Cyber Security and the Politics of Time

‘Cyber security’ is a recent addition to the global security agenda, concerned with protecting states and citizens from the misuse of computer networks for war, terrorism, economic espionage and criminal gain. Many argue that the ubiquity of computer networks calls for robust and pervasive counter-measures, not least governments concerned at their potential effects on national and economic security. Drawing on critical literature in International Relations, security studies, political theory and social theory, this is the first book that describes how these visions of future cyber security are sustained in the communities that articulate them. Specifically, it shows that conceptions of time and temporality are foundational to the politics of cyber security. It explores how cyber security communities understand the past, present and future, thereby shaping cyber security as a political practice. Integrating a wide range of conceptual and empirical resources, this innovative book provides insight for scholars, practitioners and policymakers.

Tim Stevens is Teaching Fellow in the Department of Politics and International Relations, Royal Holloway, University of London. He is the co-author of *Cyberspace and the State* (2011) and has published widely on cyber security and related issues in journals like *International Political Sociology*, *Security Dialogue* and *Contemporary Security Policy*.

Cyber Security and the Politics of Time

Tim Stevens

King's College London

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107109421

First published 2016

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Stevens, Tim, 1973–
Cyber security and the politics of time / Tim Stevens, King's College London.
pages cm
ISBN 978-1-107-10942-1 (hardback)
1. Technology and international relations. 2. Internet and international relations. 3. Computer security – Government policy. 4. Cyberspace – Security measures – Government policy. 5. Computer networks – Security measures – Government policy. I. Title.
JZ1254.S74 2015
327.10285′58–dc23
2015016413

ISBN 978-1-107-10942-1 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Cyber Security and the Politics of Time

‘Cyber security’ is a recent addition to the global security agenda, concerned with protecting states and citizens from the misuse of computer networks for war, terrorism, economic espionage and criminal gain. Many argue that the ubiquity of computer networks calls for robust and pervasive counter-measures, not least governments concerned at their potential effects on national and economic security. Drawing on critical literature in International Relations, security studies, political theory and social theory, this is the first book that describes how these visions of future cyber security are sustained in the communities that articulate them. Specifically, it shows that conceptions of time and temporality are foundational to the politics of cyber security. It explores how cyber security communities understand the past, present and future, thereby shaping cyber security as a political practice. Integrating a wide range of conceptual and empirical resources, this innovative book provides insight for scholars, practitioners and policymakers.

Tim Stevens is Teaching Fellow in the Department of Politics and International Relations, Royal Holloway, University of London. He is the co-author of *Cyberspace and the State* (2011) and has published widely on cyber security and related issues in journals like *International Political Sociology*, *Security Dialogue* and *Contemporary Security Policy*.

Cyber Security and the Politics of Time

Tim Stevens

King's College London

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107109421

First published 2016

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Stevens, Tim, 1973–
Cyber security and the politics of time / Tim Stevens, King's College London.
pages cm
ISBN 978-1-107-10942-1 (hardback)
1. Technology and international relations. 2. Internet and international relations. 3. Computer security – Government policy. 4. Cyberspace – Security measures – Government policy. 5. Computer networks – Security measures – Government policy. I. Title.
JZ1254.S74 2015
327.10285′58–dc23
2015016413

ISBN 978-1-107-10942-1 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Cyber Security and the Politics of Time

'Cyber security' is a recent addition to the global security agenda, concerned with protecting states and citizens from the misuse of computer networks for war, terrorism, economic espionage and criminal gain. Many argue that the ubiquity of computer networks calls for robust and pervasive counter-measures, not least governments concerned at their potential effects on national and economic security. Drawing on critical literature in International Relations, security studies, political theory and social theory, this is the first book that describes how these visions of future cyber security are sustained in the communities that articulate them. Specifically, it shows that conceptions of time and temporality are foundational to the politics of cyber security. It explores how cyber security communities understand the past, present and future, thereby shaping cyber security as a political practice. Integrating a wide range of conceptual and empirical resources, this innovative book provides insight for scholars, practitioners and policymakers.

Tim Stevens is Teaching Fellow in the Department of Politics and International Relations, Royal Holloway, University of London. He is the co-author of *Cyberspace and the State* (2011) and has published widely on cyber security and related issues in journals like *International Political Sociology*, *Security Dialogue* and *Contemporary Security Policy*.

Cyber Security and the Politics of Time

Tim Stevens

King's College London

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107109421

First published 2016

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Stevens, Tim, 1973–
Cyber security and the politics of time / Tim Stevens, King's College London.
pages cm
ISBN 978-1-107-10942-1 (hardback)
1. Technology and international relations. 2. Internet and international relations. 3. Computer security – Government policy. 4. Cyberspace – Security measures – Government policy. 5. Computer networks – Security measures – Government policy. I. Title.
JZ1254.S74 2015
327.10285′58–dc23
2015016413

ISBN 978-1-107-10942-1 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

I dedicate this book to the memory of my maternal grandfather, Paul Pedrick McCord (1903–89), forester and soldier.

Contents

Acknowledgements

This book started life as a doctoral thesis undertaken at the Department of War Studies, King's College London. I am immensely grateful to David Betz, who marshalled the original project to completion with great humour and patience, and to Theo Farrell, who has long been an encouraging voice without whom neither thesis nor book would have been possible. Christopher Coker and Andrew Hoskins provided comments and insights that I am fortunate to be able to incorporate into this book. I also acknowledge the financial support of an Economic and Social Research Council studentship and the generous assistance of Charles Wolfson Townsley during my doctoral studies.

I have benefited greatly from the collegiality and wisdom of my King's colleagues, notably Neville Bolt, Frank Foley, Peter McBurney, Nick Michelsen, Richard Overill, Thomas Rid and John Stone. I am grateful to the following for illuminating discussions and help with research materials: David Bhowmik, Daniel Cordle, Kathryn Marie Fisher, Chris Fryer, Mike Innes, Jo Kovacik and Sean Lawson. Thanks also to my students for their provocations and enthusiasm and to the many online commentators who have shaped my thinking over many years. No one has been more generous than Gerry Judah, who allowed his artwork to grace the cover of this book. It is an enormous privilege to be associated even in some small way with an artist I have long admired.

John Haslam and his colleagues at Cambridge University Press have been a pleasure to work with and I am deeply appreciative of their professionalism. I would like to thank Sarah Green, Carrie Parkinson, Chloé Harries and, at Integra, Sri Hari Kumar. Josh Bryson compiled the index with alacrity and precision. I reserve special gratitude for three anonymous reviewers, whose critical commentary has improved the text immeasurably. They made me think afresh about some problematic issues but any residual errors are, of course, my own.

Thank you to all of my extended family for their generosity and forbearance. I am particularly fortunate to have the support of Luisa, who makes all things possible. Finally, the rambunctious presence of two small boys has often challenged productivity but without their cheerful chaos the relative order in this book may never have emerged. I owe them more than they know.

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 cyber security has been both long and complex. Importantly, it has emerged from considerations not only of computers and computer networks, or of their implications for national security, but with the security of individuals and their data, and with the security of societal infrastructures and the economy. At the beginning of the twenty-first century, cyber security is a key concern of modern, technologically advanced countries and of the international system more generally. In its ontological register, 'cyber security' connotes the pursuit of a condition free from cyber insecurity, that is, from the risks and threats engendered by the proliferation of digital information technologies and societies' reliance upon them. In its processual forms, cyber security encompasses a wide range of political and technical practices, ranging from the defensive and protective to the offensive and subversive. Cyber security 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.

Aims of the book

The promotion of cyber security as a holistic form of security invites examinations of its political and organisational logics. The principal aim of this book is to interrogate the politics of cyber security in a deeper register than is ordinarily found in security studies. Specifically, my central intention is to open up the multiple temporalities of cyber security to intellectual and political scrutiny so that we can explore and understand how cyber security communities produce a 'politics of time'. In developing an analysis of the *chronopolitics* of cyber security, we can begin to see how the temporal perspectives of cyber security communities are fundamentally constitutive of the political behaviours that enable the policies and practices of cyber security. These assumptions about time and the world are often left unremarked, thereby enabling or tacitly allowing problematic forms of political action to go unchallenged. For instance, cyber security self-identifies with a particular periodisation of the world. The concept of the 'information age' is not unique to cyber security, but how does this idea inform cyber security and what political work is it made to perform? What are the political implications of a seduction by the perceived speed and acceleration of the modern world? In what ways do cyber security actors mobilise history in order to justify cyber security policy? How do they imagine the future and what practices do they deploy in attempting to regulate that future?

The answers to these and other questions reveal multiple temporalities at work in cyber security – some intentional, others not – which interact and combine to form a chronopolitical matrix, a 'politics of time' generated by the collective sociotemporal imaginings of cyber security communities and which performs real political work in the world. The task of this book is to describe, analyse and theorise this chronopolitical manifold and to locate it within the broader politics of security. The development of more nuanced conceptual and theoretical frameworks for the analysis of the temporalities of politics can challenge monolithic imaginings of time and temporality, and the promotion of this inherently critical perspective in International Relations (hereafter, IR, as custom dictates) and security studies is a key ambition of this book.

The chronopolitical lens is not the only available through which to view cyber security, and this enquiry respects the importance of space, place, information, matter, energy *and* time in studies of the political. However, in a global political environment that makes serious political claims upon the nature of time and temporality, reflected in cyber security's open seduction by speed and acceleration, for example, it is timely – deliberately and politically timely – that time and temporality are made explicit in this fashion. By doing so, we may better understand not only cyber security but also the nature and character of security and politics in the contemporary world.

Neither security nor time fit readily within inherited disciplinary bounds. 'Security studies' – or 'international security studies', if one prefers – is rightly considered a sub-discipline of IR, or a parallel field of enquiry to IR (Buzan and Hansen 2009: 16–19), but it is also a sub-field of social enquiry in its own right (Croft 2008). The complexity of contemporary security and its constitutive effects across society imply a presumption to analytical interdisciplinarity (Micheal Williams 2012). In historical terms, security studies has always been 'a kind of hybrid, interstitial intellectual space' located 'on the borderlands' between diverse disciplines (Gusterson 1999: 320). What has changed is the diversity of disciplines that now take security as a valid object of enquiry. This includes fields characterised by positivist epistemologies, as well as those with more interpretivist and post-positivist perspectives on international politics.

So too, time. Unlike the study of space, in which academic geography may claim seniority, the study of time has no central disciplinary core but is the object of enquiry across the natural and social sciences, humanities and the arts. All of these fields are productive in their own rights, yet, as is so often the case, much interesting work exists where these disciplines meet and where the cross-fertilisation of ideas is encouraged. In what I believe to be a necessary first step in re-grounding the study of time and security, we will encounter concepts and theories from the science, philosophy and social science of time. Time and security both make strong claims, therefore, for interdisciplinary approaches that experiment with concepts, theories and methods. This book proceeds in this pluralist spirit, albeit one located at the critical end of the intellectual spectrum.

In this book, I attempt to weave together the stories of humans and things, of animate and inanimate objects, of ideas and ideologies, into a narrative whole that enhances our understanding of cyber security and the temporalities of contemporary politics and security. In this sense, narration is the 'syntax of commonsense explanation' (Abbott 2004: 33), although I deploy theoretical insights from a variety of disciplines to expand and clarify the comprehension of particular issues. I pursue a theoretically inflected historical approach in order to develop a 'synoptic judgement' of the phenomena under examination, 'how it came to be, what it means, and what understanding of it best integrates the available evidence' (Schroeder 1997: 68).

The history of security is always 'a history of the changing problematization of what it is to be a political subject and to be politically subject', and the present enquiry adheres closely to this characterisation of security analysis as 'the critical analysis of the discursive conditions of emergence of contemporary security regimes' (Dillon and Reid 2001: 51). This orientation is readily recognisable as post-structuralist, a well-established strand of critique in IR, rooted in the continental philosophical tradition, that challenges the assumptions on which conventional understandings of international politics and security are founded (Campbell 2010). At the same time, the post-structuralist ethos considers how else politics might be imagined. By deconstructing political problems of power and knowledge, of subjectivity and identity, what alternative solutions might be found? These are the 'problems of multiple possible purposes' absent from conventional security thought (Smoke 1993: 330). This critical imperative emerges most strongly towards the end of this book.

There is a long tradition in IR of learning from other disciplines, and this book aims to promote new ways of understanding time and temporality. Much of the theoretical ground covered in this book is currently absent from IR and security studies, and a synthetic theoretical account can help further our studies of time and temporality. Additionally, I make significant use of primary materials of many kinds. They are, in fact, the data points that make the narrative possible and intelligible. The present proliferation of cyber security texts is remarkable and reflects the multifaceted character of cyber security itself. A substantial corpus is developing of government policy, national strategies, diplomatic memoranda, military doctrines, commercial reports, trade journals, media articles, op-eds, multimedia resources, think-tank reports, technical documents, conference proceedings and academic articles and books. All of these express aspects of the worldviews interrogated in this book.

Cyber security has rich historical and conceptual relations with a wide range of practices, disciplines and communities, all of which have generated valuable archival resources. Given the diversity of primary and secondary sources, an historical approach must inevitably concentrate on those texts in which 'something happens' (Latour 2005: 133). These should be 'discourse events', 'documents or statements that are reflective of or have the power to shape the overall public policy debate about cybersecurity' (Lawson 2013a: 169). Their selection allows us to concentrate on the narrative, rather than become diverted by material that might be interesting but offers little to understanding the chronopolitical dynamics of cyber security. One additional selection bias is a function of the linguistic deficiencies of the author: I have only consulted English sources and my analysis is therefore oriented to anglophone cyber security communities, principally in the United Kingdom and the United States.

This book is not an authoritative account of cyber security, nor would one be possible under current conditions. Stephen Budiansky has remarked of the closely related topic of signals intelligence that the 'practice and craft of history is a document-driven business, and the documents are not available' (Budiansky 2010: 770). The practices of bureaucratic secrecy, document suppression and textual redaction severely impede scholars' efforts to reconstruct key periods and processes in the historical development of national security. In the United Kingdom, the Public Records Act (1958) effectively embargoes release of many government documents into the public domain for thirty years. The Freedom of Information Act (2000) has improved accessibility to official records, but the exemptions afforded under the Act to the intelligence services (Section 23) and information 'required for the purposes of safeguarding national security' (Section 24) mean that primary sources about state security from the crucial period of the 1980s onwards are limited. Often, even documents statutorily made available to the public are selectively redacted, like the annual reports of the Intelligence and Security Committee (ISC) (Bochel *et al.* 2015).

Researchers are often left to concentrate on narrowly defined case studies or classes of non-governmental documents (e.g. Dover and Goodman 2011). Alternatively, they may seek official sponsorship to access restricted archives and publish authorised histories (Andrew 2009; Jeffery 2010; Goodman 2014). Retired officials draw upon their personal experiences to illustrate key dynamics in recent military and intelligence history, but they are also bound by legal restraint (Omand

2010; Pepper 2010). Those without this privilege must mould sparse evidence into credible narratives whose veracity can often only be vouchsafed by those who are unable to speak or refuse to do so (Aldrich 2010). Given the classified nature of many cyber security documents that might be of interest to the historically minded researcher, the best available course of action is perhaps to attempt to construct historical narratives, rather than authoritative histories, of the topics we find of interest. We are fortunate, therefore, that cyber security is not restricted to secret military and intelligence operations for the reasons outlined above. This book contends that the claims made by cyber security to this wider milieu of social and political action and experience make it a formidable creature indeed.

Plan of the book

Chapter 1, ‘Cyber security, community, time’, introduces the reader to the principal themes of the book. It begins by relating how cyber security has been addressed in IR and security studies, particularly in critical and constructivist analyses that explore the conceptual and political foundations of cyber security ahead of policy prescriptions and practical recommendations. From this emerges a proposition that cyber security should be understood as an ‘assemblage’ of material and ideational factors, which allows us to develop a basic model of cyber security as an entity in the world. The second theme is ‘community’, and the chapter describes how cyber security communities develop a ‘cyber security imaginary’ that frames and supports their political thoughts and actions. Crucially, this imaginary includes security communities’ conceptions of time and temporality, which shape how security politics is imagined and articulated. The third section of the chapter looks more closely at how time and temporality have been explored in IR and security studies. This discussion makes the central proposition that an exploration of how time and temporality are perceived in practices like cyber security can help us better understand the heterogeneity of social time in studies of contemporary politics and security.

Chapter 2, ‘Towards a politics of time’, develops the theoretical framework of time and temporality that supports the subsequent empirical chapters. Through a model of ‘emergent temporality’, it shows how sociotemporality as a form of social knowledge emerges from the physical universe. This knowledge is not constrained only to the (inter)subjective experiences of human time but extends through reason and technology to incorporate the temporalities of nonhuman others like machines and electromagnetism, both relevant to the study of cyber security.

Sociotemporality is part of the 'social imaginary', an intersubjectively negotiated field of knowledge that incorporates conceptions of time and space (chronotopes) in its narrative interpretation of reality. The different temporal cognitive biases that inform the chronotope are termed 'chronotypes' and co-exist within and across different social imaginaries and inform the narratives through which communities understand their social existence, their role in the world, and through which their political behaviours are shaped. Different conceptions of time give rise to different political behaviours, a process that informs the concept of the politics of time (chronopolitics). It is the task of the remainder of the book to show how chronopolitics manifests in the practices of cyber security, through an examination of various chronotypes discernible within the 'cyber security imaginary'.

Chapter 3, 'Diagnosing the Present', begins the main empirical section of the book by examining how cyber security discourses identify cyber security with a particular reading of the contemporary 'information age'. Cyber security communities frequently cite speed and acceleration as essential characteristics of this periodisation of (post)modernity. These become dominant modes of framing the threats and opportunities catalysed by global information technologies like the internet. While not entirely inaccurate representations of the modern world, the reliance upon narratives of speed and acceleration has its roots in theories of modernity and postmodernity that serve as totalising and exclusive conceptions of the world, particularly in their insistence on the obliterative temporalities of global capitalism and Western temporal hegemony. In their chronopolitical dimensions, these narratives – fostered by political and intellectual elites – perform crucial cognitive and political work that serves to mask the empirical heterogeneity of social time and constrain the possibilities of political resistance. Cyber security is peculiarly prone, it seems, to overemphasis on speed and acceleration, appropriating as it does not only the times of human others but the times of machines, the computing technologies that work at substantial fractions of the speed of light. The cyber security practices enabled by the appropriation of machine temporalities disclose the potential circumvention of customary ethics and normal political process in the names of speed and security. This process also betrays a lack of awareness of the historicisation of cyber security itself, which ignores the contingent nature of contemporary security politics in favour of politicised narratives of speed that feed the persistent subjectivity of policy deceleration relative to an accelerating and increasingly 'technological' present.

Chapter 4, 'Imagining the future', explores how cyber security communities imagine the future. Cyber security imaginaries are dominated by dystopian visions of the future that prioritise the disastrous and the catastrophic. These ‘cyber doom’ scenarios can be understood as a form of apocalyptic thinking, not just as so many make direct reference to end-times scenarios, but also because they disclose an ‘apocalyptic temporality’. Historical events of ‘cyber insecurity’, of which Stuxnet is perhaps the best-known example, are interpreted as ‘signs’ of impending catastrophe, which serve in turn to corroborate pre-determined apocalyptic scripts of imminent catastrophe. Not only are these future events imminent, these narratives stress, but they are also immanent: they are bound to happen due to the inherent insecurity of the information-technological systems of the contemporary world. This chapter links this mode of thought to theories of the ‘technological accident’ immanent in complex sociotechnical systems, suggesting that cyber security in its ‘resilience’ mode is a response to this particular aspect of apocalyptic thought. Apocalypse is, in its primary sense, revelatory and transformative, characteristics that run through cyber security in, respectively, its concerns with identifying the present political ‘failure to secure’ and the desire to rectify these mistakes and usher in ‘cyber secure’ futures.

Chapter 5, ‘Arguing through the past’, examines how political narratives of cyber security use the past as a resource, most obviously through historical analogies. Previous work on historical analogies and cyber security has tended to concentrate on the failures of analogies rather than on what political work these forms of reasoning perform. This chapter discusses how historical events are used to provoke political action in the present by analogising the nature of future catastrophes identified in concepts like ‘electronic Pearl Harbor’ and ‘digital 9/11’. These narratives tap into existing constructions of national memory and identity in order to evoke emotional identification with the aims of cyber security and to assist in eliciting political support for its furtherance. The past is a fluid resource readily remade in the image of the contemporary politics of cyber security, consonant with a general understanding that the past is not a frozen entity but exists only in its continual reinterpretation and representation in the present. Cyber security actors’ appeals to history are also a search for foundations: in the absence of a Hiroshima, for example, cyber security looks to signature events like Pearl Harbor and the Cold War to ground itself in established historical narratives of national security. History serves not only as a resource through which to analogise a future that may never happen but helps shape the identities of cyber security communities themselves.

Chapter 6, ‘Inhabiting the future’, draws attention to how cyber security communities attempt to ‘inhabit’ the future through exercises,

https://doi.org/10.1017/CBO9781316271636.001

simulations, recruitment and education. Inhabitation is meant both in the metaphorical sense of occupying future scenarios as active participants and as a way to literally populate the future with young people and cyber security professionals. These forms of anticipatory security practice prepare us for cyber security catastrophes and crises through training and simulation and are a way of knowing the future in order to mitigate surprise and uncertainty. These practices rely upon the creation of an aesthetic of anticipation which translates the abstractions of information security into physical and sensory modalities through which the 'virtual' can be made more intelligible. These efforts extend from the closed spaces of national security into the mediated public domain and even into the early stages of education and disclose intentions to raise awareness of cyber security issues and to recruit ever-younger people into cyber security communities. In chronopolitical terms, these practices of inhabiting the future not only attempt to bring the future into the present by making it comprehensible and somehow manageable but also project the present into the future through the literal population of the future with the 'next generation' of cyber security professionals and others aligned with national cyber security efforts. By channelling these individuals' energies in the present, we exert some minimal influence over the future, albeit one that reflects our own imagination and desire, rather than those of future generations themselves.

Chapter 7, 'Cyber security and the politics of time', extracts from the previous chapters four principal chronopolitical logics at work in cyber security. Understood not as universal principles but as tendencies that emerge from historical practices and assemblages, these logics are, respectively, the logics of assemblage, real time, event and *eschaton*. The logic of assemblage stresses the dual nature of sociomaterial assemblages in the mutual contingency of change and continuity, which implies that the cyber security assemblage must always find ways to extend itself in space and time in order to maintain its identity. The logic of real time appropriates but is also seduced by the temporalities of information technologies; it internalises and reproduces speed and acceleration to the potential exclusion of human politics. The logic of event propels processes of premediation and the development of an aesthetic that works to develop an affective regime of political utility in security politics. Apocalyptic anxiety is one example of this and is further located within the logic of *eschaton*, which discusses how political theology illuminates aspects of the chronopolitics of cyber security, in its concerns with the end of history and the ends of security itself. These logics are shown to constitute a provisional chronopolitical manifold of cyber security, in which they complement and contest one another. The chapter ends with a call to challenge dominant political conceptions of time and temporality as a way to approach the future and avoid foreclosing political possibilities. The concluding chapter summarises the contributions of the book to the academy and outlines possible avenues for further development and enquiry.

1 Cyber security, community, time

Security has attained an unprecedented constitutive role and visibility in contemporary life. In the immediate aftermath of World War II, 'security' in political discourse was effectively identical with 'national security' and reducible to the concerns of securing the sovereign state within an anarchic world order (Romm 1993: 1–8). Over the intervening decades, and since the end of the Cold War in particular, conceptions of security have been consciously 'widened' and 'deepened' commensurate with a range of worldviews and theoretical orientations (Buzan 1983; Smith 1999; Buzan and Hansen 2009). The widening move has involved the application of security logics beyond military conflicts and national security to a plurality of securities: human, energy, food, environment and water, to name but a few. The deepening move has shifted emphasis from the state 'down' to the level of the individual, and 'up' to the international and the global. In this double move, security has been subject to political and intellectual redefinition and redeployment as ways of understanding and transacting with the world. The logic and language of security are now inextricable from social life. Concurrently, the way we imagine security is informed by a growing sense that this period of human history is increasingly insecure. As the Chairman of the US Joint Chiefs, General Martin Dempsey, testified before Congress in 2013, the world 'is more dangerous than it has ever been' (Zenko 2013). This is not an insignificant claim, given the speaker's pivotal role in mobilising resources to meet this apparently existential challenge.

In the contemporary Western experience, the promise of security pervades the marketplace and consumers are sold 'security' panaceas to a range of quotidian problems that would not have borne that moniker only a few years ago. From domestic child safety to pensions in retirement, this marketisation of security is a process through which the security industry transforms social perceptions of insecurity into the consumption of security commodities (Neocleous 2008: 154; Krahmann 2008). The logic of security extends to architecture, with security 'designed into' everything from airports and sports stadia to nightclubs and shopping centres

(Coaffee *et al.* 2009; Coaffee 2010). No major public event can be undertaken without planners demonstrating their commitment to both visible and invisible security measures (Boyle and Haggerty 2009, 2012), for which costs escalate as much in line with clients' fears and consultants' imaginations as they do with the existence of any credible threat. Urbanists Mona Fawaz and Hiba Bou Akar write that security in the city has been normalised, 'stripped of its political significance': threats are accepted without critical interrogation and security is supplied as a public good in ignorance or denial of its particular historical, geographical or social derivation (Fawaz and Bou Akar 2012: 105). Details of this genealogical contingency are often obscured or left deliberately vague, and through this lack of clarity security can reproduce itself in multiple forms and with increasing vigour (Walker 1997: 63). If security is a signifier, it can sometimes seem as if it has cast off its semiotic moorings and taken on a free-floating life of its own.

The study of security is complicated by, but not always mindful of, a fundamental distinction between the different meanings of the word 'security' itself. These combine and cross-pollinate so that 'security' in the world is always a manifold rather than a discrete entity or idea. Security is both a condition to be attained and a process by which to achieve that condition. As Nils Bubandt states, security 'deals with the problem of order and disorder, being both the ontological condition of order, in the sense of an absence of doubt, danger, risk and anxiety, and the political means of ensuring that order' (Bubandt 2005: 278). Security is therefore not solely a condition to be achieved but has a performative function, in that it serves to order the social world rather than being an accurate description of any external or objective reality. In this constitutive sense, the pervasiveness of security transforms social relations into 'security relations' (Huysmans 1996). For some scholars, the infiltration of security logic and practice into contemporary life is so advanced that, as Michael Dillon asserts, security is not only a pillar of modern politics and society but a key signifier of modernity itself (Dillon 1996). The intensification of the imprint of security upon society has become even more apparent in the aftermath of the terrorist attacks upon the United States in September 2001. In noting the deleterious effects of post-9/11 counter-terrorism policy on the same publics it professes to protect, philosopher Langdon Winner writes that the present 'obsession with security now casts a chill upon public life and the only question is "How cold will it get?"' (Winner 2004: 162).

In the last two decades, the logic of security has found a novel mode of expression whose material ubiquity and conceptual totalitarianism make singular claims upon the nature of the modern world and challenge the extent of any previous regime of security. ‘Cyber security’ is the first attempt to foster a holistic approach to the security issues raised by information technologies, in particular the digital, electronic and networked information technologies of the internet and the related sociotechnical phenomena of the ‘information age’. Cyber security is predicated upon narratives referencing the characteristics of this historical period in the embrace of which we are commonly supposed to be. These narratives stress the speed and acceleration of the contemporary world, in which information technologies allow for instantaneous global communications, collapse traditional fixities of time and space, and catalyse risks and threats that may materialise anywhere and everywhere at any moment. This sociotechnical environment – often, if somewhat anachronistically, termed ‘cyberspace’ – is constructed as ‘ungovernable, unknowable, a cause of vulnerability, inevitably threatening, and a home to threatening actors’ (Barnard-Wills and Ashenden 2012). This environment of dynamic and metastasising threat is often presented as a space apart from normal and healthy social existence, an exceptional environment over which governance must be extended. Cyber security becomes the security of ‘cyberspace’ in its broadest sense.

This chapter explores some of the ways in which cyber security has been analysed and interpreted by scholars in International Relations (IR) and security studies. It pays particular attention to critical and constructivist studies that problematise cyber security in order to interrogate its ontological and epistemological foundations. This is contrasted with mainstream work on cyber security that is oriented towards policy and the solving of specific problems of cyber security, rather than treating cyber security as a problem in and of itself. This chapter also introduces various ways in which cyber security can be viewed: as a global ‘macrosecuritisation’, as an exercise in security convergence, and as a process, rather than a discrete entity. This last point is expanded through the proposition that cyber security should be understood in both practical and theoretical senses as an ‘assemblage’ of both knowledge and things. This conceptual framework allows us to incorporate all dimensions of cyber security – social, ideational, political, material – in a basic model of what cyber security is or might be. The issue of how knowledge is assembled is addressed in the second section, which discusses the roles of cyber security communities in developing ‘security imaginaries’ that inform and sustain political thought and action. Foreshadowing the detailed discussion of time and temporality in Chapter 2, these imaginaries include assumptions and ideas about time, which contribute to how politics is imagined and visions of social order are articulated. The final section of this chapter explores how time and temporality have been approached in disciplinary IR and makes the case for a renewed emphasis on the heterogeneity of sociotechnical time in studies of contemporary politics and security.

Interrogating cyber security

Cyber security is often elastic in definition and elusive in practice. Given its concerns with almost anything that communicates digitally and electronically, whether these be people, companies, governments, militaries, intelligence agencies, machines or algorithms, cyber security affects the world in many ways not captured by its more formal definitions. Government definitions of their own cyber security activities, for example, tend to overlook the offensive use of information technologies – currently fuelling substantial growth in the defence industrial base and demanding reorientations in military force posture, structure and rules of engagement (e.g. US Joint Chiefs of Staff 2013). Similarly, accusations of adversarial 'cyber espionage' are often blind to friendly states' uses of identical tactics in pursuit of economic and national security ends (Greenwald 2013). Both 'cyber war' and 'cyber espionage' are facets of cyber security, if not always presented in such stark and obvious terms. Critics of this position might argue that this is painting cyber security with too broad a brush: cyber security is only about defending or protecting information and the critical infrastructures that depend upon it. One classical definition, for instance, holds that cyber security is 'the defense or protection of the integrity, operations and confidentiality of computers and computer networks' (Lewis 2005: 821). However, this is a naïve misreading that is as outdated as it is incomplete because of its myopic divergence from the statements of governments and international bodies, which disclose that cyber security is a much broader suite of policies, perspectives, practices and processes than many analyses record (see also, Dunn 2007: 85).

Cyber security, as defined by two leading scholars in the field, is 'the absence of a threat either via or to information and communication technologies and networks ... cybersecurity is the security one enjoys in and from cyberspace' (Dunn Cavelty and Suter 2012: 19). Cyber security is no longer, therefore, just about the 'security of cyberspace', but is also 'security through cyberspace'. From this perspective, information technologies are the material substrate that allows for and encourages the convergence of all other forms of security (Yould 2003: 78). Cyber security is, therefore, not restricted to the security of information and information technologies but is the means through which other forms of security may be pursued, as well as being a condition of that greater security.

Studies of cyber security are commonly oriented towards policy concerns rather than the construction or exploration of theory (Eriksson and Giacomello 2007: 2). This is not to assert that existing work on cyber security is not informed by theoretical considerations but that the majority of research emphasises policy and technical implementation at the expense of theoretical application and development. This situation has been noted even by scholars working within mainstream security and strategic studies (e.g. Liff 2012). That this condition pertains is undoubtedly in part a function of the relative novelty of cyber security as an identifiable field of practice and policy. The earliest textual reference to cyber security probably dates to 1989 (Furber 1989: 298) but its roots lie in well-established and cognate forms of security such as critical infrastructure protection and information security. It is only in the last few years that computer science professionals, however, have felt it possible – or, importantly, necessary – to self-identify as practitioners of cyber security (Denning and Frailey 2011). In common with the technical work emanating from computer science, most non-technical studies of cyber security attempt to be 'problem-solving' rather than 'critical', originating as they do from within the policy analysis community (Lindsay 2013: 367). This corpus accepts and attempts to perpetuate the status quo by solving problems within the existing social order, rather than interrogating the assumptions that this problem-solving takes as its parameters and conceptual bounds (Cox 1981).

This perspective dominates security studies in general, a managerial approach always informed by 'the desire to "do" security better' (Neocleous 2008: 4). Didier Bigo has observed that despite the intradisciplinary disagreements between security scholars of diverse epistemological and methodological persuasions, it is not always apparent that they are so different when, in their mutual and exclusive discourses, 'the maximization of security becomes the horizon of discussion' (Bigo 2001: 95). In so doing, scholars seduced by proximity to power and the perception of political influence find themselves treated as one of a range of 'more or less useful bureaucratic resources' (Booth 1997: 97). Michael Dillon concludes of the security studies literature in general that it 'invokes security as a ground and seeks largely to specify what security is; how security might be attained; and which are the most basic, effective, or cost-effective means of doing so' (Dillon 1996: 18). Ultimately, as James Der Derian argues, it should be the aim of security researchers to 'get inside the operational box [of security] while staying outside the semiotic box of security discourse' (Der Derian and Finkelstein 2008: 86). This is impossible – one does not choose who reads one's publications, for example – but there is no reason why a work *on* security has to set out to contribute to the work *of* security, particularly that of the state.

This book therefore finds affinity with critical work on security that problematises security itself rather than leaving its ontological and epistemological foundations unexamined (Browning and Macdonald 2013; Hynek and Chandler 2013). Scholars in the constructivist vein are responsible for the most developed body of small-'c' critical analyses (Brown 1994) of cyber security. Constructivism, states one of its earliest proponents in IR, 'complements the Enlightenment belief in the power of language to instantiate reason and qualifies the belief in the power of language to represent the world as it is' (Onuf 1994: 4). In this broadly Kantian tradition, constructivism holds that 'the manner in which the material world shapes and is shaped by human action and interaction depends on dynamic and epistemic interpretations of the material world' (Adler 1997: 322). That is, knowledge of the world is socially constructed through collective and intersubjective understandings that manifest as ideas, identities, norms, rights and culture, which, in turn, shape how states interact and politics is enacted. Constructivism in IR, therefore, is concerned both with the 'social construction of knowledge' (epistemology) and the 'construction of social reality' (ontology) (Guzzini 2000). This post-Kantian distinction between human and world might be unsuitable for philosophers attempting to construct a categorical metaphysics (Harman 2010a: 773), but it has proven valuable and influential in IR theory and in security studies (Hopf 1998; Farrell 2002; Adler 2012).

In common with studies of other forms of security, constructivist analyses of cyber security have drawn upon securitisation theory and related approaches that privilege the constitutive role of language to show how cyber threats are constructed through cyber security discourses.[1] Securitisation theory emphasises the sociolinguistic construction of security and is constructivist in its emphasis on recognising how threats are collectively identified, understood and responded to: security cannot be defined objectively but must be considered a sociolinguistic construction. Actors label an issue as a 'security issue', which thereby enables them to claim the necessity and right to 'treat it by extraordinary means' (Buzan *et al.* 1998: 26). It is not therefore important to establish objectively whether a particular object is actually threatened and thereby deserving of being 'secured' – securitisation theory denies this is possible – but to understand how something is comprehended collectively as a

[1] Bendrath (2001, 2003), Eriksson (2001), Bendrath *et al.* (2007), Eriksson and Giacomello (2007), Hansen and Nissenbaum (2009), Lawson (2012a, 2013a, 2013b), Dunn Cavelty (2013).

security threat. Securitisation is a 'speech act' in which the utterance itself is the act: 'By saying the words, something is done' (Buzan *et al.* 1998). Securitisation theory proposes that no threat has an external objective reality but is constructed intersubjectively and should be understood solely in these terms.

Scholars have applied securitisation theory to cyber security and its related and constituent security practices. Helen Nissenbaum (2005) suggests, for example, that cyber security and 'technical computer security' are separate issues with differing processes of securitisation operating in each field. Whereas the latter is more concerned with securing networks through technical means, the former is intent on portraying cyberspace 'as a staging ground for aggressive attack on the nation' and therefore requiring just the sorts of exceptional measures predicted by securitisation theory. Cyber security can therefore be viewed as 'computer security' plus 'securitisation' (Hansen and Nissenbaum 2009: 1060). Given a liberal, democratic impulse to value free and open information and communication, cyber security may improve the security of cyberspace but 'at the expense of its core purpose as a realm of public exchange' (Nissenbaum 2005: 73). Given this pernicious effect, technical computer security should be preferred as a means to deliver network security and preserve core societal values.

By integrating securitisation theory with agenda-setting and framing theories, Johan Eriksson (2001) introduced the notion of 'threat politics' to the study of cyber security. An examination of threat politics entails understanding how and why some threat images but not others take on 'societal salience', in which securitisation is but one of many frames available to those seeking to present issues as security threats. Eriksson demonstrated how information technology became a security issue in Sweden after the end of the Cold War. This was assisted by the use of threat images that included the cultural uncertainty and fear engendered by the rapid uptake of information technologies, increased military concerns over information warfare and fearful anticipation of the 'Y2K bug', amongst others. This was a multiply framed process of securing information and communication technologies (ICTs) and their use that met with little domestic resistance during this period.

Studies of US cyber security and threat politics have shown how the frames used over the last two decades have oscillated between cyberterrorism and cyberwar, and between existential and non-lethal threats (Bendrath 2003; Bendrath *et al.* 2007). They have also related in some detail how threat frames were constructed and deployed and what the political and material effects of these have been, not least the elevation of cyber security to the top of the US political agenda, even as securitisation has not necessarily been wholly successful. Myriam Dunn Cavelty's book, *Cyber-Security and Threat Politics* (Dunn Cavelty 2008), has been particularly influential and instructive in showing how the framing of cyber threats in the US has changed since the 1980s, from concerns over technical information security and encryption to more expansive attempts to secure critical infrastructures within a 'homeland security' framework. Similarly, scholars have recounted how securitisation in the wake of the first so-called 'cyberwar' in Estonia in 2007 benefited that country in material terms – principally, the founding of the NATO Cooperative Cyber Defense Center of Excellence in Tallinn – and helped multilateral actors like NATO to promote cyber security through their own policy agendas (Hansen and Nissenbaum 2009).

Scholars inspired by securitisation theory and constructivist approaches have redressed to some degree the ahistorical nature of prevailing cyber security discourse. In attending to the historical construction of, in particular, 'cyber threats', they have convincingly shown how political and economic interest groups have sought to achieve strategic ends through discursive means often at odds with the available evidence. This is particularly true of cyberterrorism, where discourse and policy are predicated on speculative futures for which there are simply no precedents outside the imagination of security communities (Conway 2008, 2011).

