Pacific Rim rely most heavily on these infrastructures, but they enable the exchange of information across all sectors of national and international life. The accidental failure or deliberate subversion or destruction of these information infrastructures have become matters of inter/national and economic security. These are the latest examples of an historical process of identifying infrastructural vulnerabilities as security issues worthy of a collective national security response (Blumenson 1999; Collier and Lakoff 2008).

Since the 1980s, 'cyber threats' and critical infrastructures have been linked, so that in the United States information technologies not only represented an opportunity to establish competitive advantage but were also viewed as a source of asymmetric vulnerability on account of this 'information edge' (Dunn Cavelty 2008: 46–7). Many malicious actors might be enticed to concentrate their efforts on the information networks of a state. Most focus today is on foreign actors using information technologies for strategic ends – other states, their proxies and terrorists – but also transnational criminals, insurgents and the 'insider threat' in business and government. To this list, we can add whistle-blowers, hacktivists and a range of hackers and crackers who pose security threats to government, industry and the public. These categories are not static and there has been increased fluidity in conceptions of what, for example, the act of 'hacking' connotes, or which states might sponsor acts of 'cyber espionage'.

The impression persists, right or wrong, that the bugs and other security defects of information systems can be exploited by adversaries, so that dependent critical infrastructural sectors – energy, finance, government, transport and so on – will cease to function, resulting in a range of societal 'cyber doom' scenarios (Dunn Cavelty 2008: 2–4). These sometimes invoke the names – if not quite the dynamics – of events like Pearl Harbor, Hurricane Katrina and 9/11. Political argumentation along these lines has been unhelpful at best, and cynical and counterproductive at worst, but there is little doubt that governments are right to be concerned with the possible effects of cyber (in)security and are seeking to rectify existing problems and to prevent future ones.

Governments are also – and in this they depart from viewing cyber security as a protective or preventive entity or process alone – looking to exploit 'cyberspace' for their own political, economic and, sometimes, cultural ends. This includes the use of information technologies as tools and vectors of military power and as agents of domestic surveillance and control. Engineers and technicians often observe that cyber security refers only to the technical integrity of information systems rather than the

communicative 'content' carried across them, but this is evidently not the view of governments. That surveillance and related practices are justified in terms of cyber security and national security indicates that regulation of expressive and symbolic content is as important to governmental perceptions of cyber security as the physical and logical security of the information infrastructures which facilitate these communicative exchanges.

In the United Kingdom, cyber security is proposed on the one hand as the antidote to state-sponsored 'cyber attacks' on critical information infrastructures, as well as to the actions of 'cyber terrorists' and 'cyber criminals'. On the other, cyber security is framed as a means to create a more conducive environment for business, as well as affording government opportunities to exploit cyberspace as a means to achieve, inter alia, 'a potentially more effective and affordable way of achieving our national security objectives' (HM Government 2010a: 47). Similarly expressed, we may read in the United Kingdom's second national *Cyber Security Strategy* (2011) that cyber security entails both 'protecting our national interests in cyberspace' and the pro-active exploitation of 'the cyber environment for our own national security needs' (Cabinet Office 2011: 17, 26). In a traditional strategic sense, cyber security incorporates both offensive and defensive operations (Dunn 2007: 85). This offensive–defensive dichotomy is discernible in many primary documents and statements by politicians and public servants, although for political reasons it is not usually set out so obviously. Cyber security at home may translate into cyber insecurity abroad (Dunn Cavelty 2014).

The creeping militarisation of global information technologies has been noted since the early 2000s, as nations sought to gain strategic advantage through the military use of information technologies (Deibert 2003). Deibert notes the 'quiet expansion and adoption of offensive information warfare capabilities by states' over this period and the lead taken by the United States in an emerging 'cyber arms race' (Deibert 2008: 152–3). Concerned by the possibilities of escalation from *sub rosa* cyber skirmishing to all-out war, states have begun to enforce collective authority over the internet (Dunn and Mauer 2007: 152). There is not yet a global treaty on the military or political use of information technologies, but its potential parameters are a serious topic of discussion at the highest levels of international diplomacy (Hughes 2010). The Council of Europe Convention on Cybercrime (2001) is often proposed as an example of how national efforts may be harmonised to achieve international gains (Brown *et al.* 2009). Progress has long been hampered by the inability of leading powers to decide whether to prioritise their own high-level cyber capabilities or to protect the infrastructures on which those depend. At present, Western governments prefer to encourage the development of

norms of appropriate behaviour rather than a negotiated treaty instrument (Deibert and Crete-Nishihata 2012). These 'rules of the road' might help engender a putative but ill-defined 'global culture of cyber security' (Dunn and Mauer 2006).

We have yet to see an overt 'cyber war' between states, but offensive capabilities can and will be exploited for strategic ends (Betz and Stevens 2011). These are not just for the purposes of achieving military victory in war but play a central role in the cat-and-mouse games of inter-state diplomacy (e.g. Rawnsley 2009). In 2010, the revelation that a 'cyber weapon' dubbed Stuxnet was deployed in a presumed US-Israeli operation against Iranian nuclear assets was widely considered a game-changer in international affairs (Sanger 2012). In the absence of a developed body of precedence pertaining specifically to military actions in the 'cyber domain', military strategists and politicians have looked to history as a guide, with the Cold War being a particularly fertile – if problematic – source of ideas for emerging concepts like 'cyber arms control' and 'cyber deterrence' (Nye 2011; Stevens 2012). At the same time, we have seen concerted attempts to bring clarity to the applicability of international law to cyber warfare (Schmitt 2013) and the development of national doctrines for cyber warfare operations.

Despite the absence of a discernible war on the home front, cyber security is painted as the responsibility not only of government, its security agencies and the military but of industry – who own and operate most information infrastructures – and of ordinary citizens too. Remarkably, there has been sustained talk of creating civilian volunteer 'cyber militias' to assist in the defence of national interests (Klimburg 2010, 2011; Lawson and Gehl 2011). This 'whole-nation' approach to cyber security is in part explained by a simple observation: that the potential vectors of cyber (in)security are to be found not just in government communications networks, industrial control systems or commercial digital infrastructures but in the pockets and homes of citizens in the form of smartphones, personal computers and games consoles. Cyber security is ubiquitous, at least in material terms, and with its increasing focus on online content and expression is intruding into the actions of citizens ordinarily little concerned with the demands of national or economic security. There is also remarkable convergence of tactics and technologies between the governments of differing political hues, be they Asian autocracies or liberal democracies of the West.

This brief historical account of the evolution of cyber security is necessarily incomplete. The field is now so large and unwieldy that to do it historical justice would require a separate project of markedly different orientation to the present study. What is clear is that the development of