In its global dimensions, we might also propose that cyber security is a new 'macrosecuritisation' to rival those of the Cold War and the Global War on Terror (Buzan and Wæver 2009). Securitisation attempts to explain and understand the actions of middle-level entities like states and regional security groupings, but macrosecuritisation is concerned with the global systemic level of security, particularly in its subordination of middle-level processes to the higher level of the system. Buzan and Wæver do not attempt to apply this to cyber security but we can suggest that ongoing attempts to foster global norms for tackling cyber threats and preventing cyber war, international frameworks for combating cyber crime and calls for a global culture of cyber security may be expressive of this higher-level security logic. These are not just quests for global alliances but ways of 'structuring the relations of international security in much more sophisticated, large-scale and complex ways than suggested by a mere logic of individual unit survival' (Buzan and Wæver 2009: 275). The framing of cyber threats as existential and transnational – networked and cascading lethality in a globalised world – begins to make the calls for global cyber security look like appeals for macrosecuritisation. This is not to suggest that previous (Cold War) or existing (Global War on Terror) macrosecuritisations are either always successful or go unchallenged but that these processes attempt to link up existing middle-level (usually national) security frameworks and shift attention to higher-level security referents like global society and the global financial system.

Securitisation proposes that security is a dynamic process, in which there is no stable security condition to which the efforts of security actors can be directed. This perspective resonates strongly with statements coming from security communities themselves. One leading security researcher and author, Bruce Schneier, has become closely associated with the formulation, ‘security is a process, not a product’ (Schneier 2000, 2004: 84). This has attained mantra-like status in the information security community, operating, one assumes, in near-total ignorance of security academics and IR scholars. One community seeks to solve the problems of security while the other seeks to problematise security, but in this respect both speak in a language the other would understand. Information security professionals would also recognise the cultural dimensions of this argument, in which ‘culture’ – of the workplace, of information technology use – is understood as constantly changing, and of which ‘security’ is reflective and representative (Schlienger and Teufel 2002).

At the heart of cyber security discourses is a simple narrative glossing vast empirical complexity. This narrative might read as follows. Contemporary global society is dependent on vast arrays of computerised information technologies including, quintessentially but far from exclusively, the internet. These information technologies are inherently ‘insecure by design’ and new threats to individual, economic, national and international security have emerged as a result. These insecurities are as complex and interconnected as information technologies themselves and pose fundamental challenges to traditional political concepts, particularly those of national sovereignty and national power. New forms of security are therefore required to counteract these threats and cyber security is proposed as a rubric beneath which various distinct but inter-related activities are grouped. This brackets a wide spectrum of processes and practices with differing specific aims and potential outcomes but which all converge upon the global information-technological substrate as a means through which to achieve ‘cyber security’, that is, the freedom from ‘cyber insecurity’ and the freedom to pursue ‘cyber security’.

Given the undoubted importance of information technologies to all sectors of public and private life, it would be unsurprising were most forms of state and commercial security not to become ever more dependent upon them. This presents a situation in which cyber security becomes a form of security to facilitate other forms of security, be these national, economic, personal or global. More properly perhaps, cyber security converges with other forms of security. The concept of 'security convergence' has a pedigree of rather vague usage in security studies to connote the coming together of states' strategic security interests so that they pursue security policy in common, but captures little that is not otherwise explicable through well-established, and in IR theoretically contested, terms like 'cooperation'. It has a rather more specific use in corporate management, where it has referred to the consideration of physical security and logical (information) security as mutually interdependent endeavours. This has evolved and expanded to include the formal cooperation of all security functions of organisations, so that terms like 'holistic security management' may be considered synonyms (Zuccato 2007).

This invocation of the convergence and mutual interdependence of social, material, informational and ideational factors suggests that something might be missing from constructivist accounts of cyber security, which security practitioners would probably recognise all too well in their daily routines. Cyber security is not only a set of rules or policies but is also instantiated through hardware: the material infrastructures of the global information grid. Cyber security has a material reality, to which we have partial access through human senses and reason. Post-positivist approaches would generally assert that it is consensus about this reality that shapes social phenomena rather than any decisive causality on the part of material reality itself. In this sense, intersubjective epistemology takes on ontological importance in social reality whilst denying the ontology of material reality itself. This is unsatisfactory, particularly when attempting to analyse the politics and security of sociotechnical environments like the internet, in which a variety of ideational and material factors play key roles in the politics of cyber security. In short, a conceptual framework is required that allows both to be taken into account.

For instance, we can go further than suggest that security processes and practices are converging on information technologies and propose a more general 'informationalisation' of security, an 'ugly but useful' neologism (Floridi 2011: 43). As those engaged in commercial security convergence will attest, the principal factor informing convergence is the centrality of information to the life of firms themselves. Convergence security regimes seek to regulate the flow of information across organisations' networks, granting or denying access to information sources, and maintaining information as the critical asset of a given organisation. In broader terms, various frameworks have been proposed to describe the emergence of post-industrial organisational forms for which 'information' and 'information technologies' are determinant of significant changes in the production, distribution and consumption of knowledge, culture and material goods, not least of which is the concept of an 'information society' (Webster 2006). However, though the roles of information technologies are important in catalysing social, economic and political change, there is a more fundamental reorientation at work. As Jos de Mul determines, the concept of 'information' itself has moved to the centre of the contemporary worldview, which has important implications for our perception and interpretation of reality (de Mul 1999). Spurred by the increased mediation of the human experience by computers, the 'omnipresence of information technology seduces us into thinking that everything can be regarded in terms of information and that in the final analysis the world is built up of information' (de Mul 1999: 72).

Scholars of various persuasions have pursued this line of thought further, in precisely the non-metaphorical terms de Mul is keen to deflate and deflect. Two examples are provided here. In the first, RAND Corporation defence academics John Arquilla and David Ronfeldt are notable in developing the proposition that information 'may be a physical property – as physical as mass and energy, and inherent in all matter' (Arquilla and Ronfeldt 1997: 145). They do not develop this thesis in detail but they do examine its import for conceptualising and operationalising conflict as a subset of security. If information is physical, they suggest, it becomes something akin to matter and energy, which can be 'hurled' against the enemy: success in conflict comes from 'targeting whatever represents or embodies the most information on an enemy's side' (Arquilla and Ronfeldt 1997: 158). As all physical systems embody information, these targets are not restricted to intangible code or ideas alone. They also include weapons systems, physical resources and 'the most information-rich components of an adversary's order of battle', whatever those may be (Arquilla and Ronfeldt 1997: 158–9). Viewed from this perspective, although 'cyber' conflict is often dependent upon computer networks for its enactment and propagation, its potential targets are much more varied. In a complementary move, as information becomes quasi-material, power, 'long thought to be based mainly on material resources, is increasingly seen to be fundamentally immaterial, even metaphysical in nature' (Arquilla and Ronfeldt 1997: 142). At the heart of their proposed military revolution is an understanding that 'information is a bigger, deeper concept than traditionally presumed, and should be treated as a basic, underlying and overarching dynamic of all theory and practice about warfare in the information age' (Arquilla and Ronfeldt 1997: 154).

From an entirely different – and antagonistic – field of intellectual activity, Michael Dillon and his collaborators often cite Arquilla and

Ronfeldt in critical fashion but in their work we find corresponding statements like, ‘Information is the new metaphysic of power’, informed by the line of military thinking previously described (Dillon and Reid 2001: 59; Dillon 2002: 73). Broadening their thesis, and drawing substantially on Foucauldian biopolitics and non-linear science, they connect digital code with biological code beneath an informational umbrella that becomes the ways and means of power itself. When power becomes informational, ‘[t]his does not simply mean that it operates through digitised and integrated computer-mediated communication and surveillance technologies. Information is now regarded as the principle of formation of life instead’ (Dillon and Reid 2001: 49; Dillon and Lobo-Guerrero 2009). Michael Dillon asserts that ‘information as code’ is a ‘new organising principle for ordering social, economic, epistemic, political and military relations of power’ (Dillon 2004: 83). As code, ‘information is no mere asset. It is *the* constituent element of all matter—conflating the organic and the inorganic’ (Dillon 2004, original emphasis). The informationalisation of life and its manifestation in manipulable code provide new modes and targets of political intervention, particularly with respect to war and security (Dillon 2003a, 2003b; Dillon and Reid 2009; Reid 2009).

We might argue similarly about the materiality of information networks previously mentioned. The internet is not some ethereal thing but a network of material components, even if its users cannot always directly observe them. Luciano Floridi argues that the internet is ‘an epiphenomenon that cannot be physically perceived, or meaningfully located in space and time, over and above the set of interacting networks that constitute it’ (Floridi 1995: 263). These material components are as integral to understanding the internet as the information that flows through these networks and the knowledge and services that are thereby enabled (Dunn 2007: 86). The material foundations of the internet ‘present a formidable set of real constraints on the realm of the possible’, examinations of which reveal ‘methods of control and authority, many of which are buried within the subterranean layers of the network’ (Deibert 2003: 530). Similarly, infrastructure plays ‘an agential role, both constraining and enabling particular configurations’ of social and cultural practice (Aradau 2010: 492–3; also Dunn Cavelty and Kristensen 2008: 11).

The precise ontological status of information and matter is not what is at stake here. Rather, these examples demonstrate why extant critical accounts of cyber security are insufficient on their own. They tend to prioritise discourse over things, epistemology over ontology, without providing a deeper understanding of the conditions that enable the emergence of discourses in the first place. In fairness, there is no reason why all these accounts must do so: it would be unnecessarily tedious if they did. My assertion here is that there is room in the literature for preliminary attempts at re-grounding cyber security on firmer ontological foundations.

One methodological tool that may be of use in better conceptualising the environment in which we are interested is the concept of 'assemblage'. Cyber security is a sociotechnical 'assemblage', understood in its dictionary sense as a collection of related people or things but also in its academic theoretical sense as a web of actors and artefacts and their contingent and dynamic relations. As an analytical tool, 'assemblage' has been used in social theory, sociology, urban studies, human geography and other fields to conceptualise the heterogeneity of social phenomena and to trace the relations between their social and technical components (McFarlane and Anderson 2011). It also provides an opportunity to link the 'high' politics of the (inter)national with the more mundane aspects of life with which these are intertwined, if not always obviously (Collier and Ong 2005; Enloe 2011).

Cyber security *qua* assemblage is not just an object, however, a unitary and unified body possessing its own agency, capable of its own expressions and decisions without reference to any other. It is rather an aggregate of many parts and their inter-relations: the information infrastructures and their users and dependencies that are the ostensible referents of cyber security, and the political, ethical, legal, normative and ideational factors that sustain cyber security at all levels from the local to the global. No assemblage is either whole and imperturbable nor entirely reducible to its parts but is simultaneously an accumulation of smaller assemblages and a member of larger ones. This holds if we talk of a personal computer or the international community, or of entities at any scale from the sub-atomic to the cosmic. An actor may also be part of more than one assemblage simultaneously, performing several functions at once, and can be temporarily removed from one and 'plugged' into another without losing its identity (DeLanda 2006: 10). Ephemeral though they often are, assemblages retain their identity when translated across space and time if they are able to 'enrol' and 'enlist' actors—human and nonhuman—into their networks in order to reproduce and extend themselves (Latour 2005).[2]

[2] In actor-network theories, nonhumans are often termed 'actants', rather than 'actors', and have agency in the sense that they modify the actions of others but without necessarily 'intending' to do so (Latour 2005: 71–2).

We might dispute whether, for instance, an entity called ‘society’ exists but we can identify and name other relatively stable assemblages as units of analysis and describe their composition, function and interactions with others. Their precise definition and theorisation remain contested but we speak of human groups and institutions in terms that allow us to approach them analytically, even if only as convenient heuristics: family, school, faith group, tribe, government, state, market, the international, and so on. Were this not so, social enquiry would be a truly Sisyphean labour, in which, as Albert Camus wrote of the mythical king’s eternal travails, ‘the whole being is exerted toward accomplishing nothing’ (Camus 1991: 120). In this way, the cyber security assemblage of material and immaterial entities is not static but a web of social and material actors that requires constant negotiation and performance. Any analysis that attempts to characterise a postulated entity like ‘cyber security’ as a singular artefact or unitary actor is doomed to misrepresent empirical reality unless it recognises its internal heterogeneity and the mechanisms and processes that enable its continued assembled existence.

In this state of permanent change and renegotiation, assemblages must have cause both to become and to stabilise and in order to maintain their identities must have commonalities through which cohesion is mediated and coherence achieved. This is reflected in Bruno Latour’s assertion that there are ‘no groups, only group formation’: groups ‘are not silent things, but rather the provisional product of a constant uproar made by the millions of contradictory voices about what is a group and who pertains to what’ (Latour 2005: 31). These voices include those who study these groups, for whom the characterisation of assemblages as X or Y allows for analysis but which obscures the inherently ‘fuzzy’ boundaries of assemblages so circumscribed. The taming and constraining of this multivocality enables something like cyber security to cohere as an assemblage, mediated through communities of knowledge and practice that enable and instantiate the processes of cyber security. This book is about those communities and the ways in which they imagine the world. In particular, it addresses how cyber security communities think about time, how these temporal perceptions influence their politics and practices, and what effects these have on policy and people. I will now turn to the issue of community and imagination, before addressing how time and temporality have been approached in IR and security studies.

Community and imagination

One of the key findings of existing studies of cyber security has been the importance of ‘epistemic communities’ in the political processes of constructing and framing cyber threats. The concept of epistemic community is grounded in Michel Foucault's formulation of *episteme* (Foucault 2002), which was introduced into IR by John Ruggie in the 1970s (Ruggie 1975; also, Haas 1989, 1992; Adler and Haas 1992). Ruggie describes *episteme* as 'a dominant way of looking at social reality, a set of shared symbols and references, mutual expectations and a mutual predictability of intention' (Ruggie 1975: 569–70). Foucault was keen to identify a form of social knowledge specific to a particular epoch but that has been translated in IR as 'a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area' (Haas 1992: 3). An epistemic community consists of 'interrelated roles which grow up around an episteme; they delimit, for their members, the proper construction of social reality' (Ruggie 1975: 570).

The concept of epistemic community has ordinarily been applied to scientific communities, so that in cyber security we might identify a community of computer scientists or of computer security professionals being brought into the policy arena to advise on technical issues. However, there is a strong case that 'non-scientific knowledge' is as important in influencing policy as scientific knowledge, perhaps even more so (Davis Cross 2013: 148), and we can therefore locate other policy-relevant epistemic communities – political, military, intelligence, media – within the national context (e.g. May *et al.* 2014) and other collectivities organised and acting transnationally. Of particular importance in cyber security is the role of the private sector – the cyber security industry – in co-constructing cyber security through marketing, lobbying, and other forms of political engagement (Harknett and Stever 2009; Deibert and Rohozinski 2011; Aaron 2012).

Myriam Dunn Cavelty (2007) notes the important role of collective expert knowledge in shaping political outcomes in cyber security and draws attention to the various types of epistemic communities described above. Extending the work of Andreas Antoniades (2003), she describes the existence of two types of epistemic community and two levels on which they operate. *Ad hoc coalitions* emerge to address specific policy problems, whereas *constant groupings* intend 'the establishment and perpetuation of beliefs and visions as dominant social discourses' (Dunn Cavelty 2007: 128). Epistemic communities can intervene on a practical level, setting agendas and influencing policy processes, or on a cognitive level, seeking 'to impose particular discourses and worldviews on societies' (Dunn Cavelty 2007: 128). This book is concerned with constant groupings operating on the cognitive level, as they are relatively longer lasting and have more persistent effects in shaping social reality. As Dunn Cavelty states, these epistemic communities contest one another to reproduce their particular visions of social order. It follows that multiple epistemic communities can co-exist, as we find in cyber security, with communities drawn from the full spectrum of the private, public and civil sectors.

These epistemic communities are in turn comprised of 'communities of practice', which Emanuel Adler describes as temporary stabilisations of meaning and discourse within physical networks of people and things (Adler 2008: 199). In this sense, we may retrospectively conceive of these levels of intersubjective knowledge and practice as assemblages, always in the negotiated process of 'becoming', always seeking out new forms of allegiance with others and always competing for limited resources within the political economy of security that allow them to sustain and reproduce themselves. They are assisted in this existential effort by specific knowledge that informs who they are and what they do and that provides them with their sense of identity and purpose. This knowledge is what imparts meaning to the social and material resources marshalled by these communities in their attempts at self-reproduction. Practices are therefore not just actions in the world but 'socially meaningful patterns of action' that structure politics and security (Adler and Pouliot 2011). Importantly, communities of security practice and knowledge need not correspond to established institutional boundaries. Understood as assemblages, they may arise and dissipate within the global system, combining an array of social and material entities and factors that do not necessarily map to the scale or boundaries of pre-existing institutional configurations (Ong 2005: 338). This is an observation also made of 'global security assemblages', in which 'actors, technologies, norms and discourses' are 'embedded in a complex transnational architecture that defies the conventional distinctions of public-private and global-local' (Abrahamsen and Williams 2011: 217).

The social episteme connotes the configuration of semiotic and structural elements constitutive of society that allow for the self-imagining of community and society (Ruggie 1993: 157). We might alternatively describe the social episteme as a set of beliefs held by a given community and by which it navigates its interactions with the world. Beliefs manifest in the ways in which communities imagine themselves. The notion of self-imagination as an essential component of communal identity politics is well established in international studies (e.g. Anderson 2006). This book retains this sense but also extends Ruggie's 'mutual predictability of intention' (Ruggie 1975: 570) into the related concept of the 'security imaginary' (Pretorius 2008; Lawson 2011).

The self-imagining of identity is predominantly an internalised self-constitution with respect to variously defined ‘others’, but the security imaginary is the means through which the intentions of the assembled epistemic community may be internally negotiated and, ultimately, externalised. A social imaginary, according to Charles Taylor, is how people ‘imagine their social existence, how they fit together with others, how things go on between them and their fellows, the expectations that are normally met, and the deeper normative notions and images that underlie these expectations . . . that common understanding that makes possible common practices and a widely shared sense of legitimacy’ (Taylor 2004: 23; also, Appadurai 1996: 31). For Joelien Pretorius, a *security* imaginary is not only an extension of the social imaginary to the study of security but that part of the social imaginary ‘specific to society’s common understanding and expectations about security and [which] makes practices related to security possible’ (Pretorius 2008: 112). These expectations are in part reliant on the ‘mutual predictability of intention’ identified by Ruggie, which keeps a community focused on its aims and objectives and propels the means by which to achieve them.

With this in mind, we may postulate the existence, if only as a useful heuristic, of cyber security imaginaries that speak to the understanding and expectations of cyber security within cyber security communities and within society as a whole. Pretorius demonstrates that this cultural dimension of security plays an important role in spreading practices and norms of security, as may be discerned in current attempts to foster a ‘global culture of cyber security’ (Dunn and Mauer 2006; Portnoy and Goodman 2009). In common with the social episteme – by virtue of being part of it – any security imaginary will incorporate ‘an interwoven set of historically contingent intersubjective mental characteristics’ (Deibert 1997: 33), which includes spatial and temporal cognitive biases. These temporal biases are the empirical focus of this book, and the following section introduces how IR scholars have approached time and temporality.

Time in IR

Time and temporality are under-developed topics in IR. This may be due to a persistent critique that dominant IR theories are ahistorical, that they fail to account for change in time and that they ignore the temporal contingency of political phenomena, both in their historical development and in their constant dynamism and renegotiation (e.g. Rosenberg 1994; Kütting 2001). These theories prioritise the spatial over the temporal and reify the state as a fixed territorial entity that has somehow fortuitously come into 'being', rather than as a polity undergoing a perpetual process of 'becoming' (Agnew 1994; Campbell 1998). This alleged blindness to history and its philosophy inevitably shapes how we understand contemporary politics, particularly in assumptions about progress, destiny and the teleology of state- and nationhood (Walker 1989, 1993). Those authors who affirm the role of history as a 'core discipline' of IR acknowledge the distinction between viewing history as a resource for explaining the world and seeing the world as an historical phenomenon in itself (Roberts 2006; Hobson and Lawson 2008; Lawson 2012).

A putative 'historical turn' in IR has prompted recent historical reflection, but it is an incomplete perspective on time, concerned principally with remaking the past in the present, or with the construction of meaning over time. Instead of embracing the 'radical uncertainty of historical meaning', or the problematic meaning of history itself, it also stands accused of imposing its own 'interpretive closure' (Vaughan-Williams 2005: 117) on the historical record in order to suppress ambiguity and prevent explanatory superabundance. Important though the renewed emphasis on history is in IR, other aspects of time and temporality should also be of interest to students of the international, as they are elsewhere in the humanities and social sciences, in which a 'temporal turn' has been identified (Adam 1995: 149–75; Jessop 2009; Hassan 2010).

Media theorist Robert Hassan, for instance, roots this shift in the economic crises of the 1970s, which prompted a 'new spatio-temporally informed perspective with which to comprehend how planet-wide transformation (technological, social, and economic) was occurring' (Hassan 2010: 85). Spearheaded by human geographers, this reorientation of enquiry, in Hassan's analysis, prioritised space over time, an imbalance that has been redressed only since the early 1990s, with renewed attention to the social time of human experience. This earlier emphasis on space perhaps reflected Michel Foucault's famous 1967 assertion that the 'anxiety of our era has to do fundamentally with space, no doubt a great deal more than with time' (Foucault 1986: 23). The late twentieth century was a period, one leading sociologist of time argues, in which time was 'consistently theorised out of existence' (Adam 1989: 464).

Hassan argues not for the elevation of time above space but for analyses that consider space and time as equally important co-constitutive elements of the social world. While space has received significant theoretical attention, the study of time still requires 'a conscious theoretical effort to render it clearer', not least because the 'temporal turn' has shown how complex and varied are the multiple times of social life (Hassan 2010: 93). Against the backdrop of broader theoretical moves to deconstruct or pluralise 'the social', Hassan notes how the heterogeneity of social time 'reflects our messy humanity, and its baleful proneness toward hierarchy, exploitation, the concentrations of power, and increasing layers in the complexity of life' (Hassan 2010: 93–4).

However, other authors counsel caution in identifying a paradigmatic analytical shift. Helga Nowotny notes the seeming paradox between common complaints about a lack of attention to time in the social sciences being accompanied by an ever-growing literature on the topic and concludes, furthermore, that 'one can certainly not claim that "time is neglected" in the social sciences' (Nowotny 1992: 441). Moreover, she suggests this identification may be due to two factors. First, a 'protective assertion' by authors wishing to stake a claim on time and temporality without first taking the trouble to account for existing work in the social sciences. Second, that scholars might be 'discovering anew' a well-established finding that time is socially constructed and that all social life has a temporal dimension (Nowotny 1992: 423). Similarly, Bender and Wellbery describe the ubiquity of time in social analyses, noting that time 'asserts itself in contemporary enquiry less as a given than as a range of problems', but it is probably unwise to think of this as a new 'temporal paradigm' in the various disciplines in which these problems have been identified (Bender and Wellbery 1991: 15).

Bearing these warnings in mind, it is still possible to make a strong case for making time visible in analyses of the contemporary world, not least because time has a 'pervasive role' in modernity that is often unquestioned, or predicated upon simplistic and totalising conceptions of time (Adam 1995: 149–75). This problematisation of time and temporality has begun to register in IR, exemplified by Kimberly Hutchings' perceptive analyses of dominant theories of contemporary world politics and history (Hutchings 2007, 2008). Hutchings finds liberal and realist IR beholden to temporal assumptions grounded in the traditions of Western liberal modernity, principally Kant, Hegel and Marx. She provides a radical counter-balance to these hegemonic renderings of political time through her advocacy of postcolonial, feminist and post-structuralist theories of time that better reflect the 'heterotemporality' of international life. Crucially, she demonstrates how political-philosophical understandings of time relate to contemporary debates about citizenship, feminism, humanitarian intervention and globalisation. Andrew Hom also examines the issue of Western temporal 'hegemony' and its constitutive role in International Relations and IR theory (Hom 2010). He relates the co-evolution of territorial state sovereignty and Western clock time and identifies how the methods of time-reckoning that developed during the Enlightenment were crucial to the foundations of political modernity. This understanding of time became global during colonisation and world war, so that what was once *local* Western European time is now *global* in geographic and political reach. Time has become 'modernity's hegemonic metronome' (Hom 2010: 1170).

Notable too is Ian Klinke's exploration of the politics of time (chronopolitics) as a key component of critical geopolitics (Klinke 2013). Klinke interrogates the overlooked constitutive role of temporality in geopolitical discourses, while charting a productive path through the dichotomous constructions of time and space in geopolitics. In its concern with narrative constructions of identity, Klinke deploys the Bakhtinian concept of the literary chronotope – as does this book – as a means of showing how geopolitical narratives are structured around conceptions of spatiotemporality. Klinke's project is a conscious extension and critique of well-known studies in IR and critical geopolitics that include James Der Derian's work on war, information technology and the politics of speed (Der Derian 1990, 1992, 2002, 2003, 2009a). In turn, Der Derian owes much to the provocative *oeuvre* of the French 'philosopher of speed' Paul Virilio (Huysmans 1997; Der Derian 1999, 2009b), whose work informs this book also. As Klinke notes, these critiques of time and speed do not exhaust the heterotemporality of sociopolitical life and may fall prey to the very same totalising conceptions of time they set out to confront.

These proposals for restoring time and temporality to the centre of our studies of international politics find resonance with work identifying the specific benefits of such a move to particular theories of IR. Andrew Hom and Brent Steele (2010) have argued for a more reflexive realism that takes better account of its own historical contingency and intersubjectivity. A central component of this as-yet unrealised project is the necessary shift from cyclical and linear accounts of time that inform the main schools of IR. Chief among these is Waltzian realism, which settles upon a cyclical view of time as a means of forestalling 'eternal anxiety' about 'indeterminate futures' (Hom and Steele 2010: 275–6). Neoliberalism and non-critical forms of constructivism are often informed by teleological notions of progress, which imply linear conceptions of time, not least Alexander Wendt's predictions about the inevitability of a 'world-state' (Wendt 2003). Hom and Steele advocate a more 'open' time that neither denies the possibilities of change (cyclical time) nor requires narratives of progress (linear time). Such an orientation would open the 'horizons' of realism to more historically contingent understandings of political change. This is, in essence, also a call to embrace historical uncertainty and to recognise the heterotemporality of international politics.

Hom and Steele acknowledge the more 'open temporal visions' of poststructuralism and critical constructivism (Hom and Steele 2010:

279). Given its prioritisation of the uniqueness of historical context over grand and timeless theory, constructivism's translation into IR is inherently concerned with the role the past plays in how people perceive the present (Copeland 2000). Felix Berenskoetter shows how this attention to historicity has made constructivists hesitant 'to claim the future' (Berenskoetter 2011: 648), as they recognise their own roles in constructing knowledge about the future and thus their potential complicity in political discourses of the state (see also, Steele 2007). He commends constructivism as a way to understand 'the function of visions in the human attempt to establish a sense of Self in time', due to its theoretical commitments to reflexivity and the construction of identity (Berenskoetter 2011: 648). 'Visions' refers to both utopias and dystopias as a means of imagining future political order but also as modes of thinking to effect political action in the present. Moreover, these visions are essential ways in which identities are formed and which sustain – and constrain – collective future-oriented actions. They stimulate, mobilise and direct 'activities towards decreasing or increasing the distance between what is and what could be' (Berenskoetter 2011: 663), a sense that emerges in this book also.

This emphasis on temporality in the social construction of identity has taken on increased salience since 11 September 2001 and the subsequent 'war on terror'. The 'event' of 9/11 itself has been explored as a 'rupture' in historical consciousness allowing for the transformation of political order (Bousquet 2006). On the one hand, 9/11 was constructed as 'the day that changed the world', but on the other political practices in its wake were expressive of 'business as usual' (Campbell 2002). The United States and its allies sought to read meaning into 9/11 through a suite of established political responses honed in the Cold War, not least by the construction of Us/Them scenarios in which there was little room for moral subtlety or uncertainty and which foreclosed the possibilities of other forms of political response. Bousquet writes of 9/11 as an apocalyptic event, a 'revelatory and prophetic' experience that formed 'a temporal break and omnipresent point of reference around which we subsequently reinscribe our historical and political narratives' (Bousquet 2006: 741). It is both 'Ground Zero' and 'Time Zero', narrowly identified in space and time, around which everything else becomes organised. The apocalyptic 'event' of 9/11 disclosed deep anxieties in American life about terrorism and technology, which needed to be overcome through mediated processes of national identity construction, which facilitated the pursuit of a spatially and temporally unbounded war on terror (Debrix 2008). According to Lundborg, 9/11 must be understood both as an historical event and as a 'pure event' constantly in a state of 'becoming', being renegotiated and reinterpreted to serve continuing political ends (Lundborg 2012). In this way, time becomes a discursive resource in the strategic prosecution of the war on terror (see also Jarvis 2009; Fisher 2013).

This emphasis on the catastrophic event has informed an emerging interdisciplinary concern with how these events might contribute to distinct forms of post-9/11 security governance. These analyses are part of a wider concern in security studies and allied fields like human geography with technologies of governance in the global 'risk society' (Beck 1992), which identifies a shift in risk assessment 'from retrospective estimations of harm to a future-driven outlook' (Mythen and Walklate 2008: 223). This work engages with expressions of anticipatory and preemptive security post-9/11 (de Goede 2008a, 2008b; de Goede and Randalls 2009; Anderson 2010a, 2010b; Amoore 2013; Stockdale 2013), which aim to forestall certain forms of risk and social hazard before they emerge from the social fabric (Bigo 2006; Martin 2014). Because of this shift in the temporality of action, security professionals and others must operate in situations of imperfect knowledge, and Claudia Aradau and Rens van Munster describe how a paradoxical 'knowledge of the future' is developed in and through security discourses (Aradau and van Munster 2007, 2008). Of particular interest is how unknown catastrophic futures are imagined and 'inhabited' through security practices like emergency planning, disaster preparedness exercises, simulations and other ways of rendering the future aesthetically present (Aradau and van Munster 2011; Adey and Anderson 2012; de Goede and de Graaf 2013). The media play a critical role in fostering the imaginative 'plurality of possible futures' that feeds public anxiety and desire and the possibilities of political action thus facilitated (de Goede 2008b; Grusin 2010a). This sub-field of security studies has not yet turned substantively to cyber security and this book contributes to these discussions of risk, security and temporality by looking at the temporalities disclosed in cyber security discourses and practices. In the next chapter, we will look at how to begin exploring time and temporality and how social conceptions of time inform politics in the world.

2 Towards a politics of time

From time to temporality

Time is mysterious. It is at once familiar and exotic, both quotidian and extraordinary. We are aware of its ubiquity, its structuring role in our lives and in our relations with the world, yet most of us give time little serious thought beyond the pressures of the clock and the seasons, the constraints of day and night, and the memorialising of the passing of time so emblematic of human consciousness. It is so integral to our lives that we rarely interrogate its presence or its nature, except most poignantly as something that passes and of which we have too little. That we give a name to an entity or phenomenon that we can distinguish as qualitatively different from other aspects of reality suggests its peculiarity and uniqueness, even as we consistently fail to define quite what time is or might be.

This uncertainty as to the nature of time has long been recognised. In third-century Rome, the philosopher Plotinus observed that although we might intuit the nature of time, when 'we make the effort to clarify our ideas and close into the heart of the matter we are at once unsettled' (Plotinus 1992: 253). A century later, Saint Augustine of Hippo asked: 'What then is time? Provided that no one asks me, I know. If I want to explain it to an inquirer, I do not know' (Augustine 1992: 230). In our own time, the philosopher Alfred North Whitehead remarked: 'It is impossible to meditate on time and the mystery of the creative passage of nature without an overwhelming emotion at the limits of human intelligence' (Whitehead 1920: 73). These limits are felt keenly by all who would engage with the problem of time in physics, in philosophy or, as in the current enquiry, as a key aspect of contemporary politics and security.

It is remarkable that at the beginning of the twenty-first century, as we develop ever more sophisticated ways of exploring the cosmos and understanding our place within it, neither philosophy nor science can determine conclusively if time is even real (Wesson 2010). In 2013, scientists running the most ambitious scientific experiment in history, conducted at the

Large Hadron Collider on the Franco-Swiss border, announced the existence of a subatomic particle – the Higgs boson – hitherto only predicted in theory, thereby validating decades of physical research and experiment. Despite the intellectual, financial, political and material resources harnessed in the search for the Higgs, no scientist working on this paradigmatically 'big science' (Galison and Hevly 1992) project would be able to tell you definitively if time – as an ontological constituent of reality – exists or not. Indeed, no one has ever carried out or imagined an experiment that would allow us to decide either way. It may even be that time – expressed as the physicists' t – has no ontological reality at all, yet the language of time remains rooted firmly in almost all cultures and societies. The philosopher Daniel Dennett even argues that language itself is a prosthesis 'that permits us to play such glorious tricks with time' (Dennett 2000: 24). In the English language, 'time' is the most common noun, even above 'person', 'thing', 'world' and 'life'.[1] Whatever we perceive or think of as time is clearly something of fundamental importance to the human mind and to human culture.

At its most elementary, human culture is itself an expression of the awareness of time manifest as inevitable death. Hundreds of millennia before cities, agriculture and the other civilisational trappings with which we presently identify the human, Palaeolithic humans 'awoke to the predicament of ourselves in time' (Frank 2011: xviii). This predicament marks the realisation that irrespective of what we do in life, death marks the finitude of earthly existence. Our inherent 'being-towards-death' (Heidegger 2010) is the inevitable context of all human action and the driving force behind 'our determination to live in such a fashion that we transcend our tragic limitation' (McManners 1981: 2). As Ovid reminds us in *Metamorphoses*: 'O Time, thou great devourer, and thou, envious Age, together you destroy all things; and, slowly gnawing with your teeth, you finally consume all things in lingering death!' (Ovid 1916: 381). From our perspective, this most certainly includes humans of mind, flesh and bone. This sense of the inexorable passing of time leads us to perceive time as the dimension of change, in which we witness the perpetual rhythm of days and nights, the turning of leaves on the trees, the extraordinary physical and mental growth of our offspring, and the melancholia of senescence and death. Through these observations, we identify temporal variation in the lives of things, people and places, over which we have little or no control: time passes, irrespective of human

[1] 'The OEC: Facts About the Language', http://oxforddictionaries.com/words/the-oec-facts-about-the-language. 'Time' is the 55th most common word in the Oxford English Corpus of over two billion words.

desires and interventions. We induce from commonplace observation and the application of no greatly sophisticated reason the larger and uncontroversial truth that time is a fundamental constituent of reality: ontologically, it just *is*.

Yet, this is not a philosophically sustainable position. There is a key distinction between 'time felt' and 'time understood', an unresolvable conflict arising from the emergent nature of reality itself (Fraser 1999: 40). At its most ordinary, we may discern a difference between the objective ('understood') time of the clocks and calendars by which we reckon time and order society, and the subjective ('felt') time of human experience, ancient and modern, in which *tempus fugit* (time flies) but a minute may seem like an age. There is an 'asymmetry between the obviousness of the experience of time, and the unobviousness of the idea of time', which introduces a considerable 'perplexity to reflective thought' on the nature of time (Fraser 2003: 15).

It is therefore unsurprising that our knowledge of time should be contested and subject to continual negotiation, or that it constitutes a central facet of political behaviour, as is the premise of this book. The time of humans does not exist a priori but must be constructed intersubjectively as a field of social knowledge. Whether time is a dimension of the fabric of the universe or not is mostly irrelevant to our everyday conception of what time is or might be. It is not unimportant in cosmological terms, but to discover the reality or otherwise of time as a component of physical reality would not materially change the social existence of the human animal, at least not immediately. To believe in the (non-)existence of physical time is itself to speculate as to the nature of reality; it is an epistemological statement about reality that is open to challenge. Philosophical realists are as likely to dispute the nature of time as postmodernist relativists are to reject any realist or materialist position on the scientific existence of time. To speak of time is, potentially, to mean many things, 'many species' of time (Castoriadis 1991). In all cases, how we perceive time is integral to how we understand, interpret and communicate our world to others, not least in the realm of politics.

This chapter proposes an initial understanding of the politics of time (chronopolitics) as a social construct, in which the temporal perspectives of human groups are fundamentally constitutive of political behaviours, including security as an inherently political practice and orientation. The key insight is that chronopolitics, even though socially constructed, is not only concerned with the time of the human. Like time itself, the politics of time is informed by and concerned with multiple temporalities at many levels of reality, and the theoretical innovation of this chapter is to bring these other forms of nonhuman temporality into chronopolitics. This provides the basis for understanding cyber security in its chronopolitical dimensions as concerned with both human and nonhuman temporalities, as befits a form of security that intends to regulate and control the human and nonhuman entities enmeshed in vast sociotechnical assemblages like the internet.

This chapter develops the argument in six sections. The first section details how human conceptions of time emerge from the physical universe, with reference to J.T. Fraser's model of emergent temporality. It demonstrates how different forms of temporality correspond to distinct levels of complexity in the physical universe, including the collective sociotemporality of human groups that shape political behaviours. The second section examines how we can know the temporalities of nonhuman entities and through reason and technology construct a holistic conception of the temporality of the universe. This is an essential step in addressing the temporalities of information technologies, entities with which we cannot directly communicate but whose temporalities are so important to contemporary politics. Even if oriented to the future, politics is enacted in the present, and the third section examines in detail the concepts of 'nowness' and 'presentness', proposing, in common with phenomenological theories of subjective experience, that we collectively inhabit a 'social present' in which past, present and future are intertwined. Further entanglements are discussed in the fourth section, as time cannot be wholly abstracted from considerations of space, matter, energy and other constituents of physical reality. How we perceive these interactions helps shape the stories we tell about social reality, the 'chronotopes' that inform the narrative foundations of politics. Within this complex ideational manifold we can further identify specific 'chronotypes' that express particular temporal biases and through which time becomes conceptually and practically significant. The fifth section prepares the ground for chronopolitics by discussing politics as expressions of the 'temporal', differentiated from scientific and spiritual representations of eternity and cosmos. The chapter concludes by drawing together the preceding discussions, offering some preliminary thoughts as to how conceptions of time and temporality shape political behaviours in the social present.

Emergent sociotemporality

Since we wish to understand how collective perceptions of time affect and shape political behaviours, it is important to establish how collective temporalities come into being. The following discussion draws upon J.T. Fraser's hierarchical model of emergent temporality, which provides a framework for considering how collective time (sociotemporality) relates ontologically and epistemologically to reality. In an interdisciplinary project to understand time extending across decades and presented most accessibly in his penultimate book, *Time, Conflict, and Human Values* (1999), Fraser developed an epistemic framework that 'admits and correlates qualitatively different causations and times across the organizational levels of nature [as] revealed by contemporary science' (Fraser 1999: 35). Despite its grounding in scientific realism, Fraser recognised that science alone would be insufficient to attempt this task. This is not because science is incapable of answering questions about time satisfactorily (if not conclusively, as discussed previously) but that its theories and methods have not yet been, or perhaps cannot yet be, extended to all the forms of time which we can identify and in which we might be interested. Many ideas about time – particularly its 'flow' or 'passage', the problem of 'nowness' and subjective temporality – must be imported from domains of disciplinary knowledge outside science, including philosophy (Fraser 2005). At the same time, instructs Fraser, 'let us listen to philosophy but not anchor our enquiry there' (Fraser 2003: 16). Fraser's work is self-consciously and necessarily interdisciplinary and represents a general epistemological position that philosophy without science is 'immature' and science without philosophy is 'impossible' (Gjertsen 1989: 69).

Fraser's model is a cultural-cosmological model of time that draws on the sciences (including scientific cosmology) to establish its foundations and its levels of analysis. Fraser pluralises 'time' by disaggregating the term according to what he perceives as the six evolutionary levels of nature, each of which corresponds to a particular temporality. His proposition is 'that time had its genesis at the birth of the universe, has been evolving along a scale of qualitative changes appropriate to the complexity of the distinct integrative levels of natural processes, and remains evolutionarily open-ended' (Fraser 1999: 38). Each temporality is emergent from the last and together they comprise a 'nested hierarchy of presents', which are 'the canonical forms of time' (Fraser 1999: 37–8). These presents exist simultaneously because, rather than the temporality emerging later replacing that already existing, it subsumes the earlier within itself. If this were not the case, human perceptions of time, which have emerged relatively recently in cosmic evolution, would not be able to comprehend even in the most superficial way the extant forms of cosmic and biological time.

Atemporality, as the name suggests, is the time of no time and consequently of no causation (Fraser 1999: 38). This is not to equate atemporality with non-existence but rather with a particular mode of existence exemplified by electromagnetic radiation (i.e. photons, electromagnetic waves). Since Einstein formulated the theory of special relativity at the beginning of the twentieth century, we have known that due to the relativistic effects of time dilation, clocks moving away from one another at a constant velocity will each appear (to the other) to run slower than their counterpart. At the speed of light, time slows down completely and ceases to have any meaning in human terms. From the perspective of a massless photon brought into being in the early years of the universe (it must be massless or it could not travel at the speed of light), no time has passed in the nearly fourteen billion years since its apparent creation (Greene 1999: 51). More accurately still, if we consider time as the dimension of change rather than a fixed dimension, everything (from the photonic observer's perspective) has happened at once. Atemporality describes a world of electromagnetic chaos that has no time and no causation.

Prototemporality is the time of non-photonic waves and particles with non-zero rest mass (Fraser 1999: 37). These entities have mass, so they cannot travel at the absolute speed of light and must therefore possess temporality, however rudimentary. Prototemporality is the time of events or instants that may be identified statistically but that are not ordered with respect to anything we might identify as the passage of time. Causation is therefore not deterministic but probabilistic, as is the case with certain quantum mechanical processes and as the early universe must have been. Deterministic causation only emerges with *eotemporality*, the time of the observable physical universe in which matter is ordered into visible objects like stars and galaxies and in which events are 'countable and orderable' (Fraser 1999: 16). Fraser's example of the natural numbers, {*0, 1, 2, 3,* ...}, illustrates that although eotemporal events (like natural numbers) are successive they do not demonstrate a temporal direction.[2] Rather, they are time-reversible, like most known physical laws, and deterministic, in that certain outcomes must follow from their premises and initial conditions.

By contrast, *biotemporality* is the directed time of life (Fraser 1999: 36). Time proceeds in one direction for living organisms, whose automatic activities are directed towards the ends necessary for the maintenance of individual and species existence. Biotemporality is tensed, in that the past may be distinguished from the present and the future. The unwitting biological operations of humans exist in this biotemporal matrix of necessity, yet their higher cognitive functions operate in the realm of *nootemporality*, in which there is conscious awareness of the passing of time and the extrapolation of temporal boundaries into the past and the future. In the nootemporal world, intra-species subjectivity emerges in the

[2] Natural numbers are the everyday non-negative integers (whole numbers) used for counting and ordering.

distinction between self and other, and actions are directed towards the attainment of symbolic ends as well as the more tangible goals of subsistence. Causality lies in the ability of humans – or, hypothetically, any other sentient beings – to determine the character of their actions, even if the course of future events cannot be known (and assuming we believe in the freedom of will in a quantum universe). It is this human 'experience and idea of time's passage [that] must be brought to physics; they cannot be derived from it' (Fraser 1999: 35).

The highest proposed level of time is that of *sociotemporality*, the 'postulated level-specific temporality of a society . . . a social consensus necessary for the survival of a society, a definition of that society's way of being' (Fraser 1999: 37). Sociotemporality is a means to create order in the present and is also how society locates itself with respect to the past and the future. Fraser admits a certain difficulty in further defining sociotemporality, due to the lack of a higher-level language that could describe the collective in terms other than those derived – as our language must be – from that collective. In this 'open-ended' schema, there may be a 'higher' level of temporality which we presently have no access to or knowledge of but which may yet come to exist. Similarly, there is no logical reason why there should not exist a more fundamental level of reality and temporality than the atemporal (Schaffer 2003). We might also question the omission of a chemical or geological temporality, a 'mesotemporality' between eotemporality and biotemporality (Helm 2001). Nevertheless, Fraser provides an intelligible framework for the consideration of coeval temporalities that correspond to different levels of complex reality, a schema that does not rely on a strictly linear narrative of the cosmos evolving *in time* but on the emergence of time from reality itself.

Fraser moves away from Newtonian absolute time as a receptacle of knowable reality into a scientific and philosophical milieu informed by the twentieth-century revelations of relativity and quantum mechanics, in which time is relative and mutable and the only constant is the speed of light. This way of looking at emergent temporality avoids an historical tendency to relegate the times of the non-present to an unknowable and largely irrelevant prehistory, or, as anthropologist Robin Fox puts it, as 'a mere run-up to the real thing' (Fox 2001: 129). Crucially, Fraser develops the notion of sociotemporality as a form of knowledge, an intersubjectively constructed knowledge about time at all levels of reality. As Adrian Mackenzie states, time is not simply an 'entity or substance which would simply have a past, present and future as its attributes . . . temporality is an openness or disjunction affecting every level of what exists' (Mackenzie 2002: 9). This includes the temporalities of the nonhuman, whether these derive from atomic or organic entities, the inanimate or the animate. Fraser's model, although grounded in a distinctly realist view of the cosmos, is social constructivist in the sense prescribed by Ian Hacking, in which the construction metaphor retains 'one element of its literal meaning, that of building, or assembling from parts' (Hacking 1999: 49). Sociotemporality is therefore a constructed temporality – a temporal assemblage – and an assembled form of knowledge. The next section considers in more detail how, if sociotemporality is a form of knowledge incorporating temporalities at multiple organisational levels of nature, we humans can know these other temporalities.

Knowing nonhuman temporalities

There is a strong case for attempting to know and understand the temporalities of the nonhuman, although the reasons are perhaps not immediately obvious. If we propose that human temporalities are constitutive of political behaviours, why do we need to consider nonhuman temporalities at all? With respect to cyber security – and, arguably, to all forms of security and politics – the answer lies in understanding the environment in which cyber security operates and which it intends to regulate. Most cyber security discourses are highly technologically deterministic: narratives rely upon conceptions of computing machines and the networks in which they are arrayed and the electromagnetic content that passes through them. Moreover, the temporalities of these nonhuman entities – particularly those associated with speed and acceleration – are used to understand the impact of these technologies upon the human and to justify political responses and technical counter-measures, which themselves attempt to intervene in the temporal structures of the nonhuman. More accurately, these networks are sociomaterial assemblages in which humans and nonhumans are enmeshed in a dynamic and complex fashion. Cyber security has many parts operating in many modalities, each of which may offer up distinct temporalities for identification and exploration. It is not only an assemblage of things but an assemblage of the dynamic temporalities of those things, temporalities that interact and intermingle in multiple ways; time, too, is assembled. Fraser's hierarchical model of emergent temporality implies that nonhuman temporalities are inherently subsumed within the collective temporalities of human politics, which provides a fresh opportunity to understand the political linkages between human and machine.

It is inadequate to assert that human and machine are so entangled without examining further how we can know these forms of nonhuman temporality. Fraser's model interprets reality as a form of knowledge, constructed in the senses and bounded by communicative interaction with the reality in which an entity is embedded. Fraser develops this proposition with reference to the concept of *umwelt*, as theorised by biologist Jakob von Uexküll (1864–1944). Uexküll did not invent the term but did redefine its modern connotation of an animal's perceptual life-world (Winthrop-Young 2010: 215). For Uexküll, the umwelt is the subjective spatio-temporal world particular to living creatures as diverse as the burrowing worm, the butterfly and the field mouse. All animals inhabit their individual phenomenological sense-worlds from which they alone derive meaning and significance. Significantly, the animal umwelt is 'the world as it appears to the animals themselves, not as it appears to us' (von Uexküll 1957: 5). Uexküll was influenced by a Kantian understanding of reality as a phenomenon revealed through the human mind, but he expanded this to include reality revealed through the body and to the nonhuman animal (Pobojewska 2001). He refused to privilege the human umwelt over any other and is notable for his 'unreserved abandonment of every anthropocentric perspective in the life sciences and the radical dehumanization of the image of nature' (Agamben 2004: 39).

Uexküll held to a strong form of vitalism, a doctrine usually rejected by contemporary science due to its insistence on the existence of a 'life force' which marks living organisms apart from the non-living: 'a life-principle that animates matter, exists only when in a relationship with matter, but is not itself of a material nature' (Bennett 2010a: 48). Fraser implicitly rejects the Uexküllian vitalist presumption that time exists only for living beings and generalises the umwelt principle to include those worlds not ordinarily sensible to living beings. We cannot directly experience the umwelts of photons or celestial bodies, but we can begin to know the worlds of other species and material bodies so that they become part of our own 'noetic umwelt', in which 'noetic' pertains to the human mind or *nous* (Fraser 1999: 25). This is achievable through the double extension of human sense: first, by dint of our cognitive abilities and the application of reason and theory; second, through indirect interrogation by technological instrumentation and other material tools (Fraser 1999: 24–5, 2001). This second category we may understand as technical orthoses, artefacts that supplement or extend human capabilities (Clarke 2011). In the modern context, we may additionally read this orthotic extension as symptomatic of the gradual yet persistent 'cyborgisation' of the human species, in which we all become 'chimeras, theorized and fabricated hybrids of machine and organism', which produce new forms of knowledge and new sites of political contestation (Haraway 1991: 150). These forms of extension make the previously undetectable detectable.

Of this extensibility of the human experience, Martin Heidegger, also influenced by Uexküll (Buchanan 2008), wrote of the uniquely human ability to 'penetrate ever more deeply in [the] penetrability' of the world (Heidegger 1995: 193). He characterised humans as 'world-forming' (*weltbildend*), against animals that are 'poor in world' (*weltarm*) and material objects like stones, which are 'worldless' (*weltlos*). He defines 'world' as having access to beings outside the subject. The stone has no world as it has no way of accessing external beings. This is different from the animal, which, as Uexküll showed, has access to external beings, although it remains 'immured as it were within a fixed sphere that is incapable of further expansion or contraction' (Heidegger 1995: 198). The novelist J.M. Coetzee writes: for animals, 'their whole being is in the living flesh' (Coetzee 1999: 65). In this Heideggerian formulation, the animal is deprived of aspects of the world and is therefore 'poor in world'. The human ability to access other beings through the extension of the senses allows for the formation of an ever-expanding world, even if, with respect to other umwelts, we can never truly know them. This lack of phenomenological conjunction means, as Coetzee notes, 'You can be friends neither with a Martian nor with a bat, for the simple reason that you have too little in common with them' (Coetzee 1999: 65).

The influence of Heidegger on Fraser is unclear. Fraser qualifies the Heideggerian insistence on the unchanging nature of the animal umwelt by observing that animal umwelts change as they evolve (Fraser 1999: 23), an admittedly slow process that does little to diminish Heidegger's original argument that animals are poor in world. Moreover, Fraser does appear to break with Heidegger's concept of world in his extension of the umwelt principle itself, definitively including umwelts not belonging to the human or the animal. On a superficial level, this denies the worldlessness of material objects like Heidegger's stone, but this would miss Fraser's key argument that it is the human umwelt that is under discussion, rather than any attempt to establish a categorical metaphysics of reality. For Fraser, what is important is to establish a 'working concept of reality', what he terms 'the extended umwelt principle', which equates epistemology with ontology: 'the world is the way we find it to be through the many forms of human knowledge' (Fraser 1999: 25).

This is consistent with the perspective outlined previously, in which intersubjective epistemology assumes ontological importance in social reality. Knowledge is not communicated to the senses in an unmediated fashion but must be actively constructed by the cognising subject. Fraser maintains a mind–world dualism in which the subject has no direct access to external reality but does not deny the probable existence of that reality or the material origins of the human mind. This inverts the transcendentalism of Kant, asking instead: what is the nature of reality, so that knowledge of the world is made possible? We cannot know directly the temporalities of neutrons or narwhals, but through reason and technical extension we can model those temporal umwelts so that our models correspond well enough with prospective unknowable realities that they can serve as the basis for our conception of time in general. Noetic time – in its totality as the sum of human knowledge of time – is the nested hierarchy of all these temporalities, from the atemporality of electromagnetic chaos to the collective sociotemporality of the social group (Fraser 1999: 34).[3] In this way, we can begin to understand the temporalities of sociotechnical assemblages like the internet, in which cyber security intends to make its mark.

Security *qua* politics may be oriented towards the future, but those who desire and enact security are situated firmly in the present and their actions and utterances occur now. Fraser's model is explicit that temporalities are temporal 'presents' happening 'now' across all levels of reality but neither 'presentness' or 'nowness' are unproblematic categories. The following section explores these concepts further in order to provide additional means to understand sociotemporality.

Now and the present

In order to comprehend something of the nature of time, we often turn to metaphors informed by other aspects of our worldly experience and describe time in terms drawn from the spatiality of nature. In Western thought, we encounter, for example, the Newtonian *flux aequabilis*, the uniform 'flow of time' that appears to describe our sensory perception as to its inexorable passing. The metaphor of temporal fluidity is an ancient one. In Plato's *Cratylus*, Socrates tells Hermogenes:

> Heraclitus says, I think, that 'All things move and nothing is at rest', and, likening the beings to the stream of a river, that 'You could not step twice into the same river'. (Ademollo 2011: 203)

Heraclitus' emphasis on the perpetual Becoming of the cosmos has been glossed through the centuries as 'everything flows' (in Greek, *panta rhei*) (F.E. Peters 1967: 178) and which has greatly influenced subsequent thinkers. Marcus Aurelius would write in the second century AD:

[3] In practice, there may be little difference between noetic time and sociotemporality (Fraser 1999: 68). For the purposes of clarity and consistency, sociotemporality is preferred here.

> There is a river of creation, and time is a violent stream. As soon as one thing comes into sight, it is swept past and another is carried down: it too will be taken on its way. (Aurelius 2006: 31)

Philosophers and psychologists have long recognised the problems of using metaphors of spatial mobility to describe time (Williams 1951; Casasanto and Boroditsky 2008). However, as Arthur Prior notes, alluding to Isaac Watt's famous paraphrasis of Psalm 90, time may be 'like an ever-rolling stream, but it isn't really and literally an ever-rolling stream' (Prior 1993: 35), any more than it was when Heraclitus and Marcus Aurelius made similar metaphorical allusions.

Our tendency to deploy metaphor is explicable with reference to our perception of the passing of time: 'some future event to which we have been looking forward with hope or dread is now at last occurring, and soon will have occurred, and will have occurred a longer and longer time ago' (Prior 1993: 35). Time, like the language that expresses it, is 'tensed' and events and processes have locations – past, present, future – in time.[4] Moreover, these tenses portend the deeper apparent truth that time passes in one direction only. According to the astronomer Arthur Eddington, who coined the phrase in 1928, this one-way property is 'time's arrow', a projectile flying through reality with its tip always pointing towards the future (Eddington 1928: 69). Time's arrow flies from the unchangeable past to unknowable futures, passing through a transient now that itself always fades into memory.

The question of tense has acquired the status of an intractable metaphysical problem. If events that happen in the present must in the future be considered past, or any other permutation of the tenses expressed in these terms, tense cannot be an essential property of an event. If everything is situated within time as the dimension of change, everything must be changing and must possess all tenses at once. This has not escaped the attention of poets. T.S. Eliot wrote:

> Time present and time past
> Are both perhaps present in time future,
> And time future contained in time past.
> If all time is eternally present
> All time is unredeemable. (Eliot 1971: I.1–5)

All moments are therefore supposed to possess all temporal properties (pastness, presentness, futurity), but no moment can co-instantiate all these mutually exclusive properties, leading to the philosophical

[4] Etymologically, 'time' and 'tense' both derive from the Latin *tempus* (time). The three tenses themselves – past, present and future – have much older histories (Binnick 1991).

conclusion that this is an absurd proposition and tenses are unreal (Mellor 1993: 51). This problem of tense is also the foundation of J.M.E. McTaggart's famous deduction from logical principles that time too must be unreal (McTaggart 1908).

Metaphysical discussions over the unreality of tense and time aside, the nature of the present and what constitutes 'now' are key concerns for both the science and philosophy of time. Einsteinian relativity, for instance, proposes that there is no 'now' that can be experienced simultaneously by two or more observers; the 'presentness' of an event can only be experienced locally, beyond which it is not generalisable. Moreover, 'now' is only comprehensible as a point on an imaginary plane existing where past and future meet; 'the present' has no clear ontological reality in a relativistic universe (Dainton 2010: 324–7). This perturbed Einstein greatly, Rudolf Carnap reporting that it was a matter of 'painful but inevitable resignation' for Einstein that 'the Now' meant something significant to humans, yet understanding it was beyond the help of science (Barbour 1999: 143).

The philosopher of physics Simon Saunders observes, 'the meaning of time has become terribly problematic ... The situation has become so uncomfortable that by far the best thing is to declare oneself an agnostic' (Folger 2007). In common with other aspects of the problem of time, it is unlikely that a scientific resolution to the issue of the nature of nowness is immediately forthcoming. However, congruent with Fraser's thesis about the utility of philosophy, modern philosophers have been much less reticent in asserting the nature of nowness. A review of these diverse perspectives is beyond the scope of this book, but we can identify a difference between static and dynamic views of the universe, an ancient distinction that persists into contemporary metaphysics. Theories of dynamic time hold that the passage of time has an ontological reality independent of the conscious observer. Some 'dynamists' propose that 'the present' moves along the universal timeline between past and present; others that the future does not exist and only the past and the present are real. Still others refuse the status of real to past and future: for them, time is but 'a succession of ephemeral presents' (Dainton 2010: 7).

The Heraclitean, presentist view of temporal passage and Becoming is rejected by eternalists. They subscribe to a static universe in which all times are equally real and reject the notion of a dynamic present: 'nothing becomes present and then ceases to be present' (Dainton 2010: 7). The fifth-century BC philosopher Parmenides, a contemporary of Heraclitus, proposed, in the surviving fragments of his poem, *On Nature*, that change is an illusion and that reality is unchanging and static: 'uncreated and indestructible; for it is complete, immovable and without end. Nor was it ever, nor will it be; for now it is, all at once, a continuous one' (Burnet 1930: 174–5). The details of Parmenides's argument – in which he denied the logical possibility of change and therefore of an ultimate cause of Creation – are often considered absurd, but his proposition has become 'the historical symbol of a negative emotional attitude toward the flow of time' (Reichenbach and Reichenbach 1956: 6). This image of a 'block universe' holds that 'the future is just as real, solid and immutable as the past' (Dainton 2010: 9), and in its temporal determinism has serious consequences for the possibilities of free will.

Alfred North Whitehead, who subscribed to a dynamic view of time, asserted that the 'passage of nature leaves nothing between the past and the future. What we perceive as present is the vivid fringe of memory tinged with anticipation' (Whitehead 1920: 72–3). Whitehead was concerned to deny the existence of an 'instantaneous present', postulating rather that what is 'immediate for sense-awareness [of time] is duration', contained within which is both past and future: 'the temporal breadths of the immediate durations of sense-awareness are very indeterminate and dependent on the individual percipient' (Whitehead 1920: 72). Henri Bergson also recognised the impossibility of identifying a present before it disappeared and concentrated instead on identifying the subjective qualities of 'duration' rather than theorising quantitative 'time' itself (Bergson 1971). Husserl (1964) pursued a phenomenological account of 'internal time-consciousness' in which consciousness is the basis for the experience of time rather than the subjective experience of time being derivative of any external notions of universal, 'objective' time.

Like Bergson, Husserl dispensed with notions of a 'specious present' (Andersen and Grush 2009) suspended precariously between past and future, in favour of a present with 'its own thickness and temporal spread', a continuum of 'nows' constructed in human consciousness (Gell 1992: 223). Deeply influenced by Husserl, Heidegger (2010) rejected the priority granted to the present in 'vulgar' conceptions of time, preferring instead a conception of phenomenological (and finite) time as a unity of past, present and future. Rather than experience being a succession of 'nows', we 'actively draw upon our past and project ahead of ourselves into the future, to enable our present, and it is our being concerned with the present that constitutes our Being' (Ward 2008: 100). This unitary experience manifests in a 'moment of vision' (*Augenblick*), a singular and ecstatic temporality that constitutes and gives meaning to Being itself (Ward 2008: 101). These phenomenological explorations extend the concept of the present beyond physical theory and metaphysics and into the psychological realm of consciousness and subjectivity. They illuminate a conceptual shift from *time* to *temporality* as a mode of understanding what it means to speak of 'now' or the more extensive formulation of 'the present'. Rather than a miniscule or possibly illusory punctum, the present is a textured phenomenon experienced through the human mind and constitutive of human experience.

Fraser distinguishes between the 'mental present' of an individual, in which 'ideas about future and past may acquire meaning and conduct organized in the service of distant, often abstract goals', and the 'social present', through which 'collective plans and memories are organized' (Fraser 1999: 34, 1999). The concept of duration is maintained in the social present and indicates the length of time necessary to coordinate collective action. The social present is more complexly textured in its totality than the mental presents of individuals alone, but mental presents must converge in order for consensus to emerge that enables collective action, political or otherwise. In this sense, the social present is characterised by a tendency to flatten difference in pursuit of common goals. From this stabilisation of the dynamic heterogeneity of multitudinous presents emerges the sociotemporality through which the present is imagined and constructed.

Like all knowledge, our collective knowledge of time is not static. Sociotemporality does not simply emerge from temporalities at lower levels of complexity and remain there, fixed and unchanging. We have previously observed that what we collectively think of time is influenced by new scientific theories and discoveries, by continued attempts to understand the philosophy of time and by social enquiry into how time is perceived and constructed. Sociotemporality is reflexive and recursive and is the temporal umwelt that corresponds to the level of collective social entities. As such, it can be considered further in the light of social epistemology. Social epistemology is concerned with the social construction of knowledge, specifically 'the relevance of social relations, roles, interests, and institutions to knowledge' (Schmitt 1994: 1). This perspective assumes that knowledge is socially rather than individually constructed and that truth and evidence are negotiated through social relations rather than through individual cognition alone, as is the assumption of 'traditional' epistemology as a sub-field of philosophy (Goldman 1999; Fuller 2002).

With respect to the 'temporal cognitive biases' (Deibert 1997: 33) that comprise in part the social episteme, sociotemporality is that aspect concerned with the totality of social beliefs about, and experiences of, time. Anthropological studies have long shown how varied are these collective conceptions of time between social groups (Gell 1992; Munn 1992). While accentuating sociotemporal heterogeneity within the human species, this body of work posits a general understanding that conceptions of time are fundamental to collective self-understanding and social organisation. These conceptions of temporality are often culture- or language-specific, as illustrated by the difficulty people learning second languages have in accessing the subtleties and idioms of temporality embedded in those other languages (Dietrich *et al.* 1995). Being unable to speak the appropriate 'language of time' is a hindrance to full engagement with any language community, on account of the habitual strategic manipulation of the dimensions of temporality to convey 'important social messages' of similarity and difference within both interpersonal relations and societal politics (Zerubavel 1987).

Embedded within sociotemporality is its own genealogy – the stories of science and philosophy, of myth, power and imagined histories – that gives our constructed time its own additional temporal dimension: its narratives of emergence and change. This narrative dimension of sociotemporality is crucial both to its imagining and to its communication as a means of its own construction.

Temporality and narrative

In the 1930s, Mikhail Bakhtin introduced the concept of the 'chronotope' into literary criticism and the philosophy of language. Bakhtin argued that to create plausible worlds in literature, authors must draw upon how space and time are organised and understood in their own realities. Chronotope – literally, 'time-space', from the Greek *chronos* and *topos* – was Bakhtin's chosen term to represent 'the intrinsic connectedness of temporal and spatial relationships that are artistically expressed in literature' (Bakhtin 1981: 84). Chronotopes fuse 'temporal and spatial indicators' into 'one carefully thought-out, concrete whole', so that time 'thickens, takes on flesh, becomes artistically visible', and space, in similar fashion, 'becomes charged and responsive to the movements of time, plot and history' (Bakhtin 1981: 84). Bakhtin's subsequent analysis showed how chronotopes infuse and structure diverse genres of the novel; indeed, he proposed that chronotopes determine genre. Many chronotopes may co-exist in a text, but narratives tend to be dominated by single chronotopes, which act as 'organizing centers' around which 'the knots of narrative are tied and untied' (Bakhtin 1981: 250). Dominant chronotopes are stabilised and stabilising cognitive representations of spatiotemporal reality that construct meaning and shape narrative.

Illustrating that it is not just writers of fiction that draw inspiration in this way, Bakhtin was influenced by the notion of 'spacetime' developed in early twentieth-century physics. In 1908, the German mathematician

Hermann Minkowski asserted, ‘space by itself, and time by itself, are doomed to fade away into mere shadows, and only a kind of union of the two will preserve an independent reality’ (Minkowski 2010: xv). In what became known as Einstein–Minkowski spacetime, space and time were not separate constituents of reality but had equal ontological status within a four-dimensional cosmic fabric – spacetime – in which time is a physical dimension of the universe. In spacetime, objects do not change in time but describe a physical path through four-dimensional spacetime, described in geometric and mathematical terms.

Bakhtin was unconcerned with the technical definition of spacetime within physical theory, borrowing the concept instead ‘almost as a metaphor (almost, but not entirely) . . . What counts for us is the fact that [spacetime] expresses the inseparability of space and time’ (Bakhtin 1981: 84; Brandão 2006: 133–4). Taking a direct cue from Kant’s notions of space and time as transcendental of human experience (Kant 1998: 153–92), Bakhtin channelled the spirit if not the letter of the new physics in finding space and time – more properly, spacetime – as constituents of immediate rather than transcendent reality (Holquist 2010). He left behind the Newtonian formulation of space and time as separate entities and adopted the Minkowksi–Einsteinian unitary yet relative universe as inspiration, seeing it as part of a wider development in modern thought along these lines (Morson and Emerson 1990: 254). Einstein remarked a few years later, ‘time and space are modes by which we think and not conditions in which we live’ (Forsee 1963: 81, in Wheeler 1982: 559).

The Bakhtinian chronotope reminds us that there is a deep historical ‘circulation between a physical encounter with the world, the cultural forms engendered by that encounter and the shape of consciousness determining how we think and what we experience’ (Frank 2011: 9). At its most fundamental, this is a radical entanglement of matter and meaning, in which neither is ontologically separate from the other but which emerge through their mutual constitution as ‘agentially intra-acting components’ of reality (Barad 2007). Adopting the frame of cosmology to illustrate this further, we can divine the primary sense of cosmology as the study of the cosmos, a scientific endeavour to reveal and explain the workings of the universe through theoretical exposition and empirical description. In a secondary but no less important sense, cosmology refers to a *Weltanschauung* (worldview) that may or may not have a scientific basis but which forms the cultural apprehension of the cosmos and humanity’s place within it (Kragh 2007: 2).

Cosmologies are conceptualisations of the universe that impose ontological order on reality. Historically, its two senses cannot be ‘cleanly separated' and there is no reason to suppose they could be (Kragh 2007: 2). The Bakhtinian chronotope expresses this entanglement as an inescapable fact of social existence and is the 'bridge' between two worlds, one of authorial reality and the other of the imagined time-spaces of the created text (Clark and Holquist 1984: 279). The chronotope is a necessary component of the cosmological narratives through which we understand the world and by which knowledge, experience and action are enabled. The metaphor of entanglement can be extended further with respect to time. Time is integral to all cosmologies and, through processes that emerged in human prehistory, 'a remarkable dialogue between mind and matter was begun – forever linking cosmic and human time together', a symbiotic and cybernetic dynamic we might term an 'enigmatic entanglement' (Frank 2011: 10). In the contemporary West, our cultural and scientific cosmologies are deeply entangled and our conceptions of temporality are heavily informed by and infused with scientific notions of time, as evinced by Fraser's model of temporality outlined previously.

Bakhtin's analysis addressed the fictional narratives of the formal novel but chronotopes necessarily exist in all texts (Allan 1994: 211), including the source materials interrogated in the current investigation. Moreover, given the tension that exists between chronotopes within and between texts, Ian Klinke notes that through chronotopicity, 'texts construct their ideological position; they transmit political choices, forge discursive alliances, imply different forms of social organisation' (Klinke 2013: 680). Klinke affirms the utility of chronotopes for the analysis of geopolitics, in that the choice, unconscious or otherwise, of a particular conception of temporality 'is always already a political move' (Klinke 2013: 686). It is also deeply interlaced with the politics of space, as Bakhtin's original merging of *chronos* and *topos* indicates. The importance of Bakhtin's insight to contemporary politics is that the mutual organisation of time and space demonstrates that any discursive claims to totality must be false (Haraway 1997: 41). This reminds us that although we may concentrate our enquiries on time, as we do here, time cannot simply be divorced from considerations of space, place and corporeality, or from other ontological categories like matter, energy and information (Adam 2008). Our narratives of time are inextricably bound together with narratives of space and other fundamental concepts from which we draw inspiration and through which our politics are shaped in the sociotemporal present (Massey 1992; May and Thrift 2001; Starr 2013).

John Bender and David Wellbery extract from Bakhtin's chronotope its temporal aspects, which they term the *chronotype*, a model or pattern through which 'time assumes practical or conceptual significance' (Bender and Wellbery 1991: 4). This prefigures Helga Nowotny's assertion that everyone is ‘a practician and theoretician of time’ (Nowotny 1994: 6). Chronotypes exist at multiple levels of social reality and are in a state of perpetual transformation and renewal. They are assembled from existing components of social reality and are contingent upon and incorporate within themselves the temporalities of past states of that reality. Like Bakhtin’s chronotopes, which interpenetrate one another in a constant state of cooperation and conflict (Bakhtin 1981: 252), so too the complex relationships between chronotypes. Time is ‘intrinsically manifold’ and numerous chronotypes ‘intertwine to make up the fabric of time’; these multiple chronotypes ‘can become the objects of contention because individuals experience them differently and because they bear ideological implications’ (Bender and Wellbery 1991: 15). Socially constructed and historicised notions of time are open to refutation, contestation and resistance, and the potential for conflict between sociotemporal chronotypes is at the heart of chronopolitics, as discussed in the remainder of this chapter. The following section locates politics *in* time – what is the temporality of politics itself? To conclude, the final section suggests how we might think of the politics *of* time: what is chronopolitics and why does it matter?

The time of politics

Albert Einstein, who did more than most to destabilise entrenched ideas about time as the immutable backdrop to human existence, said in 1947 that equations were far more important than politics, as the former last forever, whereas politics is ‘only a matter of present concern’ (Jungk 1958: 243). As might be expected of a physicist, Einstein articulated this position correctly with respect to the grand narrative of cosmic evolution. It is no coincidence that politics has always been equated with the temporal, not just in the sense of being somehow ‘of time’ but as temporary and transient, ‘of present concern’ only. Politics is differentiated from the more profound realms of science and spirit and the enduring truths encountered therein. For instance, the members of the upper house of the British Parliament are formally divided between two estates of the Realm: ‘Lords Spiritual’ – the twenty-six bishops and archbishops of the established Church of England – and ‘Lords Temporal’, life and hereditary peers appointed for their services to state and sovereign across the centuries of political life (House of Lords 2010). Similarly, the ‘temporal’ power of the Roman Catholic popes indicates their secular and political activity in the world and *within time* as distinct from their ‘eternal’ power, spiritual authority exercised *in eternity*, a nuance long maintained in Christian theology (e.g. Teske 2000). For Augustine, the fall of man from Eden and God's eternal grace brought into being the *saeculum*, 'the realm of temporal existence in which politics takes place' (Weithman 2001: 237). In this tradition, the political identifies with the temporal as the fleeting and sinful world of Man rather than the eternal realm of the Divine.

The links between time and politics are as obvious as they are ancient. There exist many senses of 'politics': as the art of government; as the conduct and management of community and public affairs; as the resolution of conflict by compromise and consensus; and as power and the production and allocation of resources in pursuit of social ends. In all senses, politics is 'the activity through which people make, preserve and amend the general rules under which they live' (Heywood 2000: 33). It is about the imposition and maintenance of social order and is always oriented towards some future condition. Like all purposive human activities, politics has temporal dimensions: it exists in time; it connects the past and the future; and it is itself transient in the details, remembered as history if it is fortunate, forgotten like the majority of its human subjects if it is not.

An early attempt to circumscribe what we might describe today as the 'time of politics' has its roots in ancient Greece. The early philosophers distinguished between *chronos*, the quantifiable and measurable time of the cosmos, and *kairos*, the qualitative time of lived human experience (Smith 1969, 1986). Cornelius Castoriadis warns against adopting 'old-fashioned and platitudinous' dichotomies in discussions of time (Castoriadis 1991: 38–9), but the distinction between *chronos* and *kairos* retains heuristic value and analytical utility due to its persistence in considerations of time and politics, justification enough for its inclusion here.

One ancient formulation of *chronos* comes from Plato, who conceived of *chronos* as the universal clock: 'not mere succession or duration but a standard by which duration can be measured' (Guthrie 1978: 300). Since Newton in the late seventeenth century, the predominant conception of *chronos* has been of time as an intangible cosmic backcloth against which existence plays out. Newton abstracted time and space from the sensory world of experience, presenting them as divine realities independent of the world of humans. He proposed an 'absolute space' independent of matter, which existed in a uniform and unchanging fashion throughout Creation. Just as absolute space could be distinguished from the phenomenological space of humankind and the materiality of celestial bodies, so too could time: 'Absolute, True, and Mathematical Time, of itself, and from its own nature flows equably without regard to any thing external' (Newton 1729: 9). In the Newtonian universe, nothing in the material universe could alter or otherwise perturb the 'flow of time'.

In contrast, *kairos* is ‘the time that gives value’, and ancient Greek philosophers conferred upon *kairos* the qualities of ‘exact time, critical time, season, or opportunity’ (Rämö 1999: 312). Smith identifies the essential features of *kairos* as timing, tension and opportunity (Smith 1986: 10–11). In an initial sense, *kairos* is ‘the right time’ for something to happen, so that ‘timing’ may be good or bad. It may also connote a time of tension or conflict demanding of a decision not applicable at any other time. The third meaning of *kairos* is as a time of opportunity precipitated by a problem or crisis and which allows for actions prohibited or not possible at another time. *Kairos* is the time of the *sui generis* exception, which interrupts and attempts to make subservient the ordinary time of *chronos* in the process of psychological, social and political action and transformation. Returning briefly to Heidegger’s ecstatic temporality, the foundation of the *Augenblick* is *kairos*, the ‘decisive, critical point dependent on one who has the skill and wherewithal to act’ (Ward 2008: xii). Kimberly Hutchings summarises well the fundamental difference between *chronos* as the medium for existence and action, and *kairos* as the ‘creative force’ of temporal action (Hutchings 2008: 25).

Chronos and *kairos* are not ontologically exclusive temporalities, however, and are not easily divorced. Smith contends that ‘*kairos* presupposes *chronos* which is thus a necessary condition underlying qualitative times’ (Smith 1986: 6). Similarly, Agamben observes that *kairos* must be immanent to *chronos*. *Kairos* ‘does not have another time at its disposal; in other words, what we take hold of when we seize *kairos* is not another time, but a contracted and abridged *chronos*’ (Agamben 2005: 69). Like Newtonian time – the temporal dimension of the divine sensorium (Connolly 2014) – *chronos* is the basis for the existence of *kairos*, and of all other times imaginable. *Kairos* emerges from *chronos* because of humanity’s emergence from earlier forms of life and, ultimately, from the physical (chronotic) cosmos itself. This reading of *kairos* is consistent with the model of emergent temporality previously outlined, and presents *kairos* as, in part, the time of human political action. The temporality of kairotic politics can be further disassembled through considerations of duration, tempo, acceleration and timing, which allow for finer-grained analyses of how politics operates in this temporal register (Miller 1993; Grzymala-Busse 2011).

Time is not only the cosmic vessel within which we recognise tense and measure the passing of human lives and societies. The twentieth-century discoveries of Einsteinian relativity and quantum mechanics have taught us that time is a far stranger creature than we ever thought possible. It is not an absolute ‘clock in the sky’ by which all things are measurable, a concept dismissed in 1883 as ‘idle metaphysical speculation’ by the physicist Ernst Mach (Galison 2003: 236–7). As the narrator of a Marcel Aymé 1943 short story says, it ‘became obvious that the notion of time, as our ancestors had transmitted it down the millennia, was in fact absurd claptrap’ (Aymé 2012: 109). Rather, time is a local, relative, subjective and emergent property of the physical universe that differs from one place and observer to another, even if it exists at all (see Barbour 1999). A scientific framework in which the reality behind the appearance of the universe is one of dynamic relations rather than fixed entities has replaced absolute theological and cosmic time, encountered as the ancient Greek *chronos* and in the divine sensorium of Newton. The work of Einstein and others marked the beginning of the ‘radical secularization’ of time, in which metaphysical time, philosophical time and technological time converged (Galison 2003: 42, 47). Modern science has irrevocably altered how we must view time, even as we should be cautious of attempting to impose scientific ontologies on the social world (Kincanon 2004; Jackson 2011: 26–32).

In this mode of thinking, time became pliable and negotiable and might be used to further political ends. Winston Churchill is reported as saying, ‘Time is neutral; but it can be made the ally of those who will seize it and use it to the full’ (Tsouras 2000: 479). The incarcerated Martin Luther King wrote in 1963, ‘time itself is neutral; it can be used either destructively or constructively’ (King Jr 1993: 843). Time is not the silent background across which human progress unfurls inevitably but a resource for advancing one’s earthly ambitions in all their uncertainty and contingency. It follows that the time of politics – and security – is not unitary. It is not a singular, empirically identifiable entity – ‘time’ – but a multiplicity of intersubjectively constructed temporalities within the broader matrix of sociotemporality. The following section sets out how this sociotemporal matrix facilitates a ‘politics of time’.

Towards a politics of time

The preceding discussion has attempted to show how conceptions of time emerge from the physical universe and has stressed the importance of sociotemporality as a form of social knowledge about time. This knowledge is not restricted to the experienced time of the human but extends through reason and technology to incorporate what we can know about the times of nonhuman others. The ways in which we understand time and temporality shape and are shaped by the broader chronotopic narratives of history and human enquiry and contribute to all social imaginaries. We have reached a point where we can posit the existence of multiple temporal orientations in any social context, which, in their mutual and exclusive articulations and negotiations, provide a source of political tension. With respect to security imaginaries, many different temporal cognitive biases co-exist within and across different communities and shape the narratives through which these communities understand their social existence, their role in the world, and through which their political behaviours are shaped.

At its broadest, the historian Charles Maier states, politics is inevitably about time:

> Politics comprises one of the fundamental means by which all societies resolve and carry out the decisions that order their collective life . . . politics rests upon vision as well as compulsion. It is based on shared or competing concepts of collective purpose. It envisages a desired future; it invokes a formative past. To act in the political domain is to propose a view of how society should progress through history. (Maier 1987: 151–2)

There always exists a politics of time because those who govern or desire to do so will always advance their own visions of how society should 'reproduce itself through time' (Maier 1987: 152). We may observe the primary ideological role of time in politics, in which the temporal imaginings of political actors and those who provide their intellectual sustenance are powerful ways of constructing historical identities and concepts of national destiny and right (Maier 1987; Osborne 1995; Hutchings 2008).

Johannes Fabian demonstrates how temporal narratives construct the sociopolitical Other through the anthropological 'denial of coevalness' between cultures – 'I am modern, you are not' – instantiating webs of powerfully asymmetric social relations (Fabian 2002; also, Hindess 2007). To travel to a society under this anthropological contemplation is also to travel back in time, a reversal of the relationship between space and time by which we ordinarily locate ourselves in the world (Duncan 1993). In contemporary international politics, it is common to refer to the jihadist mindset as 'medieval', for example, a clear example of an attempted temporal othering that borrows deeply from the Western anthropological gaze (Patterson 2011). The savage irony in the case of a phenomenon like the self-proclaimed caliphate of the Islamic State is that it is precisely the opportunities of late capitalist globalisation that make global jihadist movements a potent threat to the 'advanced' and 'rational' West (Euben 1999; Devji 2005). In a potent example of the 'denial of coevalness' theorised by Fabian, entire regions of the globe are denied their own histories until granted them by the actions of the West. Stephen Ellis observes of sub-Saharan Africa that even those Westerners who 'recognise the errors and brutalities of colonisation . . . regard the colonial moment as Africa's true entry into time' (Ellis 2011: 10).

The continent on which humankind has flourished longest is afforded no history of its own unless it is predicated on the Western colonial project. As if to reinforce that this admittance to global history is provisional and temporary, Africa is perceived as a political anomaly, reflecting its 'place in the Western imagination in a time-zone all of its own' (Ellis 2011: 107).

Lest this attitude be thought purely a relic of Western colonialism and Kantian cosmopolitanism projected outward from western Europe, these discourses operate even within modern Europe. Italy, in particular, is often referred to in terms of 'tradition' and 'backwardness' that contrast with its otherwise obvious status as a modern country. These are moral judgements upon a nation and society and perpetuate the myth of Italy as 'non-modern' and somehow acting according to premodern rules of social and political organisation that are 'out of time' with respect to its geopolitical neighbours (Agnew 1996; also, Todorova 2005; Prozorov 2011).

As Maier notes, there is an important second dimension to the politics of time at this level of abstraction: politics is not only about how time is constructed as the medium of history but about how it is allocated for political purposes, viewed as a 'scarce collective as well as individual resource' (Maier 1987: 153). Time is essential to political order, writes Elias Canetti also, and 'the regulation of time is the primary attribute of all government' (Canetti 1973: 397). We might illustrate this, as does Maier, with reference to the sociotemporalities informing the politics of nineteenth-century liberal modernity and twentieth-century totalitarianism, respectively. The time of liberal modernity has its roots in early modern rationalism, mechanical horology and the temporal standardisation of urban working life. Politics and history unfold in a linear, absolute time from which derives teleological notions of social 'progress'.

By the beginning of the twentieth century, science and philosophy had determined that time was not only less absolute than their Newtonian predecessors had assumed but more amenable to quantification, control and distribution. In the case of Nazi Germany and the Soviet Union, totalitarian regimes could not afford 'to let time remain a private resource or market commodity', so time was 'repoliticised – on the left by an enthusiasm for centralised planning, and on the right by fascist themes of subjecting its flow to heroic control' (Maier 1987: 161). Soviet time subordinated 'the private present to the collective [socialist] future' and claimed 'social immortality'. Nazi time was more romantic and primitive and even while planning for a thousand-year *Reich* was otherwise occupied with building mausolea and sanctifying the transformative power of death; it 'sought less to subordinate the present than to perpetuate it' and to restore the glories of an imagined past (Maier 1987: 161). ‘The only thing that matters’, said Hitler in 1933, ‘is that it is we who are the last to make history in Germany’ (Koselleck 2004: 203). Conceptions of past, present and future, of history and destiny, found divergent political expressions and helped shape the lives and deaths of these political regimes.

As something to be politically controlled and distributed, time belongs to ‘the political economy of relations between individuals, classes, and nations’ (Fabian 2002: xli). Many influential accounts present the increased commodification of time as a key driver of the successful spread of global capitalism (e.g. Jessop 2009). Nowhere is this thesis presented so strongly as in Lewis Mumford’s *Technics and Civilization* (1934), in which he wrote: ‘The clock, not the steam-engine, is the key-machine of the modern industrial age . . . a piece of power-machinery whose “product” is seconds and minutes’ (Mumford 1934: 14–15). Fractions of time form the basis of a ubiquitous economy of time in which we are all subject to the desires of political elites seeking to control our access to and our production of temporal assets, ‘to influence or constrain the balance between “free time” and work, or private life and public commitments’ (Maier 1987: 152). Economic and other practices not only unfold in time but instantiate dominant political and cultural conceptions of time: time is always embedded in practices (Glennie and Thrift 2009: 68–71). However, to follow this argument uncritically is also to engage in chronopolitics. If we adhere too rigidly to popular notions of an ever-increasing economy of time – a narrative predicated principally on speed and acceleration – we submit to a form of technological determinism ‘which unproblematically maps the apparent power of things on to subjects’ (Thrift 2008: 63). Furthermore, we might argue that speed itself is a culturally relativist creation, a ‘classical modernist trope’ that itself depends upon the construction of a ‘non-speedy’ Other (Thrift 2008: 63). This is but an alternative manifestation of the forms of chronopolitical othering theorised by Fabian and others.

Yet these narratives persist, and Chapter 3 is concerned with their relevance to the chronopolitics of cyber security. In one dystopian account of contemporary ‘time wars’, the neo-Luddite Jeremy Rifkin pits the political strategists of speed and technologised efficiency against those who would pursue life more in tune with the ancient rhythms of body and nature (Rifkin 1987). From the clash between these temporal regimes emerges a conflict intelligible through the lens of chronopolitics. Recognising the emergent nature of temporality, Rifkin proposes that the nature–culture divide in human existence stems from ‘the first great separation, that point where we began the process of expropriating our own time, claiming our independence from the great temporal symphony that orchestrates the other worlds we are fashioned from' (Rifkin 1987: 43). 'Lost in a sea of perpetual technological transition', he writes, 'modern man and woman find themselves increasingly alienated from the ecological choreography of the planet' (Rifkin 1987: 13). This account insists on the separation of nature and culture as a key facet of modernity, which differentiates it from the present enquiry. Fraser shows that our human temporality subsumes within it knowledge of pre-existing and co-existing nonhuman temporalities; there is no radical split between nature and culture except as exists epistemologically as the ultimate unknowability of unmediated reality (Fraser 1999). In related fashion, Bruno Latour argues that 'we have never been modern': the artificial distinction between culture and nature serves to obscure the innumerable intense and constitutive relations between 'cultural' humans and the 'natural' objects and phenomena populating the world in which we live (Latour 1993).

Whether we agree with Rifkin or Latour does not alter the recognition that chronopolitics is embedded within all our notions of how society operates and how it might be characterised. This applies not only to the chronotypical imaginings of political elites but to those who would resist them and to our own analyses of the conflicts that arise. In the following chapters, we turn to the case of cyber security in an attempt to discern its chronopolitical dynamics, exploring how the cyber security imaginary constructs pasts, presents and futures, what informs these perspectives and what the political implications are of these ways of interpreting and shaping reality. As a first step in this process, the next chapter examines how cyber security communities imagine the present, how cyber security understands its position in time and how cyber security relates to narratives of the speed and acceleration of the modern world.

3 Diagnosing the present

The revolutionary present

Cyber security communities are often keen to emphasise the historical importance of the times in which we live. The UK *Cyber Security Strategy* (2011), for instance, suggests that the societal changes fomented by information communication technologies (ICTs) already look likely to be 'on the scale of the very biggest shifts in human history, such as the coming of the railways, or even learning to smelt metals' (Cabinet Office 2011: 11). Deploying a similarly grand historical gesture, Michael Hayden, former director of both the Central Intelligence Agency and the National Security Agency, commented that 'this cyber thing is probably the most disruptive event in human history since the European discovery of the Western hemisphere' (Hayden 2011). Inelegant though these comparisons may be, they do indicate that governments, policymakers and senior officials view ICTs as the drivers of structural change on a par with some of the most significant political, cultural and technological transformations of the Holocene.

Cyber security is located relative to the wider transformations of an 'information age', ushered in by an ongoing 'information revolution'. In the United Kingdom, this putative revolution has been registered by government since at least the mid-1950s (e.g. HM Government 1955). In more recent times, the language of revolution was established early in the Blair administration that eventually initiated the first UK cyber security strategy: 'We are no longer on the verge of a revolution. The revolution is happening now' (Central Office of Information 1998: 3). In that strategy document, the government granted cyber security the power to ensure that society will benefit from 'the wonders of an information revolution that could transform every part of our lives' (HM Government 2009b: 7). A similar understanding is at work in the United States. 'Thirty years ago', the US *International Strategy for Cyberspace* (2011) states, 'few understood that something called the Internet would lead to a revolution in how we work and live' (White House 2011: 25). Cyber security, argues the White House elsewhere, is essential to realising the ‘full potential’ of this revolution (White House 2009: i). Yet this revolution has been characterised in policy documents on both sides of the Atlantic as a ‘quiet’ one, delivering ‘seamless connectivity’ to British citizens (HM Government 2009b: 8) and responsible for making the United States a nation ‘now fully dependent on cyberspace’ (White House 2003: 5). This dependence is as cognitive as it is technological, as societies come to rely psychologically and practically on the proper functioning of computer networks like the internet.

Like all revolutions, the information revolution is not a singular point in time, even as the search for originary events, actors and technologies will always be an absorbing academic game. A revolution is a process that unfolds *over* time – it has duration – but it also marks the beginning of a new time. It serves as the convenient demarcation of one period of human history from another, even if crude periodisation has been recognised as a problematic abstraction from historical reality since at least the end of the eighteenth century (Koselleck 2004: 244–5). The development of metallurgy invoked by the UK government refers to the period labelled by antiquarians as the Bronze Age, sandwiched between an earlier Stone Age devoid of worked metals and a later Iron Age characterised by ferrous metalworking. Developed by antiquarians in the nineteenth century to provide a reliable absolute chronology of prehistory based on the archaeological recovery of material remains, the ‘three-age system’ has lost much of its explanatory power in the face of archaeological science and the erosion of teleological post-Enlightenment narratives of linear social evolution and improvement (Lucas 2005: 50–1). The evidence of artefacts and stratigraphy shows that this conceptual framework relies on constructing false boundaries between contiguous times and places. Nevertheless, this ‘epochalism’ persists and has ‘taken on a reality of its own’, with those who sustain it ‘apparently forgetting that what we call things influences how we think about them’ (Connah 2010: 63). In this case, periodisation imposes a particular form of order on the past and serves to perpetuate sanitised narratives of progress in which a primitive past leads to our civilised present.

This reminds us that the periodisation of the information age is a social construction. Michel Foucault notes that it is perhaps more accurate to speak of periodisation as expressive of an ‘attitude’ or ‘ethos’, understood as ‘a mode of relating to contemporary reality’ rather than the circumscription of a specific historical time (Foucault 1984: 39). Even recognising this, we still run the risk, writes Daniel Pick, of ‘singularising what was always plural’ (Pick 1993: 203). This is not to assert that the information revolution is an illusion, as some have argued, but it does recognise that the importance and effects of the material foundations (principally, information technologies) upon which the concept relies are defined socially through a 'matrix of particular political, economic and ideological practices' (Brants 1989: 90–1). More radically still, 'the hegemonic conception of the information revolution is an awesome phenomenon with real meaning and consequence in and for our lives' (Slack 1984: 250). The information revolution is a discursive construction, a system of knowledge, ideas and practices that shapes and constrains what is possible, sometimes even to the exclusion of dissenting and contradictory narratives: 'Everything is made to fit, to conform' (Slack 1984: 253; also, de Mul 1999).

Myriam Dunn Cavelty notes that one of the principal outcomes of this problematic periodisation in cyber security is to see all manifestations of this 'revolution' as new and therefore 'radically different' from all that preceded it (Dunn Cavelty 2008: 16). Frank Webster pinpoints a distinction between those who proclaim the 'newness' of contemporary society, in which the internet and other information technologies have fundamentally constitutive roles, and those who argue that the 'form and function' of information and the technologies that support it are 'subordinate to long-established principles and practices' (Webster 2006: 7). This is a key consideration in any discussion of cyber security and the social present. In historical perspective, it would seem that 'continuity exceeds discontinuity' (Golding 2000: 166), and it is probably therefore more accurate to describe contemporary transitions as evidence of evolution rather than revolution (Dunn Cavelty 2008: 15). That said, it is at least plausible that some aspects of the 'information revolution' do present marked differences from earlier times (Harknett 2011). The simple existence of networked digital computers is a necessary historical condition for the emergence of cyber warfare, for example. By contrast, we do not yet know if it is a sufficient condition for the development of new military strategy.

Most government cyber security discourses do not present such qualified opinion and unequivocally align with a perspective that stresses the novelty of the revolutionary present. Notwithstanding the previous identification of documents to the contrary, the UK government's first attempt to develop a holistic perspective on the 'new landscape' of information technologies and society noted, for example, that '[w]hat is so potent about the communications revolution is the way it combines the old and the new' (HM Government 2000: 7). This subtlety may now be lost and 'newness' permeates descriptions of 'cyberspace' and the contemporary world, as a dialectic between 'new threats' and 'new opportunities', in the recognition of 'new challenges', and in the desire for new ideas, structures and procedures. The latter category is central to all policy – were new things not desired or required, there would be little point in drafting policy in the first place – but in the characterisation of the ‘newness’ of the environment a distinct temporality is marked out. The social present is adrift of its temporal moorings: there is no substantive narrative of ‘before’ against which to assess the ‘new’ and the ‘now’, and the present can only operate in relation to the future.

It is the ‘great paradox of our age’, wrote the philosopher and anthropologist Ernest Gellner, ‘that although it is undergoing social and intellectual change of totally unprecedented speed and depth, its thought has become, in the main, unhistorical or antihistorical’ (Gellner 1988: 12). This tendency surfaces in the thin appeals of cyber security to historical periodisation, which articulate difference and distance rather than any sincere attempt to historicise the present. In the context of postulated revolutionary change, it can be difficult to remember that older temporal structures are not immediately replaced by the new; the material and mental conditions of existing temporalities can persist long in the presence of new ones. A similar claim may be made of technology itself, which can endure in the face of changes and exert ‘ongoing and technical influence simply because it is “there” and because people have come to depend on its being there’ (Staudenmeier 1985: 156).

The social present is a richly textured aggregate of competing and complementary temporalities, but it is also a stratified temporal assemblage (Attali 1982: 247–8). This is not a palimpsest, in which the traces of earlier temporality are erased to make way for the new, but a situation in which new temporalities can emerge alongside the old, even if they are not thoroughly understood until after they too are overshadowed. We can recognise this in the framework of emergent temporality described in Chapter 2, which proposes that sociotemporality incorporates knowledge about lower-order temporalities identifiable with nonhuman assemblages of matter and energy. Sociotemporality is assembled from pre-existing components of social and material reality. The chronotypes we use to explain and describe the world and which form the basis of political expressions of temporality show sedimented traces of the past as well as the present and the future.

Most historicisation of the relations between information technologies and security is relegated to boilerplate introductions to hundreds of articles and books, press reports, policy documents and expert analyses. In one sense, we should be grateful: extended historical prefaces to each contribution to cyber security debates would try the patience of even the most ardent supporter of contextual throat-clearing. In another sense, too, we would not expect authors of a technical or policy persuasion necessarily to indulge in historical exegeses ahead of their often fine-grained analyses of contemporary issues and problems.[1] A notable exception is provided by an extensive appendix to the US *Cyberspace Policy Review* (2009), which traces the evolution of US legal and regulatory frameworks in response to changes in information technologies since the nineteenth century. This contribution recognised that 'History Informs our Future' (White House 2009: appendix C). This bucks a dominant trend, in that it recognises the value of history in planning and policy, a perspective articulated by Gellner: 'we look at those roots in order to understand our options, not so as to prejudge our choices' (Gellner 1988: 12; see also, Dutil 2014; Stevenson 2014).

The delineation of an information age is an exercise in periodisation and an expression of sociotemporality: it is a temporal structure imagined, negotiated and sustained throughout the social body and across multiple communities. In cyber security, its characterisation may vary in the details, but in its essential revolutionary and transformative disposition, its presentation is remarkably consistent. The decoupling of the present from the past is not only a cultural phenomenon but also a political move that facilitates the construction of the present situation as exceptional and necessitating political action. The justifications for cyber security lie in the claims made for the *sui generis* present, a dehistoricised information age. It is insufficient to note that this socially negotiated construction of the present has important political implications without examining further aspects of the sociotemporal chronotype that sustains it. What are the key temporal characteristics of this period that distinguish it from any other and contribute to the sociotemporality of cyber security discourse? What forms of presentness-as-temporality are implicated in and constitutive of the politics of cyber security? How are temporal differences identified and established, and how do they facilitate and necessitate political interventions? Finally, what can we say about the imagining of the cyber security present in terms of the politics of time?

James Der Derian observes that when 'a revolution stops auguring change and begins signifying an age, it usually means that a regime has been stabilized, a cultural shift codified, predictability restored' (Der Derian 2009a: 250). 'Not so with the Information Age', he argues, of which the only constant is 'fast, repetitious, and highly reproducible change: a kind of hyper-speed' (Der Derian 2009a: 251). The present is therefore one of high speed and accelerating rates of change. Speed and acceleration are not measures of time but qualities of temporality of

[1] In the author's experience, technical professionals are often very aware of the heritage of their fields but allow this knowledge to inform their work rather than become its central feature. This may account for the frequency of historical case studies in works on information security but the dearth of histories of information security itself (but see de Leeuw and Bergstra 2007).

crucial importance to framing both the need for cyber security and the political and technical responses deemed necessary and appropriate. This chapter shows how the subjective experience of relative speed, in the forms of acceleration and deceleration, emerges from the conflict between the temporalities of machines, networks, people and institutions. Each has temporal presents that combine and conflict with others in the sociotemporality through which the cyber security present is imagined and constructed. The first section situates the concepts of speed and acceleration historically not only as an intersubjective experience common to all cultures but also as a key aspect of the politics of modernity and postmodernity. Two subsequent sections examine multiple aspects of sociotechnical speed, which I term 'netspeed', considered through the prisms of acceleration and deceleration. The practical and political effects of acceleration are perhaps rather more obvious than the decelerative 'lag' that characterises the politics of cyber security, but as these sections and the conclusion to this chapter demonstrate, both are important constituents of how the present is imagined in cyber security and what politics emerges from this sociotemporal imaginary.

Speed and acceleration

In 1964, Marshall McLuhan introduced to the world his famous aphorism that 'the medium is the message', meaning that the technology of communication is as important in shaping social affairs as the information content carried by that medium. Furthermore, the 'message' of any medium of technology is 'the scale or pace or patterns that it introduces into human affairs' (McLuhan 2006: 108). The railway, for example, did not introduce speed or transport into society, but it did accelerate the scale and scope of extant activities, and it created 'totally new kinds of cities and new kinds of work and leisure' (McLuhan 2006: 108). The railway irrevocably altered the way we perceive time and space, giving rise to new spatial and temporal configurations, new pathologies and the first distinct phenomenology of technology and speed (Schivelbusch 1986; Stephens 1989). In future decades, the airplane would accelerate the rate of transportation still further, and 'dissolve the railway form of city, politics, and association, quite independently of what the airplane is used for' (McLuhan 2006: 108). Air travel abolished movement in the terrestrial plane entirely, allowing passengers to travel the world in a day, and gave rise to new spaces like airports, which, in their existence as entry points to the global vector of speed, are just as quickly forgotten as encountered. These 'non-places', in Marc Augé's influential and evocative phrase, are 'indissociable from a more or less clear perception of

https://doi.org/10.1017/CBO9781316271636.004

the acceleration of history and the contraction of the planet' (Augé 1995: 119).

In our lifetimes, the non-places of speed have been augmented further by the emergence of a new 'cyberspace', enabled by computer networks across which communications travel at significant fractions of the speed of light. Collapsing traditional notions of space and distance, cyberspace is the contemporary apotheosis of the successive 'waves' of intensifying 'time-space compression' in capitalist modernity and postmodernity (Harvey 1990). Interestingly, the linguistic progenitor of the word 'cyberspace', the science fiction writer William Gibson, described his creation as a 'consensual hallucination' in the 'nonspace of the mind' (Gibson 1984: 67). The dimensionality of space and the locationality of place are not equivalent (Agnew 2011), but both 'non-place' and 'nonspace' suggest entities whose absence of specificity is defined only with reference to the diffused network flows and technological arrays of computerised globalisation.

Since public access to the internet was granted in the mid-1980s, 'cyberspace' and the global infrastructures that enable it have been central in 'reconfiguring space and time relationships in ways that promised to change our lives forever' (Mitchell 1995: 3). The idea of 'cyberspace' has been adopted enthusiastically by politicians, government agencies and businesses, irrespective of the validity or otherwise of its conceptualisation as a new realm of human activity, or whether it can be so easily demarcated from existing notions of sociotechnical space and experience (Rogers 2010). The term has limited social-scientific analytical utility, but it refuses to go away. Julie Cohen argues that the metaphor of cyberspace is neither a disposable literary motif nor an ontological claim on unchanging reality but a function of a deep human 'commitment to spatiality [that] runs far deeper than mere politics or intellectual fashion' (Cohen 2007: 234). The territorial basis of politics encourages the retention of the term. Politicians understandably feel more comfortable constructing 'cyberspace' as a space analogous to land or sea than any of the more ethereal or metaphysical readings of the 'virtual' (Heim 1993; Wertheim 1999). At the same time, cyberspace is constructed as a space apart from 'real life', an instantiation of 'digital dualism' that preserves a false dichotomy between 'the virtual' and 'the actual' (Boellstorff 2008: 18–21).

In cyber security – another term imparting a hard-edged technicity to discussions of society and ICTs – cyberspace is usually presented in terms of opportunity through connectivity, prioritising the economic benefits of the continuing growth of the internet and the Web. Of the United Kingdom, Frank Webster notes that since the mid-1970s government has asserted that 'the most effective way to encourage the "information revolution" is to make it into a business' (Webster 2006: 142). This is a central tenet of British cyber security policy today, which sees cyber security as a way of deriving 'huge economic and social value from a vibrant, resilient and secure cyberspace' (Cabinet Office 2011: 21). The *Cyber Security Strategy* (2011) makes economic comparison with the Industrial Revolution, a common rhetorical device in texts extolling the virtues of the information revolution (Brants 1989: 91). Specifically, it compares growth in gross domestic product (GDP) and suggests that the rate of change in GDP is three times faster in the information revolution than in its earlier industrial counterpart. Crude though this measure is, it is one example of how speed and acceleration are identified as key characteristics of the contemporary world in which ICTs are crucial to social and economic advancement. Diverse theorists argue that we are confronted with and complicit in a new temporality born of the speed of the computer networks on which society increasingly depends and of the acceleration of the rate of technological change (Hassan and Purser 2007; Hassan 2009; Rosa and Scheuerman 2009; Glezos 2012).

What are 'speed' and 'acceleration'? Speed is a form of temporality, but it is not a form of time. In strict physical terms, speed is a quantity derived from measurements of both time and space. The speed of an object is obtained by determining what spatial distance it travels in a given temporal duration, the quantity calculated giving the average speed of the object over that period. Speed is an empirical measure of continuous (if not necessarily uniform) change through space or an indicator of the distance between discrete events, whether these are social phenomena or the acts of measuring duration itself. Speed can be thought of in terms of 'tempo', that is, as the 'frequency of the "subevents" in a larger event, or between events in a process' (Grzymala-Busse 2011: 1282). Speed can only be experienced subjectively if there are discrete events whose frequency we can sense, if not necessarily measure. It follows that the subjectivity of speed is relative, even if we develop ways to objectify the frequency of events over a given duration. Acceleration, too – the increase in or 'speeding-up' of the frequency of events – and its less commonly invoked antonym, deceleration, are subjective aspects of individual and collective temporalities that depend upon the experience of changes in speed between identifiable events and entities as much as any empirical calculation of the same.

Speed and acceleration have always been problematic aspects of sociotemporality and its relations with technology. Jose Harris records that towards the end of the nineteenth century in Britain – the transformations of the Industrial Revolution by now firmly institutionalised – the 'subjective time span of modernity' became foreshortened: by the 1870s, 'modernity' referred to '*the way we live now* … rather than the longer sweep of post-classical European civilisation' (Harris 1993: 32, emphasis added). The proximate reasons for this are not hard to identify. In historical perspective, we might see phenomena like improved medicine, street lighting and public sanitation as continuations of extant processes, but for people living at the time they seemed 'like a quantum leap into a new era of human existence' (Harris 1993: 33). They marked a divergence of the artificial rhythms of urban life from the more sedate tempos of the natural world. The popular culture of *fin-de-siècle* Europe expressed this disjuncture between 'old' and 'new' temporalities, the latter characterised by 'new technologies of speed, precision, and mastery' over time and nature (Kern 1983: 117–24). Later authors have lamented this driving of 'a permanent wedge between the rhythms of culture and the rhythms of nature' (Rifkin 1987: 47), but this rupture was glorified by some at the time, including the founders of Italian Futurism, probably the first authentic European avant-garde. Marinetti wrote in 1909:

> We stand on the last promontory of the centuries! … Why should we look back, when what we want is to break down the mysterious doors of the Impossible? Time and Space died yesterday. We already live in the absolute, because we have created eternal, omnipresent speed. (Marinetti 1973: 21–2)

In its fascistic muscularity, misogyny and paeans to the glories of 'hygienic' war, Futurism is still just potent enough to energise the contemporary mind (Buelens *et al.* 2012). It is unlikely we would concede as much to the speedy temporalities ascribed to the gas lamp and civic sanitation, which once amazed the urban populace. We should, however, acknowledge the roots of our own preoccupation with the historical pace of change in nineteenth-century industrialisation and mass commercialisation, not least in its pessimistic register (Vieira 2011). It may be that we are no better positioned to objectify our co-constitutive relations with speed than were the Victorians and Edwardians, of whom Harris cautions that we should be wary of taking their modernity 'too much at its own evaluation' (Harris 1993: 34). The philosopher Robert D'Amico asserts that 'human understanding is always a "captive" of its historical situation' (D'Amico 1989: x, quoted in Deibert 1999: 81). Therefore, we should be circumspect in validating our own perceptions of the speed of contemporary life, particularly as those things that were once impossibly fast are now transformed into the epitome of 'slow', a 'dialectic of experience' that inevitably foregrounds the subjectivity of speed (Kern 1983: 129).[2] Speed has

[2] It is symptomatic of this dialectic that a Wikipedia search for 'Slow' redirects to 'Speed', http://en.wikipedia.org.

always been a feature of the natural and social worlds, and the ‘past is packed with just as much speed and ephemera as the present’ (Newitz and Glezos 2010). It did not come into being in the industrial period, preceded by some premodern past wholly in tune with the languid rhythms of deep ecology, nor is it a novel property of a recently ‘wired’ world alone. As Jacques Derrida notes, ‘[a]t the beginning there will have been speed’ (Derrida 1984: 20).

In his study of nationalism and the collapse of the Soviet Union, Marc Beissinger introduces the concept of ‘thickened history’ to describe those periods in which ‘the pace of challenging events quickens to the point that it becomes practically impossible to comprehend them and they come to constitute an increasingly significant part of their own causal structure’ (Beissinger 2002: 27). In Beissinger’s reading of thickened history, it becomes increasingly difficult to exercise an objective historical sensitivity with respect to events unfolding around us. This reminds us that living ‘inside’ history is a problematic epistemological issue, although this need not be an obstacle to enquiry so much as a restraint on inappropriate generalisation or unwarranted prediction. We are hampered by a human inability to process sufficient information about events that we can identify and understand their social and political dynamics. Our subjective experience is principally one of great speed, with multiple events occurring rapidly in sequence ‘within an extremely compressed period of time’ (Beissinger 2002: 27). We could read the current information-technological ‘revolution’ in these terms, as the speed of computer networks seems to drive an ever-faster pace of life and politics. This perceived increase in the frequency of events can lead to disorientation and an inability to interpret this acceleration in historical perspective (Beniger 1986: 1–6). As David Harvey notes, ‘time-space compression always exacts its toll on our capacity to grapple with the realities unfolding around us’ (Harvey 1990: 306).

Cyber security actors identify speed and acceleration not only as fundamental aspects of the present but also as key drivers of uncertainty and insecurity. They are important facets of the sociotemporality informing the politics and practices of cyber security, but they are not the only ones. The following discussion examines two distinct but complementary dimensions of the cyber security present. The temporalities of people, social groups, machines and networks are components of what we might call ‘netspeed’. This term references the internet (the ’Net) and has a secondary connotation as an aggregate value or assemblage of values, in this case of speeds. The first section discusses speed and acceleration as closely related but distinct aspects of netspeed. The second section considers deceleration in this light and its importance to the politics of cyber security.

Netspeed I: acceleration

Cyber security actors are explicit about the speed and acceleration of events relevant to cyber security practice and policy. A brief survey of government cyber security statements produces many examples that look banal but reveal how deeply these aspects of temporality are engrained in the chronotypes articulated by cyber security communities. The threats posed by computer networks are framed as threats happening at the speed of those networks, so that '[e]vents in cyberspace can happen at great speed' (Cabinet Office 2011: 7). Former US Deputy Secretary of Defense William Lynn said, 'we're seeing assaults come at an astonishing speed – not hours, minutes or even seconds – but in milliseconds at network speed' (Garamone 2009). 'Attacks cross borders at light speed', the White House (2009: 49) notes. Malware can infect hundreds of thousands of computers worldwide in a matter of hours, and large organisations like the US Department of Defense regularly report 'probes' and 'cyber attacks' on their networks numbering millions per day (e.g. Panetta 2012).

An accelerated frequency of events is diagnosed for ICTs and the contemporary world in general and is expressed in the language of technological change. The UK government observes that the 'technology that underpins [cyberspace] continues to develop at a rapid pace' (HM Government 2009b: 3). Not only is the pace of change rapid, but it 'will not let up'; it is 'relentless' (Cabinet Office 2011: 13, 29). We may assume that various inflections of the adjective 'relentless' are intended, in its evocation of inexorability and of its sternness or lack of mercy, in the face of which '[w]e cannot afford to be complacent' about the pace of technological change (HM Government 2009a: 48). Not only is the pace of change fast, but '[w]e expect the rapid development and exploitation of computers and electronic communication technologies to continue to accelerate' (Home Office 2010: 5).

In addition to the ultra-fast temporalities of computers, cyber security texts repeatedly stress the subordinate position of humans in computer networks. One policy article states that it is now 'a truism that most humans cannot keep up with the speed of technological development across cyber space' (Glenny and Kavanagh 2012: 287). 'Human intelligence, unlike cyber, does not move at velocities approaching the speed of light', write two prominent advocates of increased US government intervention in cyber security (Clarke and Knake 2010: 215). From the computer science perspective, the technical case is that information exchange between humans is far too slow to adapt to rapidly evolving cyber threats. In times of crisis, information exchange may be further impeded by cultural, linguistic, legal and organisational obstacles. For these reasons, humans are barriers to network efficiency and are therefore inimical to the aims of cyber security, that is, protection from a range of cyber threats. The implication is that slow humans should be removed from time-critical cyber security decision-making and action and these activities delegated to a range of automated software agents. Humans function only as supervisors of network security, with software agents – 'sergeants' and 'sentinels' – performing the bulk of work within parameters set by their supervisors (Fink *et al.* 2014).

Over the last twenty years, there has been a shift towards the automation of response systems and in many cases the gradual removal of people from cyber security decision loops (Stakhanova *et al.* 2007; Shameli-Sendi *et al.* 2012). The deliberate, rather than incidental, excision of human inputs and decision-making is particularly notable in the array of technologies marketed as 'active defence' solutions to cyber security problems. These systems have been suggested since at least the mid-1990s, when they were presented as analogous to the human immune system (Hundley and Anderson 1995: 25), a metaphor that has experienced a recent and influential resurgence (Betz and Stevens 2013).

Active defence systems – described as '[p]art sensor, part sentry, part sharpshooter' (Lynn 2010: 103) – aim to devolve decision-making to software which can detect, block and seek out the sources of malicious attacks far more quickly than could human operators (Kesan and Hayes 2010; Colbaugh and Glass 2012). In 2012, the US Defense Advanced Research Projects Agency (DARPA) proposed a new research program, 'Plan X', part of which would 'develop systems that could give commanders the ability to carry out speed-of-light attacks and counterattacks using preplanned scenarios that do not involve human operators manually typing in code – a process considered much too slow' (Nakashima 2012). In 2014, Edward Snowden, the fugitive leaker of US state secrets, provided limited details of a National Security Agency program called MonsterMind, 'a cyber defense system that would instantly and autonomously neutralize foreign cyberattacks against the US, and could be used to launch retaliatory strikes as well' (Zetter 2014). Further details are scant – MonsterMind may even be Plan X, according to journalists – but the US defence community is openly investing in automated systems that entrust tactical decision-making to software rather than the 'wetware' of the human mind (see also, Chang 2014).

These systems begin to bring the ‘cyber’ component of cyber security more in line with its etymological roots in Greek *kybernētēs* (‘steersman’), the origin of both ‘government’ and ‘cybernetics’, with their obvious connotations of the control of social as well as technical systems. The control aspect of cybernetics ‘haunts’ discourses on new media technologies (Andrejevic 2007: 18), and a similar observation might be made of its rarely acknowledged presence in cyber security discourses (but see Dunn Cavelty 2008: 16–17). It is perhaps no coincidence that post-World War II cyberneticians saw themselves at the beginning of a new informational era in which creative and destructive powers borne of technoscientific human knowledge could be brought under control: cybernetics could ‘deal simultaneously with the dark politics and bright theology of a the new age’ (Bowker 1993: 113; also, Edwards 1996). Complementary views were held on the other side of the Iron Curtain but were not translated as effectively or comprehensively into policy as they were in the United States and its allies (Gerovitch 2008).

In the scenarios informing the development of automated cyber defence systems, we see a fundamental discrepancy between, on the one hand, the speeds of computer networks and their effects and, on the other, the ability of humans to detect and understand those dynamics. Technical proposals to remove humans from those decision-making frameworks mean that threats and network problems are dealt with automatically by software that does not depend on the relatively slow reaction times and thought processes of human operators. It takes one-tenth of a second for a human to respond to an external stimulus (Canales 2009), far slower than any process relevant to technical aspects of computing. Systems will be implemented that act at the speed of the networks and the machines that comprise them; humans have no operational utility in these environments. Even serious proposals for slowing network traffic in order to restore tactical advantage to network defenders leave little scope for human decision-making (Guernsey *et al.* 2012).

The speeds of computer networks, the frequency of events and the tactical requirement of rapid response times all occur in a temporality that is not human. In a world of global optical fibre networks, consisting of bundled glass ‘light pipes’ that transmit photons from one end to the other, information is transmitted across long distances at the local speed of light. This light travels in glass rather than a vacuum, so it cannot attain the absolute speed of light (*c*) but travels instead at sub-light speed depending on the qualities of the glass fibre in question, typically around two-thirds the speed of light. Information is transmitted in a world of primitive atemporality, to which we have access through technology but no direct experience or intuition. A similar situation pertains to the electronic circuits in computers and the cables that connect them. Contrary to received wisdom, electrons do not travel at the speed of light in electronic circuits. In alternating current (AC) arrays they only vibrate within the molecular matrix of the conducting material, one reason why AC is more efficient and more common than DC (direct current), in which electrons do move, if at very low speeds. The speed of propagation of electromagnetic waves, however, which carry the informational content of communications, varies between two-thirds and 95%-plus of the absolute speed of light, depending upon the physical characteristics of the conducting material. Again, the temporality of these processes is not directly sensible to humans' biotemporal senses or their higher-level cognitive appreciation of time. This is the 'time that cannot be lived as such because its rhythms fall beneath the threshold of consciousness perception' (Mackenzie 2002: 88).

When the UK government states enthusiastically that information can be exchanged across global networks 'in timescales that were previously unimaginable' (HM Government 2009a: 190), it would be more correct to state that these timescales will never be imaginable in any coherent sense to the unaided human mind. That the fastest supercomputer currently in existence – the Tianhe-2 at the National University of Defence Technology, China – has recorded a standard operating performance of 33.86 petaflops, or nearly 34 quadrillion (10^{15}) 'floating-point operations per second' (Reuters 2014), is natively incomprehensible. Similarly, the many online applications available for testing domestic broadband speeds return results that mean almost nothing to most people. The aim of the UK government's Broadband Delivery UK unit is to 'provide universal access to standard broadband with a speed of at least 2Mbps' (Department for Culture, Media and Sport 2013). What this means is hard to intuit without technical knowledge, except that government policy aims to deliver 'the best superfast broadband network in Europe', a condition deemed 'fundamental to our future prosperity' (HM Government 2010b: 7). The national ambition 'should be for a broadband system that is the engine of the nation's mind' (HM Government 2009a: 47). This is information-technological speed as normativity and as hard-wired public good: that absolute speeds mean little to the citizen-consumer is less relevant than the desire for relative speed in the form of faster consumer products connected to a faster internet. Speed sells, politically and commercially.

Speed is commoditised and fought over in the marketplace, but it is also contested at the national level. The current drive to high-performance computing (HPC) is a competition between the owners and operators of individual machines located at research establishments in the world's major economies, a contest with its origins in Cold War military technoscience (MacKenzie 1996). Industry requirements have often prioritised qualities other than speed, like reliability and usability (Elzen and MacKenzie 1994), but speed makes the headlines, even in the mainstream press. The supercomputers that have held the number one spot on the 'TOP500' list since 2009 are monolithic creations that achieve undoubtedly staggering feats of computational speed and volume.[3] HPC speeds are phenomenal and serve the needs of 'big data' and 'big science', for which more speed equals the greater computing power necessary for processing untold billions of data points. The names of these machines – Jaguar, K, Sequoia, Titan and the aforementioned Tianhe-2 – have some of the sober resonance of their Cold War origins and they also act as technical proxies of national power and prestige. They are contemporary iterations of national contests for speed and supremacy, whose lineage includes the contests between Britain and its maritime rivals to achieve ever-faster crossings of the North Atlantic sea routes in the late nineteenth and early twentieth centuries (Kern 1983: 109–10).

Tellingly, given its historical analogues, this supercomputer rivalry is not infrequently reported as a contemporary 'arms race' (Markoff 2005). The White House has dismissed talk of an HPC 'arms race' as a distraction (President's Council of Advisors on Science and Technology 2010: 67), but President Obama has spoken of these issues in similar language. In general technological terms, said the president, '[in] the race for the future, America is in danger of falling behind' (Obama 2010). He has made repeated reference to a new American 'Sputnik moment', calling for more investment in science and education, a key pillar of which is the further development of HPC. Following the launch of Sputnik, the rhetoric of Soviet victory and American defeat was central to American narratives of the early 'space race', and a symptom of the zero-sum mentality that characterised the superpower relationship (Lule 1991). Recent presidential addresses have been less polarised, but as in the Cold War these views are expressed with reference to an eastern Other, in this case China. The president is not alone and a proposed American Super Computing Leadership Act requiring the US government to invest formally in HPC was framed by its bipartisan sponsors as a direct response to Chinese advances in this field (Thibodeau 2013). Practical steps towards this goal reached the stage of awarding contracts in late 2014 to US defence contractors to begin researching a new generation of HPC. The US intelligence community leads this Cryogenic Computing

[3] Top500 Supercomputer Sites, www.top500.org/.

Complexity (C3) program and aims to develop HPC machines about forty times faster than current supercomputers (McCaney 2014). The air of existential dread that pertained during the decades of nuclear standoff is so far generally absent from this debate, but HPC is considered an emerging national security concern elsewhere too (e.g. Ministry of Defence 2010: 140).

British Prime Minister David Cameron's formulation of the 'global race', launched at the Conservative Party conference in 2012, is rather starker:

> Britain may not be in the future what it has been in the past. Because the truth is this. We are in a global race today. And that means an hour of reckoning for countries like ours. Sink or swim. Do or decline. (Cameron 2012a)[4]

Speaking to business executives, Cameron said they needed government to be 'tough' and 'radical' but 'there's something else you desperately need from us, and that's speed, because in this global race you are quick or you're dead' (Cameron 2012b). The prime minister makes plain the existential implications of not embracing the speed of global commerce, ironically exemplified by many of the same post-colonial and post-Soviet countries often referred to in the racialised subtexts of Western political discourse as 'backward' and to which new trade envoys are to be dispatched immediately (BBC News 2012a; HM Government 2013: 5).

The philosopher John Gray, generally regarded as on the left of the political spectrum, has been scathing of the British political class in general and of David Cameron by name. The prime minister 'seems resistant to the notion that history has anything to teach, and looks for guidance to writers who extol the wisdom of crowds, explain the momentous importance of tipping points or pass on the revelation that humans are social animals – the fleeting nostrums of the airport bookstore' (Gray 2013). In this intellectual shot across the bows of political superficiality, Gray identifies two chronotypical characteristics of contemporary British right-wing politics. The first is a shallow appreciation of temporality, represented by an insufficient respect for or grasp of the contingencies of history, although this charge can hardly be levelled at the right wing alone. The second is a rather more intriguing suggestion: that the prime minister – here standing metonymically as the figurehead of the British political establishment – is, as demonstrated by Gray's unintentional nod

[4] In 1982, the Conservative government launched Information Technology Year 1982 (IT'82), adopting similar slogans: 'Has the revolution started without you?'; 'The one thing that is absolutely certain is that if we don't adopt IT, our competitors will. They are already doing so'; 'Without IT, Britain will decline – very fast'; 'There's no future without IT' (Webster and Robins 1986: 15).

to the commercial non-places of global air travel (Augé 1995), somehow enraptured by the global vector of speed. Surely, this is not an attitude expected of a *conservative* politician?

Sociologist Hartmut Rosa provides some clues as to what might be happening here, with respect to speed, acceleration and the political left and right. Catalysed by the French Revolution at the end of the eighteenth century, partisan politics identified with particular perspectives on the issue of social acceleration and deceleration. The progressive left favoured the acceleration of history, whereas the conservative right struggled to preserve the virtues of the past by slowing down the pace of change (Rosa 2005: 450). Two centuries later, this dichotomy has been eroded, perhaps even reversed, with the 'progressive' left espousing localism, environmentalism and other decelerative politics, and the 'conservative' right pressing for acceleration in the pursuit of technology, market liberalisation and rapid political decision-making (Rosa 2005: 453).

Rosa further proposes that speed has become the centre of an 'ideological battle' between left and right, which is almost the reverse of the one fought in revolutionary France two hundred years previously (Rosa 2005: 453). This might describe accurately a range of political disputes, but with respect to cyber security this 'ideological battle' is largely absent. A conflict between the nominal left and right over the fundamental politics of cyber security simply does not seem to exist. The message from both left and right is that cyber security is needed and it is needed now. One reason why this pertains may be because the sociotemporality of cyber security is shared across the traditional partisan divide: left and right are both in ecstatic thrall to speed and acceleration as much as they are terrified by the changes they bring (see Hoofd 2012). That conservative politicians are convinced by the need to embrace speed is symptomatic of the seductiveness of speed. One answer to speed – which in its identification with rapid social change has been a traditional enemy of conservatism – is not to resist it but to allow oneself to be enfolded by it. We can detest its capacity for social change while simultaneously genuflecting before its ecstatic potency. After all, writes the novelist Milan Kundera, speed is 'the form of ecstasy the technical revolution has bestowed on man' (Kundera 1997: 2). So ubiquitous is the narrative of speed and acceleration in cyber security discourses that it has ceased to be remarkable to those who think and speak it. It has become reified as ontology, rather than remaining open for epistemological or political disputation.

This is only one aspect of the sociotemporality of relative speed. Acceleration is threaded throughout cyber security policy and practice yet its counterpart – deceleration – is almost never mentioned, even though it is arguably one of the most important chronopolitical aspects of cyber security. Implicitly, deceleration is at the core of the politics of cyber security, as discussions of the present state of cyber security are dominated by an impression of being 'left behind', both by ICT environments and by adversaries with the offensive march on governments and their agents. The following section examines deceleration as an aspect of netspeed complementary to the acceleration discussed so far.

Netspeed II: deceleration

The encouragement to 'slow down' is at the heart of much historical and contemporary social activism (Parkins 2004) and is an invitation to adopt the temporality of another time or entity. Manuel Castells speaks of 'glacial time' as an organising logic of eco-activism, an allusion to 'the slow motion of time in which nature and the planet and the species live' but which is also 'the idea that we, to some extent, as a collectivity, may be eternal' (Castells 2000: 118; also, Urry 1994). Politically, therefore, deceleration is actively promoted as a necessary resistance and theoretical counterbalance to the speed and acceleration of twenty-first-century life (Gane 2006; Saward 2011).

This is not the attempted substitution of one time for another but the absorption of an earlier, less complex temporality into our higher-level sociotemporality, a process through which cultural and psychological time horizons might be expanded. An opposing dynamic is apparently at work in cyber security, given the preceding discussion about speed, acceleration and the politics of cyber security. However, like those who might embrace 'slowness' or experiment with different ways of decelerating life and lifestyle, the sociotemporality of cyber security has incorporated deceleration in quite radical fashion as a key driver of the politics of security. Deceleration is never mentioned explicitly, but it is central to cyber security politics.

As suggested, the form of deceleration under consideration is a relative rather than absolute deceleration. Establishing measurable indices of the rate of technological or social change (Rosa 2009) is less important for present purposes than establishing the subjective impression of deceleration relative to an accelerating Other moving in the same general direction. In this situation, the absolute speeds of two entities moving relative to one another matter less than the simple fact that they are moving apart from one another at an increasing rate. More accurately still, it is the perception that they are moving ever farther apart that is significant. We need not be discussing single entities either: our greater concern is in the relative motion of sociotechnical assemblages, so that at least one experiences this relative movement as deceleration. Specifically, the following discussion proposes that deceleration is experienced intersubjectively and collectively as a deceleration of political time in the face of rapid sociotechnical change. Cyber security stresses this decelerative aspect of speed *qua* temporality, although it does so in different terms. This is a critical aspect of the chronopolitics of cyber security's social present, explored here through the concept of 'lag'.

In 1968, Samuel Huntington noted that the 'primary problem of politics is the lag in the development of political institutions behind social and economic change' (Huntington 1968: 5). These changes serve to erode the authority of political institutions, argued Huntington, and cause increased disorder in political systems. As already suggested, this identification of 'lag' would resonate greatly with cyber security communities concerned about the political and institutional effects of the acceleration of sociotechnical change. In macroeconomics, the concept of 'lag' refers to time delays between the identification of economic problems and the effects of economic solutions (e.g. Friedman 1961). The 'inside lag' is the length of time between a problem arising and the implementation of policy to address it. The inside lag is further subdivided into a 'recognition lag' – the time between a problem arising and its recognition by an authority – and a 'policy lag', the time between the recognition of the problem and policy responses. This is the interval of time memorably described by H.G. Wells: 'In England we have come to rely upon a comfortable time-lag of fifty years or a century intervening between the perception that something ought to be done and a serious attempt to do it' (Wells 1934: 584). The policy lag is also known as the 'decision lag', 'administration lag' or 'implementation lag'. The 'outside lag' or 'effectiveness lag' is the time taken for authoritative action to have a measurable effect on the economy.

In cyber security, by analogy, recognition lag is a key issue. The computer security company Mandiant reported in 2014 that network attacks go undetected by the victims (or their proxies) for an average of 229 days, during which time attackers have free access to victims' networks and data (Mandiant 2014). Mandiant reported that this delay has decreased (from 243 days in 2012), but this figure is still too high for cyber security practitioners, given the damage that might be caused during this time, and the persistent inability of victim companies to detect intrusions at an early stage. Scaling from the operational level to the strategic level, cyber security has in most countries passed through a long period of recognition lag. In policy terms, most governments recognise cyber security problems as requiring serious political attention and, consequently, we are now in a situation of contested policy and effectiveness lags. The degree and emphasis of government attention to cyber security differ, but a key point of the original macroeconomic model was that lag times were variable and case-specific; they could be theorised and modelled but not predicted. New problems will continue to present themselves and these too will have their individual time lags, again derivative of multiple variables and local conditions. The duration of each form of lag in any case is not as important as the perception of lag as an expression of sociotemporality, specifically as an intersubjective experience of deceleration.

Cyber security is deserving of tailored policy because of the unique 'speed, scale, intensity, and irrevocability' of the types of events and scenarios facing contemporary societies (Bobbitt 2008: 234). The standard view of many cyber security professionals is that the current situation is 'getting worse, and it's getting worse at an increasingly fast rate' (Bruno 2008). 'To put a pessimistic face on it', writes one, 'risks are unmeasurable, we run on hamster wheels of pain, and budgets are slashed' (Shostack 2012). Similar complaints are endemic to practitioner and political discourses, and just as the biotemporality of humankind is incapable of operating at the same speed as computer networks, so the sociotemporality of politics would seem to trail behind the sociotechnical phenomena enabled by computer networks. Political deceleration is experienced relative to technological acceleration and, as McLuhan wrote so vibrantly, 'it is in this period of passionate acceleration that the world of machines begins to assume the threatening and unfriendly countenance of an inhuman wilderness even less manageable than that which once confronted prehistoric man' (McLuhan 2002: 34).

This is the impression that haunts policymakers and which is expressed frequently in cyber security texts. Cyber security practice and policymaking are forever 'playing catch-up' to technological change and the uses to which information technologies are put. Security 'guru' Bruce Schneier describes this as a 'security gap . . . the time lag between when the bad guys figure out how to exploit a new technology and when the good guys figure out how to restore society's balance' (Schneier 2013a). Crucially, Schneier observes, this gap increases when there is 'more technology' and when technological change is rapid, both conditions that obtain presently.

The inability of government to 'keep up' with information-technological change is because the digital environment 'moves too quickly and requires too much flexibility for the processes of government to be, in most cases, successful in relating to it' (Magaziner 1998, in Lewis 2010: 55). When new technologies emerge, either they are left unregulated or attempts are made to regulate them with 'the old, antiquated rules' (Lewis 2010: 63). More importantly, many argue that governments and their cumbersome bureaucracies are increasingly incapable of responding effectively to internal or external events and processes (e.g. Bolt 2009). In politics, to accuse an opponent of indecision or a reluctance to act is to impute weakness, complacency and the inability to make crucial decisions befitting the office entrusted to that person. These are common tactics in the everyday to-and-fro of politics, but they are tactical ephemera against the backdrop of greater institutional lethargy to which all politicians are subject. Bureaucratic torpor has long been the root of laments about effective government agency, but it is not entirely surprising that the making of policy should be slower than that which it seeks to regulate. Policy does not derive solely from the internal deliberations of a single territorial political entity but through the discursive interactions of 'individuals, interest groups, legislatures, courts, parties, academia, the media, and other institutions', both national and international (Hosein 2004: 187). In this light, policymaking will always tend to be a somewhat slow process.

It is not entirely clear why 'slow' policy should inherently be any worse or less effective than policy made quickly. The opposite is probably true: policy made in the white light and heat of the moment is far more likely to put political expediency ahead of accuracy, ethics and considerations of its secondary and longer-term effects. The reactions of the United States and its allies to 9/11 have occasioned much reflection on this thesis (e.g. English 2009). Robert Hassan notes the 'abbreviated thinking' expressed by kneejerk policy adoption and how it often pertains due to the 'pressure of social acceleration' (Hassan 2009: 98). It might be argued in policymakers' defence that the present rate of change is so great that the subjective experience of relative deceleration is qualitatively more intense now than at any previous historical moment (Rosa 2009). The political pressures 'to secure' may or may not be more persistent than at any other time, but the experience of technological deceleration is arguably uniquely disorienting.

Paul Virilio, the French urbanist and social theorist, is described by one of his anglophone interlocutors as 'the only contemporary radical philosopher of speed' (Armitage 1997: 206). Virilio argues that the corollary of speed is inertia, a stasis reached when one hits the 'barrier' of light speed. Once that condition is reached, there is no need to travel anywhere, as one is already there. It is no longer possible or necessary to effect action in the world and we are instead in a form of incarceration in the time of light (Armitage 1999: 39–40; Virilio 2000). This vision of a technologised future in which political agency is subject purely to the logic of absolute speed may at some point become real – and it possesses no minor predictive resonance now – but we are still in an environment of relative speeds in which this inertia does not yet exist, only acceleration and deceleration. This 'realm of mobility and anticipation', as Virilio calls it (Armitage 1999: 39), is the domain of actual politics in which cyber security policymakers operate and from which policy emerges. The sense of relative deceleration permeates concerns about the difficulties of drafting and implementing effective cyber security policy, of which there are several distinct but inter-related aspects.

The first issue is that existing policy is perceived as inadequate because it is unable to keep up with technological change. In early 2013, the UK House of Commons Defence Select Committee reported to Parliament its findings on the relations between cyber security and the British armed forces. It noted that the 'cyber threat [can] evolve with almost unimaginable speed and with serious consequences for the nation's security' (House of Commons Defence Committee 2013: 7). Elsewhere, the report quoted earlier government policy to the effect that '[e]vents in cyberspace can happen at immense speed, outstripping traditional responses' (House of Commons Defence Committee 2013: 13). One of the enquiry's respondents observed: 'the threat is evolving probably faster, I would say, than our ability to make policy to catch up with it' (House of Commons Defence Committee 2013: 26). Stated baldly in the UK *Cyber Security Strategy* (2011), the 'pace of events can make existing defences and responses look slow and inadequate' (Cabinet Office 2011: 18). This does not prevent government from aspiring to keep pace: 'In a domain where technology and change are fast-moving, responding effectively will require a consistent and extensive effort', involving 'people who have a deep understanding of cyberspace and how it is developing' (Cabinet Office 2011: 5, 29). 'We will need very agile policy decision-makers to keep up with the reality of the threats facing us' (House of Commons Defence Committee 2013: 26). A key priority will be 'to identify and tackle areas where governance arrangements are lacking, insufficient or are struggling to keep pace with the evolving threats in cyber space' (HM Government 2009b: 19–20). From these statements alone, the first dimension of lag is evident: that the acceleration of sociotechnical change means existing policies can never keep pace.

The second aspect is the likelihood that any new policies implemented will fall short of being able to cope with sociotechnical change. In the context of cyber security, a 'critical weakness of any attempt to legislate or regulate security is that specific measures may be outsmarted by new attack technologies quickly' (Bauer and van Eeten 2009: 716). As long ago as 2003, the US recognised that its *National Strategy to Secure Cyberspace* was 'not immutable' and that it must 'evolve as technologies advance, as threats and vulnerabilities change' and, significantly, 'as our understanding of the cybersecurity issues improves and clarifies' (White House 2003: 2). British think-tank Chatham House characterised the situation vividly:

> The pace of change can be so abrupt as to render the conventional action/reaction cycle of strategic evolution out of date before it has begun: it is as if a government operational analyst has been sent to observe the effects in battle of the flintlock musket, only to discover upon arrival that the Maxim gun has been invented. (Cornish *et al.* 2010: 29)

One cannot help but think this is an allusion to Hillaire Belloc's satirical poem on imperialism, 'The Modern Traveller' (Belloc 1898: 41). The conscious inversion of this famous verse now reads, with respect to contemporary perceptions of cyber security, 'Whatever happens, *they* have got / The Maxim Gun, and *we* have not.' In the face of rapid sociotechnical change, policy emphasis is frequently on 'flexibility' and 'adaptability' as the means through which to 'future-proof' cyber security policy. One civil servant from the Office of Cyber Security and Information Assurance (OCSIA) spoke openly in conference about the need for British cyber security policy to embrace innovative 'non-linear' thinking (OCSIA 2011), although this did not appear overtly in the UK *Cyber Security Strategy* (Cabinet Office 2011) published shortly afterwards and for which the OCSIA was principally responsible.

One experienced Washington insider has suggested that the pace of change is rapid but 'not blinding or impossible to describe and manage' (Lewis 2010: 56). This is because, as 'technologies mature and governments gain experience with them, they are brought into the ambit of societal control' (Lewis 2010: 63). The White House recognises this dynamic:

> The history of electronic communications in the United States reflects steady, robust technological innovation punctuated by government efforts to regulate, manage, or otherwise respond to issues presented by these new media, including security concerns. (White House 2009: C12)

This appeal to historical precedent is accurate but does not alter the perception that speed and acceleration are degrading the ability of governments to regulate and legislate for cyber security. It may be that increased direct governmental involvement in cyber security – exemplified by a shift from bottom-up voluntarism to top-down policies coordinated by the executive (Harknett and Stever 2011) – can only ever be aspirational.

In an ontological sense, what if sociotechnical change is subject to an 'open-ended form of speed, which means that the rate at which humans communicate and the rates of increase in productivity and efficiency *can never be fast enough'*? (Hassan 2009: 17, emphasis added). Policymakers and those who rely on their guidance – military, intelligence, security agencies, businesses, citizens and so on – may find themselves in a permanent state of deceleration, approaching and finally reaching the state of inertia presaged by Paul Virilio. Acceleration and deceleration themselves disappear in a new regime of temporality, the permanent nowness of 'real time', in which humans are removed from decision-making loops entirely. Being the ultimate 'time-space compression', this involves 'forgetting spatial exteriority as much as temporal exteriority ("no future") and opting exclusively for the "present" instant, the real instant of instantaneous telecommunications' (Virilio 1997: 25; see also Castells 2010: xl–xli). Democratic process will 'disappear with the advent of a new tyranny, the tyranny of real time, which would no longer permit democratic control, but only the conditioned reflex, automatism' (Virilio 1993: 283). The tyranny of real time threatens democracy because democracy demands that 'man has to reflect before acting'; in an environment where the reflex replaces the human decision, the 'temporality of democracy is threatened, because the expectation of a judgement tends to be eliminated' (Virilio and Petit 1999: 87).

Many would consider this dystopian hyperbole or, as Nicholas Zurbrugg observes of Virilio's work generally, as ignoring 'all traces of positive technological practices' (Zurbrugg 1999: 193). There are also problems with ascribing a singular temporality to the human condition, which is more a product of Western modernity than a reflection of empirical reality (Lee 2012).[5] What the concept of 'real time' reveals are the potential political effects of the logic of speed, which presents the problems of relative speed and cyber security in a new and concerning light. Operational cyber security is highly automated but high-level political decisions are still a human preserve (Buchanan 2014), even if, as in the United States, cyber security strategic decision-making is sometimes vested in the body of the president rather than in Congress. President Obama has published executive orders (White House 2013a, 2013b) aimed at unifying institutional efforts towards better security. In these cases, the justification was that normal legislative processes had failed – in particular, the collapse of the *Cyber Security Act* (2012) – and executive fiat was necessary to short-circuit the impasse caused by the decelerative

[5] Although rarely noted, we find cognate ideas in the work of H.G. Wells, who was much less critical of science and technology than Virilio: 'The revolution in transport has made all governments provisional . . . We move towards a time when any event of importance will be known of almost simultaneously throughout the planet. Everywhere it will presently be the same "now"' (Wells 1934: 122, 144).

lag between cyber security problem and solution (Clayton 2012a). However, this has led to accusations that the executive is seeking to circumvent the legislative process entirely, to the detriment of security and democracy (Little 2012).

We should be cautious in implying that there is anything untoward or exceptional about this use of executive power. Executive orders are no *lettres de cachet* but a standard tool of the US policy process, even if accusations of unilateralism and partisanship are all but inevitable once they are used (Mayer 2001). Additionally, studies suggest that presidents tend not to issue executive orders that are likely to be overturned by Congress, which imposes powerful constraints on their use (Deering and Maltzman 1999). Critics would argue, however, that this situation offers potential sustenance to the diagnosis of William Scheuerman:

> Slow-going deliberative legislatures, as well as normatively admirable visions of constitutionalism and the rule of law predicated on the quest to ensure legal stability and continuity with the past, mesh poorly with the imperatives of social speed, whereas a host of antiliberal and antidemocratic institutional trends benefit from it. (Scheuerman 2004: xiv; also, Chesneaux 2000)

Given the difficulties in steering legislative proposals through a deeply divided Congress, it is understandable that the executive would find ways to break this deadlock. It is also no surprise that (principally Republican) critics should find fault with the methods by which the (Democrat) White House hopes to achieve this. The president is caught between the need to act and criticism of the wherewithal to do so and – like the modernity of which the US presidency is so expressive – is suspended precariously, in Baudelaire's terms, in a transient, fleeting and contingent temporality in which political action may never be fast enough to provide solutions or durable enough to last.[6] This is the decelerative temporality at the heart of the politics of cyber security.

Diagnosing the present

The present is not a (meta)physically ephemeral now but a textured assemblage of tensed knowledge about what has been and what may come, as well as knowledge we generate about the worlds in which we live. The present of cyber security is constructed through the complex interplay of measurable indices of sociotechnical change and the subjectivities of individual and collective human experience. This heterogeneous zone of dissonant

[6] 'Modernity is the transient, the fleeting, the contingent; it is one half of art, the other being the eternal and the immovable' (Baudelaire 1981: 403).

temporality is an important source of political tension and opportunity with respect to speed and acceleration. The conflict between temporalities of the present is both an explicit aspect and a powerful subtext of cyber security politics and practice. The disconnect between humans and the speed of networked computing machines means that the absolute speeds of communication can never be truly known to the unaided observer and leads to ever-greater reliance on computers as the providers of security. The speed of a technologised world makes it hard enough to draft and implement policy without the increased rate of change itself making some policy proposals only aspirational and potentially counterproductive. The radical deceleration at the heart of the subjective experience of relative speed catalyses a perspectival aporia, which, in its rootlessness and concern with the present above all other, inevitably jeopardises the possibilities of democratic politics and its respect for deliberation and reliance upon the art of judgement. The ultimate political significance of speed lies not in its existence, challenging though this is, but in its transformation. As theorised by Hartmut Rosa, under these conditions there is a danger that state and civil society become ‘desynchronized’ and politics becomes ‘situationalist: it confines itself to reacting to pressures instead of developing progressive visions of its own’ (Rosa 2009: 102).

The field of cyber security seems pervaded by a profound sense of frustration and disorientation at being trapped in an accelerating present, cut off from history and with few options for controlling the future. Discourses of the cyber security present are symptomatic of a wider cultural phenomenon, what the science fiction writer Bruce Sterling describes as ‘atemporality’, in which the unprecedented availability of information in the present reduces our desire and capacity to situate ourselves with respect to greater historical structures (Sterling 2010). Luciano Floridi (2012) proposes the emergence of a new ‘hyperhistorical’ age of constant and exponential change born of our dependence on information technologies and which affords little experiential solidity. This portends an historical a-consciousness emerging – in the philosophy of history – from the ashes of modernity. Virilio articulates this dehistoricised perspective when he writes that real time marks the ‘switch from the extensive time of history to the intensive time of momentariness without history’ (Virilio 2004: 119). The ‘open horizon’ of modernity is foreshortened in the headlong rush to the future, even though this never delivers the future, or at least not one identifiable with social progress as Enlightenment ideal.

If the future as ‘horizon of expectation’ never arrives, the category of ‘future’ risks being abolished and replaced with that of the ‘extended present’, in which concerns about the future – in fact, the construction of the future itself – dictate the present, not the other way around (Nowotny 1994: 51; Leccardi 2007: 28–31). It is not that the future does not exist but that the future is increasingly lived in the present as a matter of existential urgency – that we must act now in order to save the future from ourselves; there is little sense of what might lie beyond the now or how we might attain it. This is the situation described by Manuel Castells as the 'culture of the annihilation of time, which is tantamount to the cancelling of the human adventure' (Castells 2010: xliii). The next chapter explores in more detail the relations between present and the future, through an examination of how cyber security futures are imagined in the present and what forms of politics are thereby enabled.

4 Imagining the future

Future and futurity

Saint Augustine, writing in the last years of the fourth century AD, recognised that the future is not something that stretches ahead of us and which will in time be disclosed to us. The future, for Augustine, does not exist, at least not in any concrete sense that would allow us to know it because, quite simply, it has not yet happened in order for us to know it (Augustine 1992: 243). This agrees with our common-sense notion that the future is something unknowable but always intriguing to the curious human mind. Idiomatically, we ask, 'what does the future hold?', and wait to discover its character and its complexion. This is the future perceived as something beyond human control but also a temporal receptacle into which we pour expectations and desires. We are free to imagine and wonder at the future and, as Edmund Burke observed, 'to conceive extravagant hopes of the future' is a common disposition of 'the greatest part of mankind' (Burke 1770: 3). For Augustine, when we think of a 'long future', a bright assessment of potentialities ahead, it is not because the future is in any sense long but that we have a 'long expectation of the future' (Augustine 1992: 243). Our relationship with the future changes as we change, and our perspectives on the future are expressions of our present condition as much as they are predictions about the empirical character of times yet to exist.

The previous chapter proposed that the future has been subsumed within the category of the extended present, by which visions of the future serve to regulate the present in historically unprecedented ways. This change in historical perspective represents a sense that the future is no longer open and available. In a secular age, in which historical narratives cannot necessarily advance or ensure an improved future through divinely ordained progress, and in which increased sociotechnical speed foreshortens global temporal horizons and potentially truncates democratic process, it is understandable that the future might no longer have quite the lambent appeal of its former religious or Enlightenment incarnations.

More than this alone, the present period – which is variously labelled 'late modernity', 'high modernity', 'reflexive modernity', 'supermodernity', 'hypermodernity', 'transmodernity' or 'postmodernity' – has a distinctly eschatological sensibility that filters the present through the lens not only of the future but of the final events of the world. (I retain 'postmodernity' here, not through authorial belief in a decisive disjuncture with modernity but on account of the term's relative familiarity and because it reflects upon the nature of modernity as much as it does on what postmodernity itself might be.)

This shift from optimistic modernity to pessimistic postmodernity has occurred over a century defined by war and trauma. World War I deeply altered the positive social futurism of Victorian and Edwardian intellectuals, argues the historian Richard Overy (2009). The war was a disastrous adventure that enervated national spirit and dampened prior expectations of social progress, a 'domestic malaise' further exacerbated by developing concerns over demography, economy and political turmoil (see also Hughes and Wood 2014). This depressive atmosphere so sensitised the British public that the 'escape into war' in 1939 came as something of an apocalyptic release (Overy 2009: 384). The industrial-scale carnage of Operation Barbarossa (1941) and – in British eyes – the rout of German forces at the second battle of El Alamein (1942), were considered turning points in the course of the war after which people could begin to imagine a post-war world free from tyranny. The euphoria of armistice would be tempered by the grind of rebuilding lives and economies, but a brighter future was imaginable and achievable. This feeling gradually soured as the Cold War took shape, and so irresistible was its grip on people of East and West, and so completely did it define geopolitics for four decades, that it had 'the power to represent and to create a whole world' (Gregory 1989: 12). Under the 'nuclear shadow', and alarmed by superpower brinkmanship, people's expectations of the future were unmistakably and negatively affected.

Concerns about demography and the carrying capacity of the natural world have been deepened further by increased awareness of human damage to the global environment. The possibilities of human megadeath and species extinction have brought the future very much into the present (Bostrom and Ćirković 2008). From anthropogenic environmental degradation to resource shortages born of overpopulation and the conspicuous collective inability to address climate change, the future has become an immediate concern guiding present action rather than an empty vessel into which to project human desires. In this change is often identified the shift from modernity to postmodernity, from a world that we can control through science and reason to a world foisted upon us and over which we have little influence. *Telos* gives way to chaos and contingency and the grand narratives of modernity disintegrate into the polysemic cacophony of postmodernity, robbing humankind of certainty and foundation. William Butler Yeats, writing at the end of World War I, identified this as the centre that 'cannot hold', and through the disappearance of which,

> Mere anarchy is loosed upon the world,
> The blood-dimmed tide is loosed, and everywhere
> The ceremony of innocence is drowned;
> The best lack all conviction, while the worst
> Are full of passionate intensity. (Yeats 2008: 158)

As Yeats suggested, this growing angst is intensified by increased access to knowledge and, we might extrapolate, to the technologies that facilitate its pursuit and creation. Global news media and the internet mean that the convolutions of global climate summits can be followed minute by minute in their failure to demonstrate the concerted political will necessary to avert catastrophic climate change (Dimitrov 2010). Those same technologies mediate death by 'natural' disaster and gross human violence, events that become global in their consumption and in their capacity to fuel popular imagination and corroborate narratives of global decline. They amplify concerns caused by an extant distrust of science, like the possibility that the Large Hadron Collider would conjure from the fabric of spacetime a black hole capable of swallowing up the Earth (Tegmark and Bostrom 2005). The 'new media ecology' enables 'a perpetual connectivity that appears to be the key modulator of insecurity and security today'; it becomes in its ubiquity and significance 'the very condition of terror for all of us' (Hoskins and O'Loughlin 2010: 2). This same environment means it is also ever more difficult to 'forget' the past (Hoskins 2011), so that past events and mistakes pile up behind us as a digital archive of global deterioration.

Media communicate other worries catalysed by science, exemplified recently by our growing awareness of the transits and possible collisions of near-Earth objects (NEOs) with our planet. In February 2013, the 'near miss' of asteroid 2012 DA14 was a global news event trailed long in advance, thanks to the ability of astronomers to detect, track and predict the path of this cosmic visitor with impressive accuracy (BBC News 2013a). Conciliatory assurances from the scientific community that the asteroid was no threat to life on earth were dented by the spectacular descent of a meteor over the Russian Urals the day before 2012 DA14's fly-by, damage from which injured up to 1,200 people (*Daily Telegraph* 2013). One newspaper columnist remarked of these coincidental events that like 'the prospect of being hanged, it concentrates the mind wonderfully ... [on] a sunny day, the prospect of universal annihilation adds zest to a brisk walk in the park' (Kaveney 2013). Or, as a graphic circulating on the internet had it: 'Asteroids ... are nature's way of asking: "How's that space program coming along?"' Scientific knowledge about the cosmic transits of NEOs has not increased the likelihood that one will strike Earth, but it has made it more probable we would know about an impact beforehand. More refined knowledge of our galactic neighbourhood has improved astronomical awareness but also fostered a heightened sense of the prospects of catastrophe and of existential finitude. There are many ways to imagine 'TEOTWAWKI', internet slang for The End of the World As We Know It. We appear to be, as John Gray asserts, 'a culture transfixed by the spectacle of its own fragility' (Gray 2012).

The previous chapter argued that the political imperative 'to get faster' can be understood as a response to the fear of national decline and as a way of mobilising political action through appeals to public concerns over national status. Vieira argues in his analysis of late Victorian and Edwardian politics that contemporary narratives of decline served political ends by 'rhetorically increasing the nation's imagined proximity to a temporal endpoint', greatly enhancing the perceived need for solutions to problems created by speed and the acceleration of sociotechnical change, opportunities ably exploited by political elites (Vieira 2011: 386). Perceptions of dystopia and decline shape narratives through which political change can be effected. This chapter concentrates on one manifestation of these rather sombre – although often spectacular – imaginings of the future: the notion of an 'endpoint' against which history is interpreted and through which social order is transformed. The task of this chapter is to demonstrate this eschatological aspect of cyber security as a key facet of the chronopolitics of cyber security.

Cyber security is situated with respect to contemporary military and security imaginaries dominated by dystopian visions of the future that reflect eschatological postmodernity. In cyber security discourses, one particular genre of future scenario emerges as a dominant form – that of 'cyber doom'. Catastrophic scenarios are presented as inevitable products of present insecurities and display a distinct temporality that can be identified as apocalyptic, not just in the narrative reliance on catastrophe, but in the primary sense of apocalypse as a time of revelation and transformation, both of which qualities are in some sense 'desired'. These aspects are examined in detail and linked to the concept of 'technological accident' as a theorisation of temporality and technology that is inherently apocalyptic in its dimensions of imminence and immanence. I further argue that resilience in cyber security discourses is an expression of and response to apocalyptic thinking in postmodernity.

Imagination and dystopia

In a 1902 lecture to the Royal Institution, the writer H.G. Wells hoped to convince his audience that the future could, in a real sense, be 'known' through science and theory, at least in its general direction and probable attributes. Wells distinguished the common man's inattention to the future with the rarer 'creative, organizing or masterful' minds that give value to the present principally in relation to the future (Wells 1913: 4–6). His panegyric to technological modernism would doubtless resonate with those persons today charged with securing society, who might recognise in this description their own talents as visionary agents blessed with no minor oracular powers. These future-minded professionals are characters in journalist Matt Carr's review of the 'new military futurism', which details how the British and American militaries, in partnership with the private sector, have developed ways to generate knowledge about the future (Carr 2010).

During the Cold War, Western militaries were principally concerned with managing relations with the Soviet Union, and how to win (or, as a minimum, survive) a nuclear exchange. This attitude allowed the prospect of victory and was grounded in the certainty and relative inflexibility of superpower bipolarity, in which the innovative likes of game theory could satisfactorily model diplomacy and the probable courses of military interaction. The demise of the Soviet Union destabilised this ossified superpower enmity and ushered in perceptions of a dynamic world of rapidly evolving risk and threats (Mueller 1995). In this environment, the major security threats to international order came from 'new wars', in which transnational constellations of insurgents, terrorists and criminals combined to challenge states' monopolies on legitimate violence and their ability to exert control over their restive populations (Münkler 2005; Kaldor 2006). Key actors in this emerging political economy of violence are 'global insurgents' (Kilcullen 2005; Mackinlay 2009), ideological rebels whose ambitions surpass the territorial and challenge global political order itself.

On 11 September 2001, these ambitions were realised, with al-Qaeda's attacks on the United States bringing home to continental America the tragic potency of globalised violence. The events of 9/11 caused deep reflection on whether they could have been somehow foreseen and averted. The official diagnosis of a 'failure of imagination' resulted in a renewed securocratic impulse to 'imagine the unimaginable ... a tendency which has generated imaginative scenarios that sometimes owe more to apocalyptic Hollywood movies, manga comics and science fiction than they do to sober analysis' (Carr 2010: 16). Those charged with imagining and forecasting the future are often even more pessimistic than during the Cold War and envisage an ‘unsafe and unstable world’ in which the US military perceives itself as ‘the last bastion of civilisation against encroaching chaos and disorder’ (Carr 2010: 18). These visions of dystopia are not warnings against the perils of misplaced utopianism – as per the science-fictional futures of Aldous Huxley or George Orwell – but justifications for ‘limitless military “intervention”, techno-warfare, techno-surveillance and weapons procurement programmes’ (Carr 2010: 18). This new military futurism intends to counter exactly the ‘submissive’ mindset identified by Wells, which views the future as ‘a perpetual source of convulsive surprises, as an impenetrable, incurable, perpetual blankness’ (Wells 1913: 21).

However, this new military futurism is not the body of knowledge envisioned by Wells. He wrote of ‘building up this growing body of forecast into an ordered picture of the future that will be just as certain, just as strictly science, and perhaps just as detailed as the picture that has been built up [of] the geological past’ (Wells 1913: 35). Rather than science, imagination is mobilised as an additional mode of fostering security knowledge, through which to ‘dispel secrecy and ignorance, compute risk and uncertainty, and prepare for surprise and novelty’ (Aradau and van Munster 2011: 69–70). Through imagination as an aesthetic rather than scientific approach to the future, ‘a range of apparently disparate details, perceptions, ideas and assumptions can be brought together in a seemingly coherent whole’ (Aradau and van Munster 2011: 70). In the context of ‘high impact, low probability risks’ – of which ‘cyber doom’ is surely an example – the UK government identifies a ‘lack of imagination’ in considering these risks and advises the development of tools ‘to enable risk assessors to “imagine” these risks and expand the boundaries of their mental models’ (Government Office for Science 2011: 11). Importantly, this process requires a wide range of experts from different disciplines and background to provide the ‘collective imagination’ necessary for these endeavours.

There are undoubtedly good and publicly minded reasons for adopting this approach, but these are not always apparent. By processing the future through a dystopian aesthetic, military planners may be discharging their duties to prevent the preventable but might be bringing about, by thinking the unthinkable, exactly those situations in which interventions might be required, further justifying investment and expenditure in future capabilities. Bernard Brodie noted in the late 1970s that the defence establishment is staffed by people ‘sometimes of considerable imagination’ but whose ideas are not always ‘worth a second thought', let alone investment in time and money (Brodie 1978: 83). These are wise words that Carr's account suggests may not have found the institutional home they deserve. As John Mueller wryly observes, particularly since 9/11, it is 'clearly possible to have a surfeit of imagination' in national security matters (Mueller 2010: 161).

This is the construction of a system of knowledge about the future, based in the imaginative capacities of security actors and communities and which facilitates certain political operations with respect to the future, as is the task of all security. We might extrapolate the dystopian military mindset to the cyber security imaginary more broadly, as there are affinities with the ways in which cyber security futures are imagined. However, analyses along these lines often tread the same path as the phenomena they seek to understand, in that their attention to the future forgets the history of those futures, in this case the history of dystopia as an expression of perceived societal decline and other forms of collective anxiety. Sean Lawson correctly observes that contemporary cyber security concerns are rooted in historical fears occasioned by the invention and adoption of earlier information and communications technologies, like the radio, telegraph and telephone (Lawson 2013b; also, Brosnan 1998). He notes the genealogy of anxiety accompanying the development of interconnected and interdependent infrastructures in modern industrial societies, worries consonant with general apprehension about the impact of new technologies on society. As Marshall McLuhan observed of new developments in communications, 'wherever a new environment goes around an old one there is always new terror' (Canadian Broadcasting Corporation 1967).

The pervasive ubiquity of 'cyberspace' has stimulated multiple misgivings as to its actual and potential effects. The internet has brought to the fore issues of child protection, violent media, pornography, crime and social alienation, to mention but a few, all of which have induced periodic public spasms of moral panic (Sandywell 2006; Marwick 2008; Thierer 2013). In commerce, internet technologies have threatened supposedly stable business models and encouraged a range of consumer-led activities that undercut their bottom lines. Politicians fret at the thought of the diffusion of 'power' via the internet to people and organisations at odds with their own strategic ambitions and worry at the new tools of conflict available to non-state actors. At the same time, they see no irony in their own attempts to deploy technology, law, regulation, military force and sometimes dubious moral authority in order to preserve the status quo. Cyber security intends to secure against all of these things and many more, but it also seeks to preserve and encourage what is 'good' about the internet and ICTs. In one expression of this orientation, cyber security is about ‘our struggle to have our cake and eat it too’ (Rosenzweig 2013: 2). On the one hand, cyber security is the antidote to state-sponsored cyber attacks on critical information infrastructures and to the actions of cyber terrorists and criminals. On the other, cyber security creates a more conducive environment for business and affords government opportunities for the exploitation of 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).

However, it is the darker visions of possible security futures that give principal sustenance to the cyber security imaginary. Carr asserts that American military futurism is one response to the apparent decline of the United States as the pre-eminent political – if not military – power (Carr 2010). American concerns about China’s sponsorship of commercial and political cyber espionage are framed by an interpretation of China as the potential usurper of American global power and portend the renewal of superpower rivalry (Hartnett 2011). This taps into existing stereotypes, and in the US–China context, we might assess the resurgence of reference to the ‘aggressive behaviour’ of China as a rhizomatic eruption of the persistent American cultural trope of the racialised ‘Yellow Peril’ (Shim 1998). However, we should not dismiss or excuse China’s stated strategic aims or the demonstrable activities of Chinese entities in this space. National decline is a powerful narrative and is often constructed with reference to one or more external entities rather than to abstract history alone, but there is another aspect of cyber security discourse that shifts attention from actors and entities to ‘events’. As Carr suggests, imagined events are often catastrophic and rely upon a distinctly dystopian mindset that generates predictions that are ‘often very grim indeed’ (Carr 2010: 18).

Catastrophe and apocalypse

In postmodernity, write Ulrich Beck and colleagues, ‘the future looks less like the past than ever before and has in some basic ways become very threatening’ (Beck *et al.* 1994: vii). In the cyber security imaginary, we might propose, the future looks almost nothing like the past and has become not only threatening but also catastrophic in an existential register. This is true only in one important sense, however. A key discursive strategy in cyber security is to note that the problems of ‘cyber insecurity’ are long-standing and deserving of political action that has never arrived. This applies even when referring to ‘new’ risks and threats, the possibilities of which are catalysed by extant vulnerabilities and processes rather than being truly novel in all their dimensions. The ultimate effects of these insecurities are often deferred to the future and frequently reduced to singular catastrophic events that demonstrate the shortcomings of contemporary politics and politicians. These events have no direct historical analogues, although attempts are often made to link them to other historical events with which they share superficial similarities (see Chapter 5). Given the historical dearth of comparable events, these events are necessarily the product of the security imaginary and often 'remain fiction, not to say science fiction' (Rid 2013a: 4; Dunn Cavelty 2008: 56–7). Regrettably, we cannot pursue here the rich history of science fiction as a genre instrumental to national security thinking (Gannon 2009; Jagoda 2012), but the catastrophes which populate the security imaginary are 'both the stuff of Hollywood films and the product of expert imagination' (Aradau and van Munster 2011: 69).

This emphasis on the catastrophic event has been identified repeatedly in analyses of cyber security discourses and characterised as the production of 'cyber doom' scenarios (Dunn Cavelty 2008: 2–4). These are 'worst-case' scenarios that impress upon audiences the serious consequences of inappropriate or inadequate actions to secure information infrastructures in the present yet discount the salient fact about these postulated catastrophes, their 'unsubstantiated nature' (Dunn Cavelty 2008: 3). These scenarios are examples of a tendency in cyber security towards 'hypersecuritisation', in which discourse 'hinges on multidimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence *and* the fact that [none] of these scenarios has so far taken place' (Hansen and Nissenbaum 2009: 1164, original emphasis). For example, Richard Clarke and Robert Knake's book *Cyber War* (2010), whose publication was widely reported in the press, contains a five-page description of what could happen if cyber security is not sufficiently addressed in the present. 'Cyber warriors' assault the critical national information infrastructures of the United States and aircraft begin to fall from the sky. Trains are derailed in their dozens, cars collide as traffic control networks malfunction, gas pipelines explode, chemical plants vent poison gas across urban areas, financial systems crash and satellites spin out of orbit into space. Food, water and energy distribution networks falter and fail and, when law enforcement and security agencies fail to cope with rising public panic and civil unrest, the government finally loses control (Clarke and Knake 2010: 64–8).

It is hypothetically possible, especially because software is often the 'least robust' component of infrastructural systems, that subversion and degradation of information infrastructures – by accident or design – may cause failures to cross 'infrastructure boundaries' and, potentially, to radiate throughout infrastructure networks, with potentially disastrous effects (Little 2002). Infrastructure failure might not just cascade through physical infrastructures but could ripple into the affective realm. Following Massumi's translation of Deleuze and Guattari, 'affect' is used here to denote 'an ability to affect and be affected . . . a prepersonal intensity corresponding to the passage from one experiential state of the body to another and implying an augmentation or diminution in that body's capacity to act' (Deleuze and Guattari 2004: xvii). The argument is that cascading failure would bring hunger, thirst and psychological distress, before undermining the structures of government and, ultimately, of society itself. It is possible that 'concatenating these sorts of events can trigger the economic and political panic that no recent war has ever brought to an advanced society' (Bobbitt 2008: 96). It is not only the malware or even the failure of the infrastructure that worries governments most but 'the fear of the release, the presence of a negative symbolic virus, the contagion of insecurity, which disseminates distrust and fear' (Burgess 2007: 481). However, as Howard Schmidt, later chief cyber security advisor to President Obama, wrote in his 2006 memoir: 'Is it possible for one of these events to happen? Sure. Is it likely? Absolutely not' (Schmidt 2006: 172).

More important than whether these catastrophic events will happen or not is that by definition they have not yet happened: they are always in the future, whether they eventually occur in some future present or not. Read through the lens of securitisation theory, which stresses the speaking-into-being of security threats through which to mobilise political resources, these constructed 'cyber doom' scenarios perform political work. As Myriam Dunn Cavelty concludes in her exhaustive analysis of US cyber security policy, it matters less whether threats have empirical validity or not: 'what matters is that decision-makers consider cyber-attacks a real threat and act accordingly' (Dunn Cavelty 2008: 143). This is not to ignore the practical ramifications of addressing 'real' security issues, nor of ignoring them, but to stress that these future scenarios can be nothing other than imaginative constructs, no matter how 'expert' that imagination is. This is not to say that there is no wisdom in this 'possibilistic' thinking. After all, as Lee Clarke suggests, 'the sky *could* be falling' and it might be sensible to prevent or prepare for it (Clarke 2006). The task here is to examine further the political aspects of the temporality of these constructions of catastrophe that are not reducible to their interpretations as securitising speech acts alone. In their role as future events through which present politics is shaped, cyber catastrophes represent an eschatological dimension of cyber security. We can identify an apocalyptic aesthetic in cyber security that finds expression in these scenarios, a constructed temporality that allows us to enquire more deeply into the politics of cyber security than the lens of securitisation alone.

The present enquiry delineates the apocalyptic aesthetic as a way of imagining and thinking cyber security futures rather than as literal recourse to what we ordinarily perceive as a religious sensibility. We cannot ignore the many obvious references to religious apocalypse in cyber security discourses, however. These are more often found in headlines than in high offices, with numerous references to Judaeo-Christian doctrines of the end times, including 'cybergeddon', 'cyberarmageddon', 'cybarmageddon' and 'cyber apocalypse'. A 'cyber-apocalypse', one dictionary records, is 'a cyber attack that could wreak havoc on the nation by bringing down critical information infrastructures' (Schell and Martin 2006: 78). So pervasive is the contemporary 'fear' of 'devastating viruses and worms' that the period from 2001 onwards is presented as the 'Fear of a Cyber Apocalypse Era' (Schell and Martin 2006: xxv). It is 'only a matter of time', we read, 'before cyberterrorists are able to unleash a cyber apocalypse' (Gable 2010: 118). When it happens, this cataclysmic event will 'make 9/11 look like a tea party' (*The Economist* 2012: 62).

One commentator, inviting professional fraternity, wrote, '"Cybergeddon" is imminent. I am hardly alone' (Levin 2012). He was not; one senior lawyer, writing in *The New York Times*, claimed that 'cybergeddon' is 'one of the greatest existential threats facing the United States' (Bharara 2012). Eugene Kaspersky, an influential voice in information security, told a Tel Aviv audience that when the 'event' happens, 'it will be the end of the world as we know it . . . I'm scared, believe me' (Cohen and Lubell 2012). Others, like the Atlantic Council (Healey 2011) and the World Economic Forum (2014), view 'cybergeddon' as a state of affairs rather than a single event, a condition of 'insecure growth', dominated by the inability to trust online transactions of any kind. Whatever 'cybergeddon' actually means – and many are sceptical or outright dismissive of this terminology – there is a widespread sense of fatalism in cyber security discourses (Glenny 2011). The 'sky *is* falling', writes one defence information security professional, but it is doing so 'very slowly' (Geers 2009: 4, added emphasis).

These scriptural allusions are not uncommon but should not be interpreted superficially: none of the examples above should be interrogated as if their creators truly believe that a religious apocalypse in the Judaeo-Christian mould is imminent. Rather, Armageddon and apocalypse are cultural reservoirs providing 'readily available tropes' for use in narratives of disaster (Stronach *et al.* 2014: 332). The ubiquitous sense of doom is a key indicator of a more entrenched apocalyptic aspect of cyber security: eschatological discourses are structured around events that represent end points of social order. Moreover, because they interpret history in the light of the final events of the world, eschatological narratives impart meaning to events in the present. Contemporary events are imbued with eschatological meaning and are interpreted as 'signs' of impending apocalypse (Robbins and Palmer 1997: 4–5).

In cyber security, there is a long list of 'signs' which structure a thousand texts: Cuckoo's Egg, Eligible Receiver, Morris Worm, ILOVEYOU, Estonia, Georgia, GhostNet, Conficker, Operation Aurora, Stuxnet, Flame, Duqu, Shamoon. Y2K is mentioned occasionally , a computer-related 'event' interpreted also as a sign of a more general impending apocalypse, or even the Apocalypse itself (Schwaller 1997; Schaefer 2004; Pärna 2010). The historical details and specificity of each entity in this roll-call of malware, sabotage operations, government exercises, countries and espionage programmes are less important than their construction as discrete 'events' that populate and corroborate the apocalyptic narrative. In cyber war narratives, a specific example of the cyber security apocalypse, these events become 'signifiers of the no-longer-future-but-reality of cyber war' (Dunn Cavelty 2013: 117). They ground cyber security narratives in a constructed history, in which these foundational events act as metonyms for insecurity and as mnemonics to remind audiences of the consequences of ignoring the signs. Crucially, the frequency of these events increases towards an apocalyptic end point, a 'thickening' of history (Beissinger 2002: 27) in which isolated events impart an increasingly cohesive structure to the temporality of the present. Not infrequently, these signs are constructed definitively as events bringing the future into the present. In the case of Stuxnet, for example, 'the future is now' (Farwell and Rohozinski 2011).

Prophets tend to be self-appointed and there is no shortage of people willing to 'read' these signs and pronounce upon them. There seems to be no requirement to heed Horace Walpole's advice that 'the wisest prophets make sure of the event first' (Walpole 1973: 233), given the high anecdotal quotient of many pronouncements, particularly as the 'distance' between historical event and speaker increases. This is not, however, to discount a priori the sincerity or expertise of many of these 'Cassandras of cyber warfare' (Rid 2012: 6). The importance of Cassandra is not that people thought her a false prophet but that her correct predictions were ignored. These scenarios are often the products of 'expert imagination' and perhaps should not be dismissed lightly, given the possible consequences of doing so (Hansen and Nissenbaum 2009: 1164).[1] Again, the

[1] Richard Clarke, a first-rank cyber doom-monger, is known as 'the Cassandra of the war on terror', whose warnings of a 9/11-type attack on the United States were ignored (Harris 2011).

framing of apocalypse is of most interest, particularly with direct reference to those who self-identify as prophets, like the aforementioned Eugene Kaspersky:

> The evolution of cyber-Armageddon is moving in the predicted trajectory (proof it's not just a matter of my frightening folk just for the sake of it); this is bad news. The good news is that the big-wigs have at last begun to understand . . . Looks like the Cassandra metaphor I've been battling for more than a decade is losing its mojo – people are listening to the warnings, not dismissing and/or disbelieving them. (Kaspersky 2012)

Kaspersky is partly correct, as there is no doubt that cyber security spending – if we can take that as a proxy for 'belief' in apocalyptic narratives – has increased markedly over the period he describes to a current annual level of nearly $80 billion, increasing to $120 billion by 2017 (Gartner 2014; Rashid 2014; see also, Aaron 2012). However, in the belief system espoused here, Kaspersky cannot be wrong. Unlike religious prophets, who might predict the dates and times on which future apocalyptic events will occur, secular prophets like Kaspersky have no need to excuse themselves from inaccurate predictions because they simply do not make predictions with calendrical certainty. This 'unfalsifiable cyber-augury' has been identified in other areas of 'guru'-led internet prediction too (Poole 2012). Secular prophets share with religious prophets their talents as 'masterful *bricoleurs*, skilfully recasting elements and themes within the constraints of their respective traditions and reconfiguring them to formulate new, meaningful endtimes scenarios' (Wojcik 1997: 148). They have in common that 'the error revealed by the non-fulfilment of such an expectation itself [becomes] proof that the next forecast of the End of the World [is] even more probable' (Koselleck 2004: 265).

The specific vectors of 'cyber insecurity' may change – new vulnerabilities and malware variants are discovered all the time – and the timescales may expand and contract – 'tomorrow', 'soon', 'within a decade' – but the faith and certainty in the 'cyber apocalypse' remain firm. 'I don't know when or where', opined Eugene Kaspersky in 2014, 'but I'm afraid it [global cyberterrorist attack] is going to happen' (Gibbs 2014). He may be right, but the more important point is that he is very unlikely, eventually, to be wrong. A century ago, the novelist Erskine Childers described a certain type of national security character as a 'meddlesome alarmist, who veils ignorance under noisiness, and for ever wails his chant of lugubrious pessimism' (Childers 1995: 98), a description likely to resonate in the present context. There is an historical continuity with a heritage of historical prophecy with respect to the catastrophic mindset of security imaginaries (Aradau and van Munster 2011: 18).

The level of 'apocalyptic intensity' already elevated through the reading of signs can be heightened further by making predictions that are 'imminent but indeterminate' (Bromley 1997: 36). This creates a constant state of awareness and readiness – 'a temporal liminality or intermediacy as the present is ending while the future is yet to be born' – in which those involved 'feel themselves to be standing poised on the brink of time' (Bromley 1997: 36). This leaves futuristic scenarios deliberately 'shrouded in a cloud of speculation' (Dunn Cavelty 2008: 4). This is an established tactic of security discourses, in which claims of and for security often have 'an air of slovenly imprecision' obscuring the nature of the phenomena in question but which serve as useful rhetorical resources in pursuit of political ends (Walker 1997: 63). In common with other forms of security, cyber security invokes 'realities and necessities that everyone is supposed to acknowledge, but also vague generalities about everything and nothing' (Walker 1997: 63).

The epistemic tensions between the poles of clarity and obscurity are partially resolved by reading the signs of the apocalypse as corroboration of a 'script' of the future, Kaspersky's 'predicted trajectory'. Apocalyptic worldviews are inherently deterministic and in many cases the future is – often, literally – already written (Robbins and Palmer 1997: 5). These scripts of the future gain explanatory power when events and scenarios appear to converge and potentially increase the volatility of those subscribing to this outlook, particularly if already psychologically stressed (Robbins and Palmer 1997: 5). Given the tendency to construct apocalypse in dualist terms, millenarian scripts usually have entities playing each of the 'good' and 'bad' roles. In 1993, federal agents and police stormed the millenarian Branch Davidian compound in Waco, Texas, a controversial operation that caused dozens of deaths. In this case, the government acted in ways already 'scripted' in advance, unwittingly bringing about exactly the apocalypse 'predicted' by believers (Barkun 1997: 256; Keep 1995).

The self-fulfilling and prophetic aspects of the cyber apocalypse register in the admonitions of cyber security experts not faithful to apocalyptic scripts. To the untutored, strange animals can appear unduly fearsome. The former White House cyber security 'czar' Howard Schmidt warns against letting these 'phantoms' exceed empirical reality (Schmidt 2006: 124–5). Such 'dark' imaginings can 'easily become the darkest driving force of all should we over react' (Deibert 2012: 261). In this way, apocalypse may be brought about by those who, even if they do not desire it, cannot imagine an alternative outcome. This brings into sharper focus another aspect of apocalypse. The apocalypse is imminent, but it is also immanent: it is inevitable given the conditions of humanity and the world.

In this respect, it finds great affinity with the concept of the 'technological accident', itself an apocalyptic expression of postmodernity. The following section addresses the relations between these two concepts and with cyber security.

Immanence and accident

In considering the origins of apocalypticism, Jeff Lewis identifies the 'eschatological-Faustian pact' that led prehistoric humans to settle in fertile and resource-rich areas at high risk from tectonic and volcanic activity, like the Pacific 'ring of fire' and the Mediterranean basin, a process that continues and intensifies to this day (Lewis 2012: 97). Lewis refers to the apocalypse movie *2012* (dir. Roland Emmerich, 2009), in which Los Angeles is spectacularly destroyed by earthquake and consigned to the ocean. Los Angeles's precarious location between the tsunami-prone Pacific and the seismically active San Andreas Fault, along with its long history of wild fires, floods, killer bees and other life-threatening phenomena, has led to its portrayal by sociologist Mike Davis as 'Doom City', permanently on the edge of disaster (Davis 1999). Such is its reputation and potential that it serves as a cipher for American fears (and desires) of urban catastrophe, being destroyed in popular novels and films some 138 times during the twentieth century (Davis 1999: 276). With the possible exceptions of London (A. Taylor 2012) and Tokyo (Tsutsui 2010), Los Angeles has few rivals in its role as a symbolic sacrifice to assuage the violence of nature or the myopia of man, but to fulfil its mediated destiny it must always rise again in order to be demolished once more. Los Angeles' marginal existence means it is destined one day to be destroyed, either partially or wholly, a city built in denial of nature but unable finally to withstand it.

Theorising the human-ness of 'natural' disaster may be an expression of intellectual anthropocentrism, but it does imply humanity's complicity in its own downfall rather than a mere dumb recipient of cosmic ill fortune (Murphy 2001). Like many other commentators on the American condition, Mike Davis cites Henry David Thoreau's *Walden* (1854), the quintessentially American meditation on nature and modernity, in which he 'sounded the tocsin against the potentially catastrophic environmental threat of the industrial revolution' (Davis 1999: 15). Thoreau's analysis of modernisation does not restrict itself to the effects of humanity on nature. In one striking passage, he writes of the impact of humankind's technology on itself, equating the enthusiasm for railroads with 'grading the whole surface of the planet':

> Men have an indistinct notion that if they keep up this activity of joint stocks and spades long enough all will at length ride somewhere, in next to no time, and for nothing; but though a crowd rushes to a depot, and the conductor shouts 'All aboard!' when the smoke is blown away and the vapour condensed, it will be perceived that a few are riding, but the rest are run over, – and it will be called, and will be, 'A melancholy accident'. (Thoreau 1888: 52)

Thoreau does not say if he had in mind the death of William Huskisson MP, who in September 1830 had become the first railway fatality, killed by George Stephenson's *Rocket* at the inauguration of the Liverpool and Manchester Railway, an archetypal death often described *in memoriam* as a 'melancholy accident' (Pietz 1997: 99). Rather than cancel the event, the railway directors decided to proceed, in order to show that the incident was, as *The Times* of London reported, 'a mere accident, and had not happened through any fault of the machinery' (Pietz 1997: 99). A jury swiftly convened by the Liverpool coroner decided no criminal homicide had taken place and 'acquitted the engineers and the machinery of all blame' (Pietz 1997: 99). The verse of one contemporary poet reflected this conclusion, recording that Huskisson by 'unforeseen mischance was over-run' (Baker 1857: 189, in Viereck 1949: 91). These interpretations of Huskisson's death as 'bad luck' differ greatly in emphasis from Thoreau's reading of the same type of 'accident'. For Thoreau, the railroad accident is immanent to the technology of the railway, rather than some mishap or trick of fortune.

This perspective is familiar to critics of technology, from the machine-breaking Luddites of the nineteenth century to the anarchists and primitivists of the twentieth and twenty-first centuries, who see in technology the seeds both of its own downfall and of society itself. The anarchist writer George Woodcock observed that it is 'a frequent circumstance of history that a culture or civilization develops the device that will later be used for its destruction' (Woodcock 1977: 133). Theodore Kaczynski, the notorious Unabomber and prominent neo-Luddite, based his ideology (and practice) around the idea that 'technology' itself, rather than any technological form or function, is the cause of societal destruction (Kaczynksi 1995). 'Technology' is seen as a unitary if internally heterogeneous entity, possessive of an auto-generative 'life force', a view shared with some contemporary technophiles (e.g. Kelly 2010). Moreover, once *en train*, 'technological progress marches in only one direction; it can never be reversed' (Kaczynski 1995: paragraph 129). This places technology at the heart of a teleological interpretation of history, in which technology often stands as a proxy for the Western humanist and liberal ethos of progress (Gordon 2009).

Wolfgang Schivelbusch records that prior to the Industrial Revolution there was no coherent concept of the 'technological accident' as something brought about through the existence of technology itself. After the Industrial Revolution, however, 'destruction by technological accident came from the inside', and the more intensely packed the physical forces of technology, 'the more thorough-going was its destruction in the case of dysfunction' (Schivelbusch 1986: 131). The speeding projectile of the steam train – or, later, the airplane and motor vehicle – causes carnage upon impact with another object, obliterating itself, its passengers and other entities caught up in the maelstrom of the accident. But this catastrophe is local, and its causality linear and traceable: the points failed, the brakes locked, the accident happened. A different category of accident emerges from non-linear technological systems, the inherent catastrophic potential of the 'normal accident'.

Sociologist Charles Perrow popularised the idea that highly complex technological systems will always produce 'normal accidents'. These are 'normal', like the Three Mile Island nuclear accident (1979) that prompted Perrow's original work in this field, not because they are not 'unexpected', 'incomprehensible' or 'uncontrollable', but because they are 'unavoidable' (Perrow 1981). Far from alleviating this situation, attempts to reduce risk often increase it, by adding more layers to the very complexity which increased the risk in the first place (Perrow 1999; see also Beck *et al.* 1994: vii). Moreover, because accidents are often initiated by the interactions of multiple small failures, large accidents usually have banal and trivial causes, which take untold possible forms: 'We have produced designs so complicated that we cannot anticipate all the possible interactions of the inevitable failures' (Perrow 1999: 11). Even if we could somehow attain perfect 'system knowledge', we could never know enough about the potential interactions of components to predict when and where failures might occur and with what other components they would interact and magnify – cascade – through the system and those connected with it (Zimmerman 2001). Failures are immanent to complex technical systems and will occasionally be catastrophic.

This is the accident as ontology of technological modernity, a perspective that also permeates Paul Virilio's progressive theorisation of the accident over the last two decades. Perrow, Schivelbusch and others have also recognised that to 'invent the train is to invent derailment; to invent the ship is to invent the shipwreck' (Virilio and Der Derian 1998: 20). This is the 'technological accident', which is always 'local' because vehicles moving relative to one another collide in highly specific locations, restricted in space and time. A qualitative difference emerges, Virilio argues, between these accidents and the accidents created by nuclear and information technologies, which deploy the absolute velocities of electromagnetism. When this occurs, the accident is no longer local but 'general', as radioactive fallout and information circulate globally (Virilio 1997: 70).

Unlike radioactivity, however, the information accident will happen everywhere *simultaneously* because of the 'interactivity, the networks and the globalization brought about by the communication revolution' (Virilio and Petit 1999: 91). As with the Janus-like power of radioactive fission, interactivity too 'can bring about union of society, but it also has the power to dissolve it and disintegrate it on a world scale' (Virilio and Petit 1999: 91). Virilio saw in the 1987 stock market crash, for instance, a harbinger – a 'sign' – of this 'integral', 'global' or 'generalised' accident, responsibility for which he ascribes to the high-frequency trading programs of a highly automated global financial system (Crosthwaite 2011). Since 2007, the ongoing financial crisis has – for Virilio – shown the accident lurking at the heart of the global system of turbocharged capitalism and the 'instant and simultaneous globalisation of affects and fears' caused by cascading failures of financial institutions and the resulting strains on socioeconomic relations (Virilio *et al.* 2008; also, Wilson 2012). In the previous chapter, we encountered Virilio's conception of speed; the accident of technology is also the accident of speed. They are inseparable and integral aspects of the integral accident itself. For Virilio, time itself – the *chronos* of the world – is constructed through technology and is 'rapidly moving to an (apocalyptic) end' (Hutchings 2008: 131).[2]

In the 'Flash Crash' of the US stock exchange on 6 May 2010, the Dow Jones experienced its largest-ever one-day decline, only to recoup those losses within a few hours. Early suspicions that the crash was caused by a 'cyber attack' – launched by persons unknown – were subsequently dismissed in favour of explanations calling into question the nature of algorithmic trading and the positive feedback loops that can develop before failsafe mechanisms kick in or human operators intervene (US Commodity Futures Trading Commission and US Securities and Exchange Commission 2010). Virilio asks a pertinent question of the federal investigation into the crash: 'When you are incapable of detecting the origin of a stock exchange crash and, so, find it impossible to know if it's a cyber attack of some reach by one state against another, or whether

[2] Contrast Virilio's theorisation of the socioeconomic accident with that of his old professor Raymond Aron, who diagnosed of the 'dramatic accident' of the Great Depression that it was 'made possible at the time by the nature of our societies' but was not inevitable (Aron 1984: 224). It could have been avoided by alternative political action, the possibilities of which, under conditions of the technological accident, Virilio mostly discards.

it's a systemic crash that's purely accidental, what do you do?' (Virilio 2012: 79–80). Virilio echoes here one of the key – and most intractable – epistemological concerns at the core of cyber security practice and politics: the 'attribution problem' (Brenner 2009: 79–161; Libicki 2009; Rid 2013a: 139–62; Rid and Buchanan 2015).

The 'problem' is simultaneously evidentiary and technical, normative and legal, political and strategic. It is situated at the juncture between two temporal regimes of commission and response. The first relates to the past: who did it? and why? and the proof thereof. The second concerns the future – what can we do? what must or should we do? and the justifications for those actions. During the Cold War, attribution of a hostile act to its perpetrator was a relatively straightforward issue, but the complexities of a post-bipolar strategic environment introduce fundamental uncertainty to the issue of cyber attacks and their causality. Adversaries can remain anonymous, hide their tracks, falsify identities, mislead investigators, shift blame to third parties and, sometimes, simply refuse to declare their hand. The ability to determine the source and intent of adversarial actions is central to determining the appropriate technical, tactical, political and strategic responses available to an authority charged with cyber security. This is particularly the case at the national level, where governments require a substantial burden of proof before, for example, responding to another state with military action.

There are three notable responses to the attribution problem. The first seeks to resolve the technical aspects of attribution, in order to prove causality through forensic methods and provide a firm legal basis for consideration of further action. The second jettisons the burden of absolute proof – difficult to obtain, if not impossible – by taking into account contextual factors like prevailing inter-state relations and the probable responses of other strategic actors should particular responses be enacted. This is a probabilistic mode of risk management that prioritises the need to respond over the need to determine causality and operates below the threshold of 'reasonable doubt'. Technical attribution is more straightforward: it is forensic, scientific and seeks to establish the empirical 'truth' of causality. Strategic attribution steps into the breach where technical attribution is unobtainable, or requires contextualisation, and is an epistemological suture bridging the gaps between fields of ignorance and knowledge. The principal intent of both technical and strategic attribution is not to trace the causes of a particular phenomenon but to facilitate modes of future action and the category of future action itself. Strategic attribution, in particular, is less about 'truth' than creating the impression that there is a truth at all. Where technical attribution finds complexity, strategic attribution craves simplicity. It seeks to create and exploit the 'strategic ambiguity' (Libicki 2011) that emerges from not naming that truth, whether it is known or not, keeping an opponent or opponents guessing as to one's subsequent actions and intentions.

A third approach shifts focus from the cause of an event to its effects. This involves a change in the risk calculus, from the protective security of information infrastructures to their resilience in the face of attack and compromise.[3] What matters more than establishing the cause of an event is 'the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable cost and time' (Haimes *et al.* 2008: 291). Cyber security is not only about 'strengthening defences' to prevent attacks but also about 'improving resilience and diminishing the impact of cyber attacks' (Cabinet Office 2011: 39). Temporally, this creates a new locus of action and responsibility after the event as well as before it.

In resilience, we find a tentative answer to Virilio's original question about what the search for causality says about the system we inhabit. Both technical and strategic attribution require that a cause be named, even if one is not found, but resilience derogates the issue of causality entirely. It is less important to resilience – and to the notion of the technological 'accident' – whether humans, machines or faulty code bring about the event than it is that these entities are embedded in systems that make accidents unavoidable and inevitable. Given the ubiquity of sociotechnical systems, resilience takes on the distinct inflection of postmodernity: we can only deal with the effects of the world in which we live rather than its causes. The cause is banal because the system is the cause. We know that the accident will occur but we do not know when or what its effects will be. Resilience prepares us for those unknown eventualities but seeks to restore at least a sense of security to a field of epistemological uncertainty (Dunn Cavelty and Giroux 2015). Imagining worst-case scenarios allows us to develop 'cognitive resilience', so that we can learn about what happens 'if the world breaks' (Clarke 2006: 76). Practically, suggests Bruce Schneier, resilience 'is the best answer we have right now': 'We need to recognise that large-scale [cyber] attacks will happen, that society can survive more than we give it credit for, and that we can design systems to survive these sorts of attacks' (Schneier 2013b).

Resilience as a response to an epistemological shortfall discounts causality and intent and implicitly recognises 'an inherent ontological insecurity within computer systems' (Hansen and Nissenbaum 2009: 1160). The pioneering computer scientist Grace Hopper remarked, 'Life was simple before World War II. After that, we had systems' (Schieber 1987).

[3] On the emergence of resilience as a security concept, see Walker and Cooper (2011).

With these systems came 'bugs', two categories of which were soon formalised (Gill 1951). The first arose from faults in the machine itself; the second from input and programming errors leading to poor or nonsensical output, what would later become known in computer science as the 'garbage in, garbage out' principle. Removing all bugs from a large system ('debugging') is, unfortunately for the computer security professional, 'provably impossible' (Edwards 1996: 291; Mackenzie and Pottinger 1997). Not all bugs have security dimensions, but a great many do and can be exploited by those with the will and skill to do so.

No information system can claim to be wholly secure, a condition recognised over four decades ago. In a famous 1967 conference at Fort Meade, Maryland, Bernard Peters of the National Security Agency observed: 'Security cannot be obtained in the absolute sense. Every security system seeks to attain a probability of loss which is commensurate with the value returned by the operation being secured' (B. Peters 1967: 283). We would now recognise this as an equation of risk, but it is also an assertion of the inherent 'insecurity' of information-technological systems. In the light of the technological accident, ICT failures and cyber attacks are both immanent to technological postmodernity. In their eschatological dimensions, the accident and the apocalypse share the same core characteristic of immanence: the catastrophic accident is inherent to complex sociotechnical systems like global ICTs. There is another sense too in which immanence lies not just in the processual interactions of complex systems but in a system that brings into being technologies that contain within themselves the potential for societal catastrophe: the 'producibility of the catastrophe *is* the catastrophe' (Scherpe 1986: 96, original emphasis). This sense of the anthropogenic catastrophe circumscribes postmodernity and the accidents – apocalypses – that may arise. Yet our common comprehension of 'catastrophe' as an embodiment of destructive negativity does justice neither to the fullness of the concept of apocalypse nor to its utility in the analysis of cyber security. The primary sense of apocalypse is not of catastrophe but of revelation and transformation, both qualities that are in some sense 'desired' and which are examined in the following section.

Revelation, transformation and desire

The relationship of postmodernity to time has been characterised by Jean Baudrillard as a reversal, in which time 'is no longer counted progressively, by addition, starting from an origin, but by subtraction, starting from the end', a countdown through which 'the maximal utopia of life gives way to the minimal utopia of survival' (Baudrillard 1997: 448).

Resilience is an expression of this postmodern concern with survival, but contained within this broad statement of societal eschatology is the recognition that apocalypse is not, despite common impressions to the contrary, the end. All apocalypses are passage points leading from one form of social order to another. The nature of the 'post-apocalypse' is not only a staple of popular culture but is congruent with secular and religious imaginings of 'the end'. Apocalyptic fiction is less about the apocalypse than about the world that follows it, whether that be 'paradise or wasteland' (Berger 1999: 6). The apocalypse is not just the end but 'a beginning, an uncovering, an illumination unveiled precisely at the very moment of the greatest darkness and danger' (Aho 1997: 65). The apocalypse is not only a point of transition and transformation but also a process of revelation and, importantly, an object of desire. These three foundational aspects of apocalyptic thinking – revelation, transformation and desire – are the themes of our continued examination of cyber security's discursive relations with the future.

Implicit in Virilio's interpretation of the global financial accident is his characterisation of the integral accident as 'the revelation of the destructive capacity of hyper-modernity for humanity' (Featherstone 2010). Virilio denies any similarity between the accident and the religious apocalypse: the catastrophism he describes has 'nothing in common' with 'the pessimism of the "millenarian" obscurantism of days gone by' (Virilio 2007: 28). This 'new notion of the accident has nothing to do with the Apocalypse', he insists elsewhere (Virilio and Petit 1999: 93). However, he does not dispense with a secular apocalyptic reading of the accident, especially in his insistence on 'exposing the accident' as a way of understanding technologised society and thereby to query and resist its political foundations (Virilio 2007: 29). Virilio understands that 'apocalypse' is not a priori negative and, in its primary sense of 'revelation', apocalypse is a 'singular instant both revealing the meaning of the past and announcing the future' (Bousquet 2006: 756). This, one assumes, is what Virilio means to communicate through the 'exposing' of the accident through the accident itself, a revelation that is intended to be partly positive rather than wholly pessimistic (Hutchings 2008: 141). Virilio has diagnosed his own orientation as concerned less with 'truth and falsehood' than with apocalypse: 'I am not a revolutionary but a revelationary . . . what is revealed forces itself above what is past and forces itself upon our situation as a revelation, as in the case of the integral accident and finitude' (Virilio and Armitage 2011: 39).

In imagined cyber apocalypses, the criticality of 'critical infrastructures' is revealed physically and in its social and political dimensions. Revelation occurs when the mundane functionality of ICT systems is disrupted, whether deliberately by adversaries – as is the principal preoccupation of cyber security – or in the less sensational circumstances occasioned by accident or disrepair. Information technologies like the internet are infrastructures that, etymologically, are the foundations of a greater whole, the 'collective term for the subordinate parts of an undertaking'.[4] In this case, infrastructure is the physical and organisational substructure essential for the maintenance and progressive functionality of society as a whole. 'Infrastructure' is a twentieth-century coinage, but what we today would classify as infrastructures are attested archaeologically, like the diverse examples of the hydraulic systems of ancient Egypt and the Middle East, the *cloacae* (sewers) of early Rome or the road networks of the pre-Columbian Americas. In each case, these infrastructures were not just pragmatic contributions to the common good but symbolic and constitutive of political power and control, as well as being expressive of local cultural cosmologies.

In the modern urban context developed an 'infrastructural ideal', in which centralised infrastructure development and urban planning co-instantiated the harmonious and integrative tenets of modernity itself, 'as Enlightenment ideals of universal rationality, progress, justice, emancipation and reason were applied to all areas of social life' (Graham and Marvin 2001: 41). Infrastructure, even in today's managerial political climate and the decline of the infrastructural ideal (Kaika and Swyngedouw 2000), may still be an expression and source of this civic spirit (Greenberg 1998). Joseph Bazalgette's sewerage system for London, opened in the 1860s and 1870s, is even today invoked as a model for public urban works, including by the incumbent (and classically minded) Mayor of London, whose plans to improve Bazalgette's overloaded yet 'remarkable system' include a new '*cloaca maxima*' for the city (Johnson 2011).

Information infrastructures tend not to be as visible as their counterparts of concrete, steel, brick and tarmac. They are not only just unseen but un-cognised: for most people, the existence of infrastructures is 'more or less imaginary' (Burgess 2007: 476). Like Bazalgette's Londoners, most internet users 'are frequently unconscious of the magnitude, intricacy, and extent of the underground works, which have been designed and constructed at great cost, and are necessary for the maintenance of their health and comfort' (Bazalgette 1865: 3). Infrastructures are ordinarily 'invisible' (Star 1999), and because this applies especially to the hidden world of internet cables, routers, switches and satellites, we often

[4] 'Infrastructure', OED Online, December 2012.

assume that it is ‘as ethereal and virtual as the information and communication that it supports’ (Dodge and Kitchin 2004: 160).

These mundane technologies ‘only come into visible focus as things when they become inoperable – they break or stutter and they then become the object of attention’ (Graham and Thrift 2007: 2). This physical manifestation of ‘virtual’ infrastructures is a key component of the violent scenarios described by apocalyptic cyber security discourses and, following Heidegger (2010: 66–71), is the way through which information technologies – in fact, all objects and things – reveal aspects of themselves ordinarily hidden from view: ‘These entities were once silent and withdrawn, but have now become obtrusive . . . An entity malfunctions and loudly announces itself; later, the entity might retreat into the background and be taken for granted once again’ (Harman 2010b: 19). The personal computer, for instance, is taken entirely for granted until it malfunctions, at which point the ‘trustworthy world’ around it collapses and the machine ‘abruptly demands interaction with itself’ (Verbeek 2004: 79–80, in Graham and Thrift 2007: 3).

We can scale this concern with the proper functioning of information technology to the societal level. In ‘cascading failures’, small events trigger wider and more damaging ripple effects in secondary infrastructures (Rinaldi *et al.* 2001; Little 2002; Grubesic and Murray 2006). This is particularly the case with the ‘negative technological synergies’ created in ‘hybridised’ infrastructures due to the combined effects of deliberate, accidental or latent ‘interference’ between elements of one or more technological systems (Hellström 2003, 2007). In information infrastructures, failures thereby catalysed will ‘escalate rapidly beyond control before anyone understands what is happening and is able to intervene’ (Dunn Cavelty 2008: 18). Cascading failures are a core component of imagined scenarios of cyber and wider infrastructural failure. For instance, cascading failures in an urban environment would reveal the coupling of electrical and electronic infrastructures in its messy complexity. The electrical grid enables information infrastructures, which in turn support other infrastructures, as well as acting as control mechanisms for the electrical grid itself. Whether by accident or by design, the failure of the electrical system reveals both its own self and the fact that all other infrastructures rely on it (Bennett 2010b: 36; Byrd and Matthewman 2014). In turn, the ‘virtual’ social spaces and information flows enabled by the material substrate of the internet are exposed in their fragility and precariousness. The ultimate revelation is the extent to which societies are both technologically and cognitively dependent upon ICTs, the ‘invisible global infrastructure serving as a global nervous system for the people and processes of this planet’ (Kleinrock 2003: 11).

Catastrophic infrastructure failures also reveal aspects of temporality that ordinarily remain hidden and – literally – unthought. Time is always embedded in objects and artefacts, in which are enfolded ‘heterogeneous temporalities’ (Latour 2002: 248–9; Hodder 2012). When the space shuttle Challenger exploded in 1986, it allowed the official investigators – and the curious public – the opportunity to retrace the material and immaterial developments through which this remarkable object came into being. Such accidents are, according to Bruno Latour, another ‘way of hearing what the machines silently did and said’ (Latour 1992: 233). Failures not only reveal the bureaucratic and material histories of objects and the assemblages in which they are networked, but they also draw attention to the temporality of the present. In London, the high leakage rates and bursting pipes of Bazalgette’s ageing sewers have in our own time brought into focus problematic aspects of utility privatisation, consumer confidence and corporate remuneration (Kaika and Swyngedouw 2000: 136). Although Y2K was not nearly as catastrophic as many predicted, its problematisation revealed a ‘hangover from previous decisions made in the growth of a system’ (Hodder 2012: 100). In similar fashion, the prophesied cyber security apocalypse would reveal the historical failure of governments and businesses to take cyber insecurity into proper account, and for which catastrophe is the price. Moreover, because catastrophes often come ‘covered in the fingerprints of organised silence’ (Keane 2012), accidents often reveal the hidden politics that allow catastrophes to develop and, like Deepwater Horizon and Fukushima, literally explode into public consciousness.

In its reliance on the revelation of what is wrong, apocalyptic thinking inherently allows for the complementary disclosure of what can be made right. This is the transformative message of all apocalypticism, in which the revelation is both of the passing of one problematic social order and of the advent of a new one. The ‘prophetic method’ proposes visions of a transformed social order in defiance of ‘official’ versions of reality but discounts the past in favour of the future. In understanding the world ‘in terms of what is to come rather than what has been’, writes sociologist David Bromley, ‘the future is given greater eminence, and both past and present recede in importance’ (Bromley 1997: 36). Moreover, very often the present is consequently ‘reduced to simply a gateway moment leading to the future’ (Bromley 1997: 36). However, apocalypse is also a necessary event, without which a better future will not arrive; not only is the future desired, but so too is the apocalypse. Without a cataclysmic ‘cyber’ event, many argue, governments will not respond sufficiently to the cyber security problem (Bliss 2010; Goldsmith and Hathaway 2010).

This is a catastrophic form of apocalypticism, rooted in ‘a pessimistic evaluation of human nature and society [and] in the pervasive human tendency to think in dualistic categories’ (Wessinger 1997: 50). It is hardly surprising to find catastrophic apocalypticism in politics, which is not ordinarily inclined to representing the subtleties of human nature in its pursuit of power, and in security, which, as already suggested, is shot through with dystopian visions of the future conditional on bad things always being done by bad people. This Hobbesian inflection is evident in the assertion that the biggest global cyber security challenge is preventing *bellum omnium contra omnes* in cyberspace (Hughes 2010; Forsyth 2013). To do further violence to Hobbes, these are visions of a ‘perpetuall cyber warre’ of all against all. Where, wonders one author, is the Leviathan empowered by citizens to deliver us from this parlous state of nature? (Kaminski 2010).

For some, the interminable wait for the apocalypse is an unacceptable frustration and they attempt to bring the future into the present by initiating the apocalypse themselves (Rapoport 1988). In recent history, we can detect this autopoietic apocalypticism in American reactions to 9/11 as obviously as in the jihadist beliefs of those who prosecuted the 9/11 attacks themselves (Lewis 2012: 12). Utopian belief in apocalyptic transformation of human affairs through catastrophe informs the avoidable tragedy of the subsequent ‘war on terror’ as strongly as it does impossible dreams of a global caliphate (Gray 2007). Aside from these obvious attempts to effect social change through apocalyptic violence, it is demonstrable historically that although the apocalypse may never arrive, ‘true believers’ often succeed in one specialised sense: ‘the world is a different place after them’ (Landes 1998: 2, in Tapia 2003: 484). The Y2K ‘technocalypse’ did not happen in the manner prophesied, for instance, but it did catalyse political, technical and social changes to extant practices and beliefs, not least by implanting ‘seeds of technological doubt’ in mainstream culture (Tapia 2003: 509; also, Eriksson 2001). Concerns that similar intercalary time and date problems may occur in computer systems in 2038, 2042 and 2107 are mediated partially through ‘lessons learnt’ from the ‘non-event’ of Y2K, as are other processes that alter the *chronos* of internet time (Kamp 2011). Non-catastrophic events can have material and cognitive effects just as enduring as catastrophes (Erikson 1994; Williams 2012).

Imagining the future

Cyber security futures are imagined and represented through ‘events’ that illustrate the present insecurity of information infrastructures. The recent past is read as a series of 'event-signs' that presage the forthcoming catastrophe and constitute a narrative of political 'failure to secure'. Beissinger notes, however, that not all events are equal and some 'fail to exercise much of an impact at all or are barely noticed' (Beissinger 2002: 15). The ecology of cyber security is one in which millions of events of 'insecurity' happen daily: automated malware and human actors exploit multiple vulnerabilities, events which, while of immediate concern to the information security professional, may not rise to the level of a collective security issue unless identified and communicated as one. Diverse studies have shown that cyber security has a history of securitisation, in which these events – and the broader processes they help structure – are translated from the mundane realm of technical security to the 'higher' levels of economic, national and existential security (e.g. Nissenbaum 2005; Hansen and Nissenbaum 2009). The apocalyptic framing of cyber security discloses the construction of a distinct category of large-scale 'cyber' events that exist in the speculative future but act also in the present. The threat of apocalypse is 'real and ever-present and folds future potentiality into the present' and the security practices that emerge are 'a kind of death-dance, a ritual in which future catastrophe is mimed and theatrically composed in order to ward off crises' (Martin and Simon 2008: 294).

Were such an event to occur, we might characterise it as an accident *sensu* Virilio, or as a 'global event', as proposed by James Der Derian. This is an 'unfavourable symptom' of a contemporary information-technological condition, 'a disruption in the predictable flow of events, a breakdown of the present en route to the past, a rude awakening into the contingency of the future' (Der Derian 2001: 674). Beissinger quotes the historian William Sewell to the effect that some events have a 'transformative power' beyond the politics of government alone, shaping history and 'changing people's possibilities for meaningful action (Sewell 1990: 548, in Beissinger 2002: 15; Berenskoetter 2011). In the global accident/event, we must wonder at the possibilities for meaningful action, given the genesis of the cyber apocalypse in the belly of technological postmodernity. Resilience, for example, is presented as a *fait accompli* in the face of the immanent accident and characterised by a fatalistic acceptance that we cannot change the world, thereby closing down vectors of possible political agency (Bourbeau 2013). It is also an attempt to foster policies and practices that would enable a tolerable level of post-catastrophic survival and might be considered in a more positive, and possibly emancipatory, light (Chandler 2012). Resilience and, perhaps, the cyber apocalypse itself are attempts to generate 'new understandings of time and temporality with which to conceptualize both our precarious predicament and a possible escape from a seemingly inevitable dystopian closure' (van Loon 2000: 347–8).

The reading of apocalyptic postmodernity informing this discussion is in keeping with the historical tendency of apocalyptic belief to find multiple contemporaneous modes of expression (Cohn 2004). There is no singular body of theory, outstanding political movement or exemplary form of cultural practice that embodies this apocalyptic aesthetic *in toto*, but there are many vectors of the aesthetic itself. This chapter has argued that cyber security is one such vector, even if this analysis exhausts neither the concept of apocalypse nor the futurity of the cyber security imaginary. It may be more fruitful to think of this preoccupation with finitude and existential crisis not as the dismantling and ultimate disposal of *telos* but as 'the beginning of the infinity of heterogeneous finalities' (Lyotard 1987: 179). The core characteristic of this diverse postmodernity is the apocalyptic 'destruction of the symbolic order', whether coded as 'God, metaphysics, history, ideology, revolution, and finally death itself' (Scherpe 1986: 98–9). Or, if this symbolic order is contemporary politics, blamed by prophets of cyber apocalypse for inaction and inadequacy in the face of existential threat. People tell these stories not only in order to shift the blame onto other parties but so that they can present themselves as the ones with the ability to implement the necessary solutions to given problems (Stone 1989). This desire for political transformation is surely at the heart of the apocalyptic narrative through which cyber security futures are so often imagined. Desire is not only an urge or a means of informing action, however, but a powerful means of constructing the political subject (Solomon 2014; see also, Nishimura 2011). Desire is an expression of sociotemporality that stabilises the individual and binds her together with others and sustains the 'predictability of intention' (Ruggie 1975: 570) so necessary to collective political action.

The poet Octavio Paz identifies accidents in the Virilian sense as 'cogs of the historic order' (Paz 1974: 112; also, Der Derian 2001). This chapter has explored the construction of the future order but has yet to examine in any detail the mobilisation of history as a way of understanding cyber security presents and futures. We have identified historical events as 'signs' leading to the cyber apocalypse, but by their nature none attain the practical or symbolic level of catastrophe. However, cyber security discourses do make clear reference to historical 'catastrophes' in order to analogise particular aspects of cyber security, some of which we have touched on cursorily in this chapter. The next chapter considers the role of these analogies and deeper history in the making of cyber security and how this can help us illuminate further the chronopolitics of cyber security.

5 Arguing through the past

Past, present and the appeal to history

In Chapter 2, we encountered numerous difficulties in ascribing definitive ontological status to past, present and future. It is not necessary to rehearse those arguments to accept that from the perspective of subjective human experience the past in some sense happened 'before' the present. Our phenomenological engagement with the 'arrow of time' means that, care of another spatial metaphor, the past is behind us and the future ahead.[1] Our common experience is that this is always so and our customary apprehension of time is that the past exists as something inviolate and unchangeable; it is 'closed', in contrast to the 'open' present and future. This is an expression of the temporality of formal modernity, a linear and mechanistic time theorised by Newton and materialised in the clockwork assemblages of capitalist production. It informs the conceptual framework through which other, usually non-Western, societies and cultures are characterised as temporally 'backward' Others, whose political agency is suppressed by their dwelling in an immobile and immutable past.

To be accused of 'living in the past' is to fall foul of one of the commandments of modernity: 'thou shalt not commit anachronism' by failing to recognise the 'radical distinction' between the present and the past (Hindess 2007: 330). Western environmentalism, for instance, seeks 'an unrealistic spatiotemporality' differentiating change and stability as ontologically exclusive entities, through which the past is constructed as 'a timeless, ahistorical refuge for virtue' (Cannavò 2012: 866). Such an imagined past is outside of history, narratives about which ignore that the past is continually remade in the present as part of the normal operations of historical change (Jordan 1995: 283). For most purposes, it matters little if there is or there is not a physical 'world' called 'the past' with which

[1] Unlike physical equations, in which the 'future and the past seem physically to be on a completely equal footing' (Penrose 1989: 392).

we might possibly co-exist if our primary experience of the past is as an individual and collective construct in the social present.

For the furthest reaches of the past, material remains provide us with clues as to the nature of the world in those earlier times. The early modern 'discovery' of a geological 'deep time' was a key development in the contextualisation of human existence within the immense duration of cosmic time, as important a cognitive reorientation as the later revelations of relativity and quantum mechanics (Toulmin and Goodfield 1965: 141–70; Gould 1987). Geology revealed that religion and myth might not be the most accurate guides to the past, loosening the grip on the Western imagination of literal readings of the Judaeo-Christian creation. For the prominent Victorian critic John Ruskin, the geologists' 'dreadful hammers' chipped away at the authority of Christianity itself: 'I hear the clink of them at the end of every cadence of the Bible verses' (Klaver 1997: xi). In the nineteenth century, antiquarians applied geological techniques to the history of humankind itself, excavating evidence that subverted narrow interpretations of ancient remains in Egypt and Near East that seemed to corroborate Biblical narratives. Eventually, the weight of scientific evidence became too much for all but the most ardent literalists to ignore: the Old Testament was a story of doubtful authenticity and one restricted to a 'rather minor strand' of human history (Toulmin and Goodfield 1965: 238). Moreover, the new 'science' of archaeology added the 'testimony of things' to the textual evidence and irrevocably undermined simplistic, linear models of historical progress (Toulmin and Goodfield 1965: 237).

For archaeologists, neither things nor the pasts from which they originally derive are fixed or stable. Archaeological artefacts are surprisingly durable – and must be so for them to re-emerge 'artefactually' in the present – but their meanings change through later reuse and reinterpretation and are never fixed. Artefacts are *things*, contingent assemblages – 'heterogeneous bundles' – of matter, information and energy, entangled in a web of connections with other things, not least the particular species of thing we call 'human' (Hodder 2012: 8). This dynamic approach to thingness is consistent with an interpretation of the archaeological record as not cleanly demarcated from the archaeologist. Gavin Lucas observes that it is difficult enough to interpret the 'resurrection and irruption' of artefacts into the present, without insisting on an artificial boundary between past and present (Lucas 2005: 36–7). Like the present, the past is an assembled temporality of events and durations, which includes the past *and* the present (Lucas 2005: 38).

We might even argue that all archaeology, even if it is *about* the past, is actually *of* the present. Integral to this perspective is that the past is interpreted in the present. We might begin to understand the original functionality or meaning of an artefact discarded millennia ago, but we can never escape our own interpretive subjectivity in the present. Laurent Olivier notes that 'archaeology does not exhume parts of history that took place before and outside of it [but] directly contributes to the construction of this history by inscribing them in the present' (Olivier 2011: 60). It follows that interpretation of the archaeological record can be directed towards particular ends, including the political. The role of archaeology in the construction and maintenance of national identity has a long history, including the promotion of ethnically charged constructions of distinct European 'cultures', of which Nazi Germany's self-promotion through the work of archaeologist Gustaf Kossinna remains perhaps the most uncomfortable assertion of cultural-historical superiority (Trigger 1989: 163–7). This approach continues to manifest, particularly when people seek 'to glorify the "primitive vigour" and creativity of people assumed to be national ancestors rather than to draw attention to their low cultural status' (Trigger 1989: 174). In late twentieth-century Europe there were conscious political moves to develop a pan-European Celtic heritage as a foundation of the modern and future Europe, including in countries like Spain not normally considered 'Celtic' (Díaz-Andreu 1996). Even the recent exhumation of the remains of English King Richard III, which sparked a legal challenge by his supposed 'descendants' over their right to decide the location of his re-burial, can be read in terms of identity politics (Arnold 2014). We might consider these dynamics orthogonal to the temporal Othering identified by Fabian (2002) and others: rather than seeking to exclude people of the present they seek to include people of the past. Rather than denying coevalness, these political moves impose contemporaneity across the centuries.

Given its potential for political manipulation, archaeology is 'a discipline almost in wait of state interference' (Kohl and Fawcett 1995: 8). So too is history, in which the past is always remade in the political present in order to shape the future. 'Does the past exist concretely, in space?' asks Winston Smith's torturer in George Orwell's *Nineteen Eighty-Four* (Orwell 1965). 'Is there somewhere or other a place, a world of solid objects, where the past is still happening?' he continues. Smith replies under duress that there is not, and that the past only exists in records and in memories, records and memories that the Party wishes to convince him are controlled exclusively by them. But the torturer detects in Smith a hidden belief in the existence of a reality outside of the Party, a reality that might afford the possibilities of individual human remembering, and is reminded that reality only exists in 'the mind of the Party, which is collective and immortal. Whatever the Party holds to be truth, *is* truth.'

The past is the sole preserve of the Party, to be remoulded in the image of their politics, as encapsulated in the fictional Party slogan now normalised in our own culture: 'Who controls the past controls the future: who controls the present controls the past.'

The political gaze, like sociotemporality itself, therefore extends into both the past and the future as a way to achieve symbolic and material ends through the manipulation of constructed and imagined histories. The uses of history and appeals to the past are at the core of the construction of statehood and nationhood (Anderson 2006). As Carmen Leccardi observes in her discussion of movements of resistance to the clock time of global capitalism and the vertiginous pace of hypermodernity, these are more than just politics through which to conceive possible futures. They emphasise the contingent relations between past and present, in particular 'the strategic question of memory: the teleological chains linking the past to the present' (Leccardi 2007: 33). This chapter intends to excavate some of these 'chains' linking the past to the cyber security present in the service of futurity and to augment the developing picture of the temporality of the cyber security imaginary.

The previous two chapters have put forward two propositions with respect to the temporality of cyber security. Chapter 3 proposed that cyber security is sufficiently preoccupied with the uniqueness of the present that it tends to ignore both its own history and the historicity of the present. In Chapter 4, this concern with the present was revealed not as a baseless preoccupation with the 'now' but as a response to the future, a form of eschatological thinking in which the future conditions the political imperatives of the present. In each case, there appears to be little engagement with the past, except as a source of 'signs' that corroborate apocalyptic narratives and which confirm the likelihood of forthcoming cyber catastrophe. These 'events' are collectively shaped into a narrative of past 'cyber insecurity' that cyber security must overcome in order to avert even more insecure futures, thereby acting as a quasi-historical resource for the political promotion of cyber security.

We can see a similar process at work in the selective peppering of the UK cyber security strategies with brief case studies and statistical factoids. Culled from industry, media and government reports, these data are used to illustrate particular arguments in the main text and represent highly formalised and decontextualised interpretations of events and processes in the recent past. In contrast to the signs of apocalypse discussed previously, they are often used to illustrate positive as well as negative aspects of the use of ICTs for government, business and society that will be enhanced or assured through the policies proposed in the remainder of the document. Often, they are data points rather than events of enduring historical interest and are often out of date by the time of publication, although this is hardly unusual or unforgivable in discussions of contemporary ICTs. However, they do not contribute historical knowledge to our understanding of the present but instead adhere awkwardly to the principal narratives of these documents as statistical and anecdotal ballast.

Is there really such limited interplay between cyber security and the past? Can cyber security as an assemblage of political and technical practices be so selective and perhaps even amnesiac about the past, or are deeper connections with the past decipherable in political discourses of cyber security? The foregoing examples illustrate that there is no definitive break with the past but a patrolled boundary across which only selected 'facts' may pass, plucked from recent history for narrative purposes. In the examples examined previously, events of the recent past are not the only ones that become part of the narrative present. Long histories of Judaeo-Christian culture are sedimented in the figurative constructions of future cyber catastrophe as 'Armageddon', with its allusions to the real entity of Tell Megiddo in Israel and the battles that occurred there in the second and first millennia BC. The apocalyptic reading of Megiddo as the future site of Armageddon is fanciful and not supported by scripture or doctrine but the *sense* that Armageddon is tied to a specific place and past events is a powerful one and will escape few who use the term seriously. Those who warn of 'cybergeddon' are not deliberately invoking the spirit either of ancient wars against the Egyptians or of a literal Armageddon still to occur, but there are multiple historical layers of cyber security discourses, even if etymology is often subordinate to more contemporary inflections and available meanings.

The language of 'cybergeddon' and 'cyber-apocalypse' is freighted with past meanings and connotations and is usually avoided by public officials: elected politicians, civil servants, senior security personnel and military officers tend not to deploy language that is so obviously hyperbolic, even if, as argued in the previous chapter, their discourses remain strongly apocalyptic in tone if not in obvious intent. No similar restraint applies to those answerable to shareholders rather than voters: media and industry reports and commentary are the principal loci of overtly apocalyptic discourses, including the contributions of those who were once but are no longer in public service. This might imply there are normative constraints on Western public officials deploying Biblical-sounding apocalyptic utterances, but this, historically, is not the case at all.

For instance, the millennialism of US president Ronald Reagan is a matter of record, as are the beliefs and public statements of officials during his administration (Wojcik 1997: 29–30). In common with other millennialist Christians, Reagan was keen to garner the spiritual bounties promised to the true believer and, with his finger on the metaphorical button, was in a better position than most to ensure the Armageddon of divinely sanctioned nuclear war that would deliver them (Cook 2004). 'It is later than we think', he remarked, in direct reference to the temporal proximity of the end times (Chandler 1985: 1), although he would later claim not to have allowed his eschatological beliefs to influence policy decisions or plans for nuclear war (Boyer 1992: 42). With the passing of Reagan and the Cold War, millennial rhetoric of this nature seems to have faded from high-level political discourse and become one with the general apocalyptic underpinnings and more subtle expressions of eschatological postmodernity. For all its overt 'born-again' Christianity, the Bush II administration did not attempt to resurrect Reaganite language of this kind, either in marshalling support for the 'war on terror' or to justify its ongoing prosecution, despite its many allusions to 'holy war' and the divinity of its mandate (Jackson 2005: 103–5; McLaren 2002).

Analogies, especially of war, are a commonplace of political speeches and help to explain in culturally intelligible terms particular aspects of the present situation or of catastrophes yet to happen. On one level, there is the simple metaphor of war to describe the present Hobbesian cyber security situation of 'cyber war' of all against all (Hughes 2010). 'We are currently at war', reported BBC's *The One Show*, 'on a battlefield we can't see, with weapons most of us know nothing about' (BBC 2012). 'Britain is under attack, constantly, every day', Sky News told its viewers a month later, 'but most of us would never know. This is the cyber war; not a new conflict but an ever-developing battle' (Sky News 2013). This campaign is proceeding badly for the home side, as it is a battle that 'the British government and military isn't winning but is containing. Just' (Sky News 2013). Other influential voices go a step further, one former senior intelligence official stating, the 'United States is fighting a cyber-war today, and we are losing. It's that simple' (McConnell 2010). We read of a 'hidden battle' in cyberspace, a report to the US president stated in 2008, referring to the Allied code-breakers of World War II: 'It is, like Ultra and Enigma, a battle fought mainly in the shadows. It is a battle we are losing' (CSIS 2008: 11). Stretching historical tolerance a little further, 'We are in a "Hundred Years War" against formidable, adaptive, and creative opponents . . . The war will be a struggle for the survival of a way of life' (Hall 2003: x–xi).

These latter examples are *historical analogies*, which 'signifies an inference that if two or more events separated in time agree in one respect, then they may also agree in another' (Khong 1992: 6–7). Politicians might wish to avoid the slightly hysterical language of Armageddon and religious apocalypse, but less caution exists in their invocation of historical events and processes in political cyber security discourses. The security orientation of this rhetoric means that historical events mobilised for contemporary political purposes are also usually 'security events', the most common being 9/11, the Cold War and Pearl Harbor, an extended discussion of which forms the basis of the two main sections of this chapter. With respect to cyber security, the principal issue is not – as policy scholars like to debate – whether the analogies used are 'accurate' but what purposes the deployment of historical analogies serve: what is the 'value' assigned to them? (Coker 2013: 184). Given their highly mediated nature, these processes also deploy 'media templates', in which historical events are 'key reference points' used analogically to 'encourage a particular understanding' of new events (Kitzinger 2000: 75).

The focus of this chapter is not on the failures of historical analogies but on their 'success'. The political work they perform helps to explain why this form of argument and justification persists, despite the often seemingly inappropriate use of particular analogies. It is not that politicians are ignorant of history, an assumption sustaining the strategic studies literature in particular, in which the proffered solution is managerial: educate politicians and their staff so that they can learn 'to use history more successfully' (Khong 1992: 12; Neustadt and May 1986). Politicians are often keenly aware of the limitations of their chosen analogies but choose to pursue them for their utility in ways that aid policy and political decision-making. We might not be able to quantify the political efficacy of these analogies, but we can begin to see how they might be effective, although this is not the primary intention of the current exercise. Rather, the aim is to explore how the use of history in cyber security discourses expresses temporal aspects of the cyber security imaginary: what does the use of history say about the temporality of cyber security and how does it shape its politics?

Provocative politics

On 8 December 1941, a day after the Japanese attack on the US naval base at Pearl Harbor, Hawaii, President Roosevelt went before a joint session of Congress seeking assent for a declaration of war against Imperial Japan, a request duly granted by the assembled legislators. The president described the previous day's events as 'a date which will live in infamy', and his short address is widely considered one of the most important political speeches of the twentieth century. Not only did it precipitate US involvement in World War II, but both attack and speech were subsequently central to the continual remaking of American national identity. Emily Rosenberg notes in her exemplary study of the construction of Pearl Harbor that in American memory, 'the near-sacred symbol of Pearl Harbor ... "lives" in a thousand guises and symbolizes dozens of often conflicting historical "lessons"' (Rosenberg 2003: 5–6). The repurposing of the memory of Pearl Harbor is symptomatic of its status as 'a figurative site of contested meanings where power is exerted and challenged' (Rosenberg 2003: 6). Pearl Harbor lives 'less as a specific occurrence in the past than as a highly emotive and spectacularized icon in an ongoing present – always in interaction with the mediated representations that constitute memory/history' (Rosenberg 2003: 7).

As Rosenberg and many others have pointed out, 9/11 was recast rapidly as a new 'day of infamy', President George Bush even writing in his personal diary: 'The Pearl Harbor of the 21st century took place today' (Woodward 2002: 37). President, politicians, press and pundits were ready and eager to equate Pearl Harbor with 9/11, portraying 9/11 as an act of treachery and as an 'act of war', and framing the coming American response as 'saving the world' once more from a perfidious and inhuman foe. Thus was 'resurrected the sense of a divine mission' through 'the reiteration of innocence violated, the language of trauma, and the expression of the need for retaliation against a faceless enemy who has come to resemble earlier evildoers in the saga of Western civilization against barbarism' (Landy 2004: 86).

The transformation of Pearl Harbor into an allegory for the present is indicative of its continuing ability to inspire a range of emotions and reactions congruent with the American identity and mythos it has done so much to shape. Responses to 9/11 comprise probably the largest assemblage of analogical uses of Pearl Harbor since the original event, but the most consistent deployment of Pearl Harbor as historical analogy is in cyber security discourse, where it has been in regular use for over twenty years (Conway 2008: 117; Dunn Cavelty 2008: 130). Whereas 9/11 demonstrably did happen – even if conspiracy theorists contest otherwise consensual narratives of causality and representation – cyber security constructs its interpretations of Pearl Harbor with reference to future catastrophic events like those imagined in the previous chapter, which have yet to happen, if they ever will.

The earliest reference to an 'electronic Pearl Harbor' appears to be by information security specialist Winn Schwartau, 'the rock manager-turned-preacher of "information warfare"' (Bendrath *et al.* 2007: 57). In an op-ed for *Computerworld* magazine in January 1991, Schwartau wrote that for 'a motivated individual or organization, an assault on our information processing capabilities would be an effective attack on a global Achilles Heel, an electronic Pearl Harbor' (Schwartau 1991b: 23). Schwartau continued to popularise the term throughout 1991, including in testimony to a US Congressional Subcommittee on 27 June, which he claims to have told: 'Government and commercial computer systems are so poorly protected today they can essentially be considered defenceless – an electronic Pearl Harbor waiting to happen' (Schwartau 1994: 43).

Other authors connect early use of the term to D. James Bidzos, president of computer and network security company RSA, who was reported in 1991 as saying there was 'no assurance that foreign governments cannot break the [US government's digital standards] system, running the risk of a digital Pearl Harbor' (Berinato 2003: 72). However, Schwartau's long-standing claim to have coined the phrase was bolstered by the publication, in the same month as his Congressional testimony, of his first novel, *Terminal Compromise* (Schwartau 1991a). This plot-driven and thinly disguised chunk of policy exhortation refers to both the historical Pearl Harbor and its electronic counterpart, concepts that come together in the title of the novel's post-9/11 reissue as *Pearl Harbor Dot Com* (Schwartau 2002). In the novel, the villainous Japanese Homosoto plots against the United States, intending to avenge the death of his family at Hiroshima and to assuage his own shame at being *hibakusha*, a survivor of the nuclear blast. The historical Pearl Harbor plays a constitutive role in Homosoto's own thought: 'We may have lost after Pearl Harbor', he says, 'but we won with the transistor radios and VCRs. The war is not over.' The forthcoming 'Electronic Pearl Harbor' would be 'the ultimate cyberwar attack against the United States' (Schwartau 2002: 442).

Since its inception, variations of this term have been used with 'startling frequency' to conjure up 'images of a sudden crippling blow against critical infrastructures resulting in chaos and destruction' (Conway 2008: 117). By 1997, it was considered the 'most common analogy' in US military planning discourse, in which it represented a future event that would sever front-line soldiers from their informational life-support systems (Partridge 1997). By 2003, the term was described as 'bromidic', so frequently was it used and so attenuated had its meaning become (Berinato 2003: 73). Former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism Richard Clarke changed the target set compromised by these attacks to include private companies as well as government and military assets (Clarke 1999; Sarkar 2002). These statements pluralised the previously singular 'event' and located them across multiple sectors, altering the presentation of the relations between cyber (in)security and the state. The integrity of the historical event is subverted still further by reference to the possibility of multiple 'small-scale' digital Pearl Harbors (Geers 2009: 4; NPR 2010).

Clarke, for example, asserted that ‘digital Pearl Harbors are happening every day’, an idiosyncratic leap of illogic too far, which all but destroyed any sensible use of the metaphor (Berinato 2003: 73). By 2011, the phrase had become, in understated academic language, ‘rather stale from overuse’ (Spellman and Stoudt 2011: 124).

In the autumn of 2012, its stock rose again, with US Defense Secretary Leon Panetta using it in a high-profile speech to business executives to articulate a familiar ‘cyber doom’ scenario:

> The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability. (Panetta 2012)

The speech was widely reported but with little critical comment, save for that implicitly recognised in the Pentagon’s denial that the defense secretary’s words were in any sense hyperbolic (Bumiller and Shanker 2012). Panetta had deployed the analogy on at least two previous public occasions – before a House intelligence committee in February 2011 (when director of the CIA) (Daniel 2011) and during his confirmation hearing as defense secretary in June 2011 (Mulrine 2011). His use of the phrase only attracted widespread attention at the end of 2012 and into 2013, as he continued to use it to illustrate the hypothetical American vulnerability to a massive and debilitating cyber attack (e.g. Panetta 2013). Panetta’s is perhaps the most high-profile use of the phrase and it is notable that other high-ranking officials have refused to use the Pearl Harbor analogy. Howard Schmidt, who in 2009 would become President Obama’s cyber security ‘czar’, expressed his dislike of the phrase in his memoirs, albeit without explaining why (Schmidt 2006: 160). One of Washington, DC’s most astute cyber security commentators and policy advisers, James Lewis of the Center for Strategic and International Studies, has long been opposed to overuse of the Pearl Harbor analogy: ‘it would be nice if the phrase went away’, he said after Panetta’s comments, ‘but it seems to be stuck’ (Clayton 2012b; Lewis 2003, 2005).

Critics of the Pearl Harbor analogy populate two principal categories. The first aims to dismiss the notion of future catastrophe entirely and is intent on ‘debunking’ what is seen as a wider symptom of faulty logic and political self-interest. The second is determined to show where the analogy fails and suggests alternative ways of conceptualising the relevant issues. Panetta's determination to breathe new life into the 'stale' Pearl Harbor analogy was in part successful if we are to judge by the volume of reactive commentary his remarks elicited, examples of which fall into both categories of criticism. In the first category, some, like Russia Today, rejected Panetta's 'scare-mantra' as outright fear-mongering and part of a concerted campaign of American 'scare tactics' intended to give 'Washington bureaucrats greater control over what happens online in the US' (Russia Today 2013). Writing in *The Guardian*, Glenn Greenwald expressed similar sentiments, identifying Panetta's use of the analogy as the culmination of a process of 'fear-mongering rhetoric from government officials [which] has relentlessly intensified, all devoted to scaring citizens into believing that the US is at serious risk of cataclysmic cyber-attacks from "aggressors"' (Greenwald 2013). This echoes an earlier academic statement that the analogy works 'to manufacture fear in the simplest and most direct way possible' (Conway 2008: 117). Greenwald was correct to note that the defense secretary failed to report that the United States is still the only state (in probable partnership with Israel) known to have launched a sophisticated cyber 'weapon' (Stuxnet) against another sovereign entity. In this light, US complaints about foreign aggression ring rather hollow, an omission noted by other commentators, including *The Financial Times* (Dyer 2012).

In the second category, John Arquilla's op-ed in *Foreign Policy* magazine took Panetta to task for his choice of the 'wrong metaphor', offering instead a vision of the internet as analogous to the North Atlantic shipping lanes under assault from German naval forces in 1942 (Arquilla 2012). Thomas Rid also noted in an essay that there have been no cyber events bearing 'any resemblance to World War II in the Pacific' (Rid 2013b). As far back as 1999, Arquilla, professor of defense analysis at the US Naval Postgraduate School and a veteran of debates on strategy and information technologies, had urged the United States to discard 'digital Pearl Harbor' as the central metaphor of strategic thought, offering an alternative metaphor, 'a "Manifest Destiny" for the information age' (Arquilla and Ronfeldt 1999: 75). This idea was neither elaborated nor its possible ramifications examined, but it is hard to see how this metaphor is any less problematic than that of Pearl Harbor. From its initial coinage in the 1840s, '[i]t meant expansion, prearranged by Heaven, over an area not clearly defined' (Merk 1995: 24). US statesman Carl Schurz observed in 1893 that when the cry of 'manifest destiny' is raised, it creates 'the impression that all opposition to such a project is a struggle against fate' (Schurz 1913: 191). Use of the term has negative connotations of divinely sanctioned

American imperialism and territorial expansion and an American intolerance to dissent against that narrative. This is especially pertinent because accusations have for a long time been levelled against the United States that it is attempting in some fashion to 'colonise cyberspace' through normative, commercial, military and other means (e.g. Saco 1999). However, it illustrates further that influential persons often seek analogies in order to frame speculative cyber security futures in terms drawn from the non-cyber security past.

Most discussions of cyber security at some point mention the Pearl Harbor analogy and many identify reasons why it fails to illuminate particular technical and strategic aspects of cyber security. This is to be expected; as Arquilla concedes, 'no metaphor can address every aspect of a problem' (Arquilla 2012). Given that the Pearl Harbor analogy in cyber security has always attracted hostility, if not outright ridicule, we should perhaps assume that Panetta and others were not ignorant of this when they used it. This implies a degree of deliberateness in their choice of analogy and the likelihood that those who use it are aware of its rhetorical force. They may also recognise the cognitive work the analogy advances, rather than dwell on the inaccuracies of the analogy itself with respect to the historical record and geopolitical context. Possibly the most extensive engagement with the term is a 2003 article in *CIO* (*Chief Information Officer*) magazine by journalist Scott Berinato. Berinato reviewed the historical and conceptual use of the phrase and – perhaps unsurprisingly, given the depth of his analysis – found it lacking. He argued that most of the scenarios painted by policymakers and others do not rise to the level of a Pearl Harbor for the simple reason that they fail 'to inflict significant, collective psychological damage' (Berinato 2003).

Berinato outlined five requirements for something to qualify as an event of Pearl Harbor magnitude. One, it would disrupt the back-up systems that would ordinarily mitigate the effects of large-scale cyber incidents. Two, it would lead to cascading failures in networked infrastructures. Three, its effects would continue for many weeks. Four, the vulnerability responsible would be determined after the event, which would lead to, five, the public revelation that 'the loss of property and life was completely and absolutely and tragically avoidable'. At this 'exposure of negligence to the public', security would start to improve as public outrage led to litigation, regulation and the imposition of security standards on the public and private sectors. Given the previous discussion of catastrophe in Chapter 4, we can again see the apocalyptic consciousness at work. The digital Pearl Harbor is an event – or a series of tightly bound events constituting an 'accident' or apocalypse – marking the end of one world and the beginning of another. The current world is one in which politicians pay insufficient heed to security experts and software manufacturers and systems designers ignore important security issues. Catastrophe is inevitable and imminent, but it is necessary in order to shock relevant parties into constructive action, always in the direction of more and better cyber security. The digital Pearl Harbor is transformative and, because of the belief in a positive, post-Pearl Harbor future, both desired and desirable.

Jason Healey, director of the Cyber Statecraft Initiative of the Atlantic Council of the United States, responded to Leon Panetta's use of the Pearl Harbor analogy:

> While the possibility of a catastrophic first cyber strike is indeed not a new idea – and likely fails to capture just what such an attack would be like – Panetta is using this loaded phrase to startle people, to convince them we are not paying enough attention to our cyber problems. (Healey 2012)

Healey supported this provocative stance, noting that the 'administration is reaching for more visceral imagery': 'After two decades, yelling "fire" to get attention isn't enough and people must smell the smoke and feel the heat on their own faces' (Healey 2012). He argued that Panetta was probably right to invoke Pearl Harbor but the government needed to support its warnings of catastrophe with sufficient information 'to win over enough of the doubters' to enable reform (see also, Rid 2013a: 174). In 1998, Arthur Cebrowski, founding director of the US Office of Force Transformation and chief architect of network-centric warfare, articulated this dimension of the digital Pearl Harbor analogy. Effectively noting that to pick holes in the analogy was 'to miss the point', Cebrowski identified its continuing political utility:

> [W]hat really happened at Pearl Harbor was that a threat that had been sketchy, abstract, and distant became personal and immediate. Then, as now, there were those who saw the growing danger and strove to be heard and to influence policy and priorities. However, it took the actual attack to galvanize the nation. I suggest that Pearl Harbor's real effects were felt in the areas of policy, law, and national commitment to respond to a recognizable threat. (Cebrowski 1998)

In order to bring cyber attacks into the affective orbit of policymakers and public alike, physical scenarios are required in order to visualise the 'virtual' threat. The Pearl Harbor analogy is positioned in American memory as a visual and conceptual means of making the 'abstract and distant' materially comprehensible. As with 9/11, this is exogenous violence hitting at the heart of the nation, an emotional and physical jolt which might have the desired effect of 'waking' America from its cyber security slumber. The metaphor of sleep is integral to the Pearl Harbor myth, in which American national innocence is twinned with political complacency. With respect to cyber security, ‘it seems the “sleeping giant” is again awaiting a public, catastrophic event before awakening’ (Magee 2013: 78). It is evocative of Pearl Harbor that the list of cyber security events presented as signs of the apocalypse in Chapter 4 are also sometimes framed as ‘wake-up calls’ to the nation and its politicians (e.g. Healey 2013). The Pearl Harbor analogy serves to warn of the dangers of not being alert to the possibility of new Pearl Harbor-type events, particularly as they might arise, like Pearl Harbor, without sufficient ‘strategic warning’ to be prevented (Wohlstetter 1962). Moreover, when the nation is shaken from its state of ‘childlike innocence’, maturity and manhood, often in the form of military force, follow (Rosenberg 2003: 18). During the Cold War, security elites used the analogy to help improve intelligence, build new weapons and increase military budgets, and it became a ‘[p]owerful metaphor for international vigilance, a large military establishment, and a need for standing tough and unified against forces that might threaten the nation’ (Rosenberg 2003: 27). This is precisely the argument of many commentators who argue that the military should take the lead in national cyber defence. The Pearl Harbor metaphor plays a role in shaping this discourse to their benefit.

As suggested previously, references to Pearl Harbor are not accidental and continue the analogy’s long history of becoming ‘ever more elastic, connoting any potential national security disaster . . . an all-purpose cue for those wishing to trigger insecurity and a proactive response’ (Rosenberg 2003: 31). We cannot trace definitively the causal relationship between use of the analogy and the increase in US cyber security spending, institutional reorganisation and frequent attempts at legislation. If Healey is right that the administration is actively seeking to cultivate fear through ‘visceral imagery’, it seems likely that Pearl Harbor once again serves to assist the political processes required for resource allocation, doctrinal development, changes in force posture and other signs of institutional change in the pursuit of cyber security. The mobilisation of collective memory and identity are important aspects of this dynamic and the following section discusses Pearl Harbor, and historical analogies more generally, from the perspectives of memory and identity.

Memory and identity

Cyber security communities have invoked Pearl Harbor analogically for two decades, ‘with each cyber incident that reaches the media articulated as proof of its encroaching inevitability’ (Barnard-Wills and Ashenden 2012: 118). If steps are not taken to ‘defend our nation against this gathering cyberthreat', write two prominent US legislators, 'the day on which those cyberweapons strike will be another "date which will live in infamy", because we knew it was coming and didn't come together to stop it' (Lieberman and Collins 2012; also Hoekstra and Finch 2013). For some academics too, Pearl Harbor is always imminent and inevitable (Molfino 2012). However, the final cataclysm that must wake government from its complacency is forever deferred, creating a temporal hiatus filled with fearful anticipation and longing.

Many policymakers reject the inevitability or necessity of a digital Pearl Harbor and distinguish between the inevitability of a future attack – 'not a matter of if, but when' – and the preventability of a Pearl Harbor-type event. Attacks will happen, but they will not reach the catastrophic level of a digital Pearl Harbor if appropriate political action is taken now. The future is therefore still open for negotiation and is to some degree contingent upon the present, even if the future overwhelmingly shapes the contemporary politics of cyber security. These individuals challenge the narrative of imminent and immanent catastrophe from within, restoring a sense of agency to the political present, although the omnipresent threat of future disaster is only deferred rather than cancelled altogether.

This future-oriented aspect of the Pearl Harbor analogy is only one part of its potency and the past surfaces in its contemporary invocation and is constantly remade through its repeated enunciation. More accurately, without the present and future imaginings of the past, we cannot begin to understand the future through historical analogy. This is the source of disagreements over the validity of the metaphor itself, as there is no satisfactory way of comparing a future that has not yet happened with a past that cannot be experienced directly. Without an appreciation of the past, Pearl Harbor would lack its emotive qualities and the history of the term itself does political work in cyber security before it is even linked to threats, however specific or general these may be.

How is this so? What influence does this have on the politics of cyber security? Revisiting Roosevelt's 1942 speech, Rosenberg describes how it tapped into existing structures of national memory and identity. Roosevelt deliberately pitched his speech in order to recall key events in American frontier lore like the Alamo and Custer's Last Stand. Like Pearl Harbor, these looked initially like awful defeats but quickly became touchstones for 'overwhelming military counterforce leading to total victory', in each case an 'inevitable triumph' for the American people (Rosenberg 2003: 12). Most importantly, she argues, the 'infamy framework' was already widely present in frontier myths, and it was this pre-existing structure that allowed the Pearl Harbor narrative to take hold so rapidly and so effectively.

One could make a similar argument for cyber security, in which the frontier myth is foundational of narratives of future cyber security. A report by the Center for a New American Security asserted that 'governance in cyberspace resembles the American Wild West of the 1870s and 1880s, with limited governmental authority and engagement', even if this 'condition of anarchy is not absolute' (Rattray *et al.* 2010: 149, 150). Because its interests depend upon cyberspace, they write, the United States 'cannot allow a regression toward a Wild West of continuous malicious activity' (Rattray *et al.* 2010: 171). The authors call for 'a cleaner, healthier cyber environment in order to secure a broad range of United States and international interests' (Rattray *et al.* 2010: 140). The report based its policy proposals on models of public health, a common and long-established gambit in cyber security (Betz and Stevens 2013). It might easily have expressed the cultural trope of 'cleaning up' recalcitrant and problematic communities of the American West, no great leap as the authors had already established the Wild West as a foundational metaphor of their argument. It did not do so because it was avoiding suppressed national memories of aboriginal genocide (bad) and trying instead to remember the role of pioneer Americans in making the frontiers safe and prosperous (good). In an environment of few tangible borders (the internet), it is the role of America to ensure no space is left ungoverned, lest these interstices harbour enemies that may strike at American interests home or abroad (e.g. Innes 2007).

Like Pearl Harbor, the American West has always been a flexible concept, reimagined for multiple ends. It is 'a region of endless possibilities, a vast, magnificent, ideal stage for the national drama of liberty, equality, and the pursuit of happiness' (McLure 2000: 457). It is a cultural myth that relies on 'the uniquely-American frontier spirit and pioneer values that propelled the US to the West Coast in the nineteenth century, into space in the twentieth, and to the forefront of the so-called Information Age at the dawn of the twenty-first' (McLure 2000: 457; also, Taylor 1999: 157–9). In the hands of anti-authoritarian cyber-utopian groups like the Electronic Frontier Foundation, the myth becomes the basis for visions of opportunity and libertarian futures; in the security imaginary, the Wild West is something to be tamed and regulated. Each draws upon different aspects of the myth to guide and direct their aspirations for the future; each remakes the past in so doing.

However, as historian Eric Hobsbawm noted in a posthumously published essay, 'only Americans live in Marlboro country' (Hobsbawm 2013: 287). The world no longer consumes American cultural exports like movie Westerns with the gusto it once did, and the image of the rugged cowboy is no longer an international pin-up representing manly vigour and moral rectitude, however misplaced that original interpretation. This has not prevented recent US presidents – Reagan and Bush Jr, in particular – from adopting the semiotic trappings of the mythic gunslinger and the pioneer, often willingly assisted by the news media. George W. Bush, in particular, made concerted efforts in his first presidential campaign to veil his blue-blood east coast origins with the persona of a working-class hero dispensing justice on behalf of honest America, a role he revived successfully after 9/11 (West and Carey 2006; Malphurs 2008) – successfully, that is, for domestic audiences. The international press, by contrast, dropped their belief that Bush 'could be a statesman [and] now had no doubt that Bush was destined to remain the loathsome cowboy . . . "Bush thinks he is Wyatt Earp"' (Malphurs 2008: 195). One prominent British journalist described Bush's recourse to Wild West rhetoric after 9/11 as 'a man reaching for a childhood cliché rather than a subtle thought' (Naughtie 2005: 119). Similarly, contempt was heaped upon Tony Blair's infamous 'thumbs-in-belt' 2002 photo call with President Bush, after which he was pilloried as a subservient Tonto to Bush's Lone Ranger (Johnson 2002). For their respective audiences, it might just be acceptable for an American president to impersonate a cowboy, but it was unthinkable for a British prime minister to do so.

Cultural snobbery might partly explain non-American attitudes to American myth and its attempted appropriation by someone like Blair, but 'the cowboy' has come to mean different things to different audiences: one nation's self-image does not necessarily translate well across cultural boundaries. This is true of Pearl Harbor, which has a local specificity that does not necessarily reveal itself in all its dimensions when communicated to a global audience. When Maura Conway writes that this analogy has 'immediate resonance and attracts wide understanding' (Conway 2008: 117), this is probably the case across multiple audiences, but it is only in the United States that it will elicit what John Arquilla calls its 'surefire emotional effect' (Arquilla 2012). It is hard to imagine it having the same resonance elsewhere. Even among the United States' Western allies, Pearl Harbor is more likely to be remembered as the critical event that precipitated decisive US involvement in World War II than as a blow that struck at the heart of American society and self-image.

Pearl Harbor discourse mobilises some aspects of the frontier myth, but it has its own powerful role in constructing memory and maintaining national identity. In cyber security, Pearl Harbor as 'historical trauma' is linked to the 'new risks' of the globalised and interconnected world (Bendrath *et al.* 2007: 58). Just as the original attacks on Pearl Harbor showed that the United States was not isolated from the rest of the world, future Pearl Harbors warn against considering the United States invulnerable from foes located ‘geographically and morally’ outside it (Dunn Cavelty 2008: 130). Bendrath extends this argument further: this construction of an external Other ‘reinforces the idea of the nation as a collective self . . . [the] referent object of security, then, is the whole [of] American society’ (Bendrath 2001). A serious cyber attack would already demand a high-level political response, but this pressure would be increased considerably by constructing an ‘attack’ on infrastructure – even an attack perpetrated by an invisible and undeclared protagonist – as an attack upon American nationhood itself, bound together, in Benedict Anderson’s phrase, by a ‘deep, horizontal comradeship’ (Anderson 2006: 7). It assists in constructing an event as an issue of national, rather than only technical, security, one, in fact, that requires a militarised response. Pearl Harbor is part of the ‘national symbolic’, that discursive regime which ‘transforms [American-born] individuals into subjects of a collectively-held history’, with all the rights and responsibilities this ‘pseudo-genetic condition’ confers (Berlant 1991: 20).

The United States is framed as vulnerable, but it is also presented as *uniquely* vulnerable to catastrophic cyber attacks. This is expressed in two ways, both stemming from the American condition of high dependency on sophisticated information infrastructures. First, it is more vulnerable than other countries: ‘its overwhelming military superiority and its leading edge in information technology’, writes one commercial security expert, ‘have also made the United States the country most vulnerable to cyber-attack’ and other forms of asymmetric warfare (Adams 2001: 98). Second, the United States is more vulnerable now than it has ever been, with its ‘digital underbelly’ exposed for the world to see, a point made by probably hundreds of authors. Moreover, this is exacerbated by the inability of the federal government and military to protect the nation from cyber attacks. Even those who believe the Pearl Harbor scenario – ‘there may well be an electronic fleet preparing off our shores tonight’ – assert that ‘this is the first time in history where the American military cannot defend the American people’ (Clarke 1999: 43, 38). Writes one well-connected former public servant and lawyer: ‘We can’t hire an army or a police force that’s large enough to protect all of America’s cell phones or pagers or computer networks’ (Vatis 2002: 2). The United States is therefore supremely vulnerable in space, where it is an over-exposed global hegemon, and in time: at no point in its history has it been so open to catastrophic attacks of this nature.

Pearl Harbor was a moment of extreme vulnerability, as was 9/11, narratives of which frequently invoke Pearl Harbor, as already discussed.

American narratives of 'cyber' vulnerability also use 9/11 as a specific historical analogy. As Myriam Dunn Cavelty has found, 9/11 had the profound effect of recalibrating 'cyber-doom' discourses by strengthening that element concerned with terrorism, particularly Islamist terrorism (Dunn Cavelty 2007; Dunn Cavelty 2008: 117–21). Linking conventional terrorism to aggressive use of ICTs, 'cyberterrorism' was mentioned twice as often in *The New York Times* and *Washington Post* after 9/11 as before (Conway 2008: 122). Discourses of cyberterrorism are now almost as prevalent as – and frequently confused with – those of cyberwar, a 'hyping of an (imagined) fatal connection between virtual networks and critical infrastructures that, to date, has very little form or substance' (Conway 2008: 122; Conway 2011).

Cyberterrorism connects strategic terrorism with information technologies, but 9/11 provides an analogical bridge between information technologies and 9/11 as a spectacular national security event *not* restricted to terrorism alone. Since approximately 2003, there have been many assertions as to the likelihood of a digital, electronic or cyber 9/11. Mike McConnell, formerly director of the National Security Agency and later Director of National Intelligence, was an early adopter of the phrase, asserting the likelihood of a cyber attack equivalent to 9/11 in scale and impact, while embracing it as a 'forcing issue' to improve cyber security across public and private sectors (Cant 2003). McConnell frequently obscured the distinction between acts of cyberterrorism and other forms of ICT-mediated aggression, and a decade later his references to 'the cyber equivalent of the World Trade Center' were a straightforward cipher for any large-scale cyber attack on the United States, regardless of perpetrator or intent (P. Taylor 2012). The tendency has become to attribute a 'cyber 9/11' not to terrorists but to an assemblage of other actors: 'an attack [like this] could see a country like Iran work with Russian criminals or Chinese hackers', suggested McConnell (P. Taylor 2012). In January 2013, Secretary of Homeland Security Janet Napolitano also referred to the imminence of a 'cyber 9/11'. Speaking at the Wilson Center in Washington, DC, she explained: 'We shouldn't wait until there is a 9/11 in the cyber world. There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage' (Napolitano 2013).

It is possible that the choice of analogy partly reflects the institutions each official represented: the defense secretary opted to refer to an episode in military history (Pearl Harbor); the homeland security secretary preferred comparisons with a terrorist attack (9/11), which was, after all, the direct catalyst for the creation of her department in 2003. However, the question of actors' intent was, by 2012, all but absent from both analogies. Neither Pearl Harbor nor 9/11 were being used by senior officials with much consideration of the causes of future catastrophic events, except with reference to a non-specific external threat and to the problems arising from the general insecurity of sociotechnical systems. This is not to deny that these analogies continue to work in sophisticated registers, but it does suggest there is more concern about the effects of potential cyber catastrophes than their causes, exemplified by a further subset of historical analogies drawn from a catalogue of recent 'natural' disasters.

In 2005, Hurricane Katrina collided with the southern US seaboard, killing nearly 1900 people, causing upwards of $80 billion of property damage, and severely disrupting socioeconomic activities across the southern states. It was, by all estimates, one of the deadliest and costliest weather events ever to hit the United States, the official meteorological report recording simply that the extent, magnitude and effects of the hurricane were 'staggering' (Knabb *et al.* 2005). Not only were the physical impacts of Katrina of a severity not experienced in living memory, but the images of public panic, government impotence and social disorder – notably, looting in New Orleans – are now synonymous with what can go terribly wrong in the immediate aftermath of a disaster, including in the standards of press reporting (Tierney *et al.* 2006). It was perhaps inevitable that Katrina would enter cyber security discourse in the form of 'cyber Katrina' to connote a forthcoming catastrophe (e.g. Epstein 2009).

The proximal purpose in invoking a 'natural' event in this fashion is to highlight the lack of current attention to resilience, particularly with respect to government disaster planning (Bhaskar 2006; Boin and McConnell 2007). That political utility might outweigh decency and respect for persons caught up in unfolding crises is amply demonstrated by Secretary Napolitano's invocation of a cyber equivalent to Hurricane Sandy, even as the endgame of that destructive event was still playing out in late 2012. Sean Lawson points out that '[n]o natural disaster in the last several years has passed without a government official or civilian "expert" using it to raise fears of cyber threats' (Lawson 2012b). Like 9/11, Katrina is presented as a 'focusing event' for national disaster response policy; without these events, the forms of multi-sector cooperation required to mitigate the impact of disasters will not be explored and developed (Birkland 2006). Once again, the cyber disaster is constructed – through historical analogy – as something necessary in the formulation of appropriate policy and strategy.

Previous discussions of these analogies have teased out where they succeed and fail (e.g. Lawson 2013b). What is less commonly noted is their national specificity. We might argue that the discussion to this point has been heavily weighted in favour of US cyber security discourse to the exclusion of any other. This is a valid criticism but defensible partly with reference to an established analytical tendency to prioritise the United States in cyber security discourses, on account, principally, of its historical pre-eminence in the field of critical infrastructures and their security and protection (Dunn Cavelty and Kristensen 2008: 4). This apparent bias demonstrates the importance of that national particularity, indicating that the emotional and cultural aspects of historical analogies are equally as important as their other points of comparison. They may, in fact, be selected on this basis, in the knowledge that more accurate analogies might be available but which do not trigger specific collective aspects of identity and memory of greater political than technical utility.

Maura Conway notes that a 1998 report by the Center for Strategic and International Studies (CSIS) in Washington, DC, found the term ‘electronic Waterloo’ a more accurate comparison, although it is rarely, if ever, used today (Conway 2008: 125). The Battle of Waterloo (1815) was the decisive encounter of the Anglo-Allied campaign to unseat Napoleon from the French imperial throne. This inspired the CSIS authors to sketch the character of a possible future ‘information warfare’ campaign against the United States, ‘where technology, planning, and careful execution were used as part of a long-range plan aimed at altering the world’s political, military, and economic order’ (CSIS 1998: 2). Even were it able to capture the dynamics of the present situation better than the Pearl Harbor analogy, it would stand little chance of widespread adoption in the United States because Waterloo does not resonate with American audiences as it might with the British. The Victorian Poet Laureate Tennyson constructed Waterloo as a ‘world-earthquake’ (Tennyson 1971) and its tremors are perhaps felt today in the continuing importance of the British victory at Waterloo to the British national psyche. However, it means much less to a United States who by June 1815 had only recently fought imperial Britain to a draw, a war in turn mostly forgotten by a British nation preoccupied with Napoleon’s challenge to European stability.

The two events are very different, but Pearl Harbor has as unique a role in American national memory as Waterloo does in the British. These are both archetypal events that still possess the power to shock and inspire, to rouse popular emotion, and through which to pursue political ends. We should not be surprised to find that other nations appropriate and repurpose their own histories to narrate and explain present cyber insecurities. In Australia, for instance, we find mention of an ‘electronic Gallipoli’ in an article written ahead of both Y2K and the Sydney Olympics (Cobb

1999). This article is notable for mentioning Gallipoli in its title but not once in the body of the piece itself. Given the importance of the disastrous Gallipoli campaign of 1915 to Australian national identity, it seems it is enough just to allude to it in passing to stir the patriotic emotions of populace and politicians and (hopefully) thereby to further the ends of cyber security. Gallipoli is often regarded as the beginnings of a true Australian national consciousness and one wonders whether the 'electronic Gallipoli' is intended to arouse a cyber security 'consciousness' in its Australian audience. The concluding section discusses how this search for foundations is characteristic of cyber security's argumentation through the past.

Arguing through the past

The reliance on historical analogies to describe and explain speculative future scenarios is comprehensible in terms of appealing to existing national archetypes that stimulate emotional responses, mobilise patriotic sentiment, raise awareness of potent insecurities and facilitate the political processes of legislative attention and resource allocation. In this sense, both 'national memory', the curated historical discourses of nationhood, and 'cultural memory', that 'memory that is shared outside the avenues of formal historical discourse yet is entangled with cultural products and imbued with cultural meaning', are evoked and politicised (Sturken 1997). This process is greatly assisted by the recall of explanatory 'media templates' of historical events which, rather than 'opening up historical reflection [...] reify a kind of historical determinism which can filter out dissenting accounts, camouflage conflicting facts and promote one type of narrative' (Kitzinger 2000: 76). These established modalities of discursive action exist in many other fields of security, although they are notable in cyber security for their persistence even in the face of the non-appearance of the future catastrophes this analogical reasoning portends. Another facet of this form of representation and argumentation speaks more fundamentally still to the temporality of cyber security: historical analogies also serve as proxies for the foundational events that cyber security lacks.

In its attempts to sketch the contours of the future, cyber security cannot appeal only to its own limited past but has recourse to a generalised past of national security lodged in the memory not only of policymakers and those who execute policy and strategy but in the broader and deeper memories of the societies they exist to serve. As Hansen and Nissenbaum (2009) demonstrate, it is difficult to communicate and represent cyber security through images alone. Chapter 4 proposed that this is why future scenarios are sketched principally in physical terms. It is easier to evoke emotion and catalyse political action through narratives of death and obviously material destruction than to expect audiences to comprehend a rather abstracted vision of digital ones and zeroes comprising and circulating in a medium somehow ‘less real’ than everyday reality itself (Borgmann 1999; Virilio 2009). This applies even if the societal impact of illegal data transfer, subversion and deletion far outweighs the importance of the disasters imagined and communicated through catastrophic cyber security discourses (Lawson 2013a). This is one reason why a generic attendance to catastrophic ‘cyber war’ is distinctly deleterious to the progress of appropriate cyber security policy, as it ignores the rather less glamorous but arguably more insidious effects of increasingly banal and ubiquitous cyber crime and cyber espionage (e.g. Guitton 2013). Due to the inherent difficulty of visually representing even cyber security events which have already happened – except in language only accessible to specialists – it is perhaps easier to draw upon a repertoire of ‘real’ rather than ‘virtual’ events that offer spectacular imagery accessible to a wide audience.

However, as Hansen and Nissenbaum assert, while cyber security always mobilises the ‘specter of the future’, the past is articulated as ‘a legitimising reference that underscores the gravity of the [present] situation’ (Hansen and Nissenbaum 2009: 1164). This appeal is necessary because cyber security has no history of ‘founding incidents’ comparable to Hiroshima and Nagasaki, which, in the field of nuclear security and global politics, were illustrative of what might happen should the Cold War become ‘hot’ (also Rid 2013a: 174). Many examples of cyber insecurity are used to construct narratives of the future, as the previous discussion of apocalyptic signs demonstrates, but the catastrophic cyber security events imagined by many interlocutors have no historical precedents that might ground these speculations in empirical reality, as far as history can ever serve as such.

The search for foundations is frequently expressed with direct analogical reference to nuclear weapons. The speaker of the Estonian parliament, Ene Ergma, compared the 2007 cyber attacks on her country to a nuclear explosion and its resulting fallout: ‘When I look at a nuclear explosion and the explosion that happened to our country in May, I see the same thing. Like nuclear radiation, cyber warfare doesn’t make you bleed, but it can destroy everything’ (Davis 2007). The comparison with Virilio’s information accident is striking, which substitutes interactivity for radioactivity but has disruptive, perhaps even destructive, effects (Virilio and Petit 1999: 91). For Ergma, wrote the journalist who reported her thoughts, Estonia was as significant a moment in world history as the coming of nuclear weapons (Davis 2007). For similar reasons, journalists and defence analysts both asked: was Estonia 'Web War One'? (e.g. Blank 2008). Estonia was a sign of future catastrophe, but in this formulation it became a foundational event too, an historical anchor that grounded cyber security and the construction of cyber war itself (Kaiser 2015).

When news of Stuxnet, the computer worm that plagued Iranian uranium enrichment facilities, emerged in 2010, comparisons with nuclear weapons were not far behind. 'Stuxnet is the Hiroshima of cyber-war', wrote one journalist in *Vanity Fair*, 'We have crossed a threshold, and there is no turning back' (Gross 2011). One veteran of the US Department of Homeland Security proposed that cyberspace was as geopolitically transformative as atomic weapons. Stuxnet, in particular, was 'the first explosion of a cyber atomic bomb' and as globally disruptive of the status quo as Hiroshima (Rosenzweig 2013: 2). The search for an originary event upon which to build policy and strategy is evident in these statements. The atomic destruction of Hiroshima and Nagasaki in August 1945 became the quintessential reference points for all subsequent nuclear strategy and the absence of these events in the 'virtual' realm has hampered the quest for strategic 'cyber' deterrence, for example (Adams 2001: 86; Stevens 2012). Repeated attempts to frame contemporary cyber security – in its military and societal dimensions – as a 'new Cold War' have foundered on inaccuracies and misconceptions (Lawson 2012a), including the inability to identify historically important 'moments' from which this postulated new era might spring. The quest to analogise cyber security has prompted authors to find other 'beginnings' of this Cold War, like the Yalta Conference of 1945 (e.g. Klimburg 2013). These analogies may help to rally support for a particular cause, but it is undeniable that cyber security communities would benefit greatly from 'a catastrophe to call their own', which could serve as a touchstone for their own communal identity and as a powerful motivating tool for shaping the wider politics of cyber security.

We have identified previously a tendency to reduce temporally extended phenomena to discrete moments, by which a series of interconnected processes is compressed into a single, more easily digestible 'event'. An event is more readily assimilated into discourses of identity construction, persuasion and political coercion than is a complex assemblage of historically contingent processes that belie easy description or explanation (see Sulek and Moran 2009: 128–30). In the United States, Rosenberg identifies this dynamic in the 'diverse meanings that cluster around the icon of Pearl Harbor', which 'suggest emplotments of the past that are centered on the detail of conspicuous events, linked together in frequently overblown or all-too-clear cause and effect relationships'

(Rosenberg 2003: 188). Narratives that appropriate Pearl Harbor always potentially ‘downplay’ the *longue durée*, she writes, ignoring historical specificities to construct identity and politics in the present. Cyber security would seem to accord with that conclusion, cut off from its own history but selecting historical events as the discursive means through which to motivate memory and identity in pursuit of political aims in the present.

This chapter has attempted to demonstrate how the past contributes to the temporality of cyber security. Selective though the examples have been, including an extended discussion of the historical analogy of Pearl Harbor, we can see that proponents of cyber security attempt to construct narratives of the future through narratives of the past. This requires the idiosyncratic use of history to illustrate contemporary problems and their possible future solutions and, as suggested above, shapes the identity of cyber security communities themselves. In the absence of a foundational catastrophe of its own, cyber security looks to history for significant security events from which it may draw inspiration and identity, most often within the context of national memory and the military experience. However, some final comments are required that draw out the effects of this form of arguing through the past, particularly with respect to the interplay between memory, metaphor, history and myth.

Andreas Huyssen observes that the ‘real can be mythologized, just as the mythic may engender strong reality effects’ (Huyssen 2003: 16). Myth is ‘not simply a reflection of an existing reality [but] a source and condition of that reality’ (Cameron 1994: 270, in Farrell 1996: 130). This reminds us that the stories we tell about the past are not in the past at all but are told in the present and shape our actions and identities now and for the future. As archaeologist Laurent Olivier states, the past ‘does not lie behind us, like some older state of things. It lies ahead of us, with us’ (Olivier 2011: 9). The past is continually remade and repurposed and will always be so, particularly as ‘the capacity to construct a myth of origins carries enormous political advantage’ (Walker 1989: 170). The contradictions between myth and history are summarised by Raymond Aron, who surmises that mythologies require ‘the substitution of a single factor for the plurality of causes’ (Aron 1954: 97–8). There are dangers, therefore, in the mythological mode of thought, aside from the obvious implications of identity politics for the communal evils stemming from the creation and maintenance of artificial divisions and discrimination. The use of analogies and metaphors to construct myth and identity plays a particularly important role in ‘structuring political reality for manipulative purposes’ (Hook 1984: 259). The contemporary study of metaphor is greatly influenced by the idea that metaphors influence what we say and the cognitive frameworks that allow us to speak and act; they are, in a real sense, ‘metaphors we live by’ (Lakoff and Johnson 1980). It is no surprise that analogies and metaphors can be important factors in fomenting ‘groupthink’ and closing off other avenues of intellectual enquiry (Schafer and Crichlow 1996). Murray Edelman notes that this can result in the ‘dulling’ rather than ‘awakening’ of our critical capacities, which impacts negatively on our collective ability to enact appropriate and progressive policy and legislation (Edelman 1964: 124–5).

The forms of analogical reasoning we choose come with ‘practical implications about contents, causes, expectations, norms, and strategic choices’ (Bobrow 1986: 436). In cyber security, Martin Libicki contends that to ‘use metaphor in place of analysis verges on intellectual abuse’ and counsels strongly that situations be avoided in which analysts and policymakers are ‘apt to make their metaphors do their thinking for them’ (Libicki 1997: 6). This suggests that over-reliance on the explanatory potential of some of the historical analogies discussed above may constrain our capacities to think about future cyber security scenarios productively as much as they enhance them (Betz and Stevens 2013). Historical analogies will not a priori foreclose on particular exploratory avenues of policy or strategy nor necessarily affect the outcomes of political decision-making, but, as more comprehensive studies show, analogies can help political decision-makers both to understand contemporary situations and to justify their political agendas (e.g. Khong 1992).

The uses to which cyber security actors put the past demonstrate both these characteristics, but it is far too early to tell how longer-term decision-making might be impacted by these selective uses of historical analogies. What is clear is that cyber security, while always imagining and, sometimes, desiring a catastrophic future, is seemingly always forced back to history in an attempt to understand the future, most often by situating itself within grand narratives of national security threat and response. Not least this is because of cyber security’s expression of a contemporary tendency for mediated discourses to ‘plunder the past for signs of stability, as though to mitigate the inherent instability of an obsession with the here-and-now with an intelligible there-and-then’ (Hoskins 2006). In this light, the historical past will be continually remade in the image of cyber security’s present and future, as cyber security discourses are built on more concrete foundations than their own short histories can alone provide. The dazzling speed and acceleration of the cyber security present needs, in order to be intelligible to public and politicians, metaphors that anchor discourses in historical events and times more readily comprehensible to the human mind.

6 Inhabiting the future

Anticipation and preparation

As if to illustrate further how a national icon can be repurposed by contemporary security logics, in July 2002 the US Naval War College hosted 'Digital Pearl Harbor', a three-day war game co-sponsored by IT advisory firm Gartner Inc. The objective of the exercise was to identify points of vulnerability and potential failure in the nation's critical infrastructure through a simulation of a major cyber attack on computer and communications systems across a range of industrial and government sectors (Wilson 2005: 9–10). The organisers concluded that a large-scale event analogous to its historical namesake was unlikely to occur in the future, but they could not rule out cyber attacks causing major disruptions. They found that a dedicated group of hackers or cyber terrorists could not single-handedly bring US critical information infrastructures to a halt, but it could do 'significant localized damage' to components of infrastructural systems (Kane 2002). The exercise indicated that the most vulnerable systems were the internet and parts of the digital infrastructure of US financial systems (Wilson 2005: 10). Digital Pearl Harbor illustrates one of the key aims of this form of activity: to identify defensive weaknesses in 'friendly' systems and the probable effects of their deliberate targeting by adversaries. Exercises and simulations of this type are a key area of cyber security practice and intend both to anticipate the character of future events and to prepare and train participants how to act should such events occur. At the very least, one Gartner analyst explained, participants in Digital Pearl Harbor would 'come away with a healthy dose of paranoia' (Radcliff 2002).

Computer scientists and hobbyists have always attempted to compromise the defences of other people's systems and networks, but by the 1970s 'penetration testing' ('pen-testing') was formalised as a method of checking the robustness of one's own systems. This was particularly true of the defence sector, where 'tiger teams' were routinely deployed as part of software and hardware development and testing (Mackenzie and

Pottinger 1997; Hunt 2012). Unfortunately for systems designers, the tiger teams usually found ways to breach system security, even after the patching of vulnerabilities revealed by earlier testing (Mackenzie and Pottinger 1997: 46). These exercises revealed that ad hoc approaches to security would never provide perfect security, leading to new forms of security specification and verification that by the early 1980s had crystallised into what we would now regard as 'classical' models of computer security. Foremost among these was the Bell-LaPadula security model, which restricted access to data by granting users security clearances only to data labelled as accessible to that level of clearance and which remains influential today (Bell 2005). The efficacy of these models was not to last, as multiuser mainframes became networked systems and there was 'no clear unitary route to the solution of network security' (Mackenzie and Pottinger 1997: 56).

Cuts in defence expenditure after the end of the Cold War contributed to this problem of computer security without obvious boundaries. Defence procurers sought cheaper commercial 'off-the-shelf' IT solutions, with research and development costs borne by industry rather than the taxpayer (Mackenzie and Pottinger 1997). The requirement that software operate with many different hardware and network configurations effectively made it impossible for any manufacturer to keep abreast of new security vulnerabilities, except by issuing more and more retrospective patches to their products. The unimaginably large number of possible combinations of hardware and software meant that, effectively, 'there is no such thing as a forced entry in cyberspace' (Libicki 2007: 35). There will always be gaps into which attackers can insinuate malicious code or through which data, in the jargon, can be 'exfiltrated'. Today, the Pentagon notes that tiger teams still 'invariably' manage to penetrate Department of Defense systems (Defense Science Board 2013: 28).

This is the environment in which 'cyber exercises' and their ilk operate. No longer designed principally to identify points of vulnerability and failure in friendly systems, they exist because of an acceptance that vulnerability and failure will always exist and must be dealt with on those terms. They operate as forms of anticipatory security that do not aim principally to prevent a cyber attack from happening – although other aspects of cyber security do aspire to that – but as a minimum to reduce the impact of these events through present attention to all aspects of network operation and management, both social and technical. The intention is not just to identify technical problems exposed and caused by the simulated attacks but also to reveal flaws in existing organisational protocols, working practices, emergency response frameworks and other managerial and cultural aspects of institutional life (de Goede and Randalls 2009; Anderson 2010b). As one analyst argues, most organisations' knowledge of their own cyber security issues is so limited as to be 'alarming' (Geers 2010).

Security communities consider simulations and exercises necessary because there is a limited set of 'real-world' case studies from which to develop anticipatory knowledge about the future. The number of cases directly relevant to the specific institution or company in question range from very limited to non-existent, particularly as one moves towards the military end of the 'attack spectrum'. For example, there has not yet been a conflict between two state militaries in which cyber operations have played the dominant or decisive role. This makes it difficult to model how these conflicts evolve and what their secondary effects might be on non-military sectors of society.

Such practices have become increasingly common across multiple sectors, bringing together government, private sector and civil society actors in sophisticated exercises intended to mitigate future uncertainty. In this respect, cyber security accords with developments elsewhere in security governance. Claudia Aradau and Rens van Munster relate how a range of public officials, security professionals and citizens are enrolled in 'the sensorial regime of future catastrophic events' by exercises and simulations (Aradau and van Munster 2011: 95). Crucially, by 'making the unexpected visible and perceivable, preparedness exercises stage an encounter with the future in which subjects are not just spectators but active participants' (Aradau and van Munster 2011). Aradau and van Munster argue that in order to achieve these ends, an aesthetic 'sensorium of anticipation' is developed with respect to catastrophic security futures. This is not just a visual aesthetic but a full-spectrum aesthetic that 'entails modalities of tactilizing [all] the senses in order to render the future palpable and foster subjects who can inhabit the future not just through fear and anxiety but also through desire' (Aradau and van Munster 2011: 85–6). There are clear correspondences here with the forms of chronotypical imagination articulated with respect to apocalyptic futures in Chapter 4.

The informing logic of the many forms of cyber security practice we may situate in this category of preparedness is a temporal one, a distinct temporality of anticipation and longing that we have already encountered in previous chapters, particularly in apocalyptic discourses of future cyber (in)security. Cyber security exercises, in common with similar practices elsewhere, shift attention 'from the pre-evental temporality of prevention and precaution to the time of the event' itself and by engaging in rehearsals of future attacks 'bind future decisions to decisions in the present'

(Aradau and van Munster 2011: 86). This is the essence of all training, practice and rehearsal in which future actions are shaped by preparatory actions undertaken in the present, and in which ‘memory’ and ‘body memory’ are equally important aspects of ‘remembering’ how to respond to particular situations. As Philip Sabin notes in his study of war gaming and military simulation, humans are not ‘mere helpless victims of an utterly uncertain world, but are capable of shaping their futures to a very considerable extent by taking actions founded on past learning and experience’ (Sabin 2012: 56; also, van Creveld 2013).

Aradau and van Munster distinguish between catastrophe and crisis, arguing convincingly that in contrast to the responses elicited by crises – through which crisis can be controlled and risk managed – catastrophes are ‘incalculable, uncontrollable and ultimately ungovernable’ (Aradau and van Munster 2011: 28–9). Sociologists of disaster identify a similar typology. Crises develop and escalate over time, but catastrophes simply happen: they are unexpected and unpredictable events that disrupt ordinary social conduct. Catastrophes are ‘more profound’ forms of disaster on account of their scale and impact (Birkland 2006: 5). The anticipatory forms of ‘inhabiting the future’ are responses to this uncertainty and the means through which to govern the unpredictability of catastrophe. This is an analytically useful distinction, but this chapter asserts that the concepts of inhabitation and sensory aesthetics are also applicable to the crises potentially encountered in cyber security. The instances of cyber security ‘emergency’ for which actors prepare are frequently not, despite rhetoric to the contrary, single catastrophic events like the terrorist attacks that are the principal objects of the forms of security governance examined by Aradau and van Munster. Most future cyber security scenarios consist of a concatenation of small events and are often better described as crises rather than catastrophes, even if the rhetorical emphasis is often on the latter. A common cyber security metaphor that demarcates perceived reality from predicted catastrophe is the ‘death by a thousand cuts’ scenario, in which the nation slowly bleeds to economic death rather than suffering a terminal militarised assault (Lindsay 2013: 370; Singer and Friedman 2014: 70). This is very much in keeping with the idea that the ‘modern crisis is not boxed in by set dates that mark a clear beginning and ending: it is an embedded vulnerability that emerges, fades, mutates, and strikes again’ (Boin 2004: 166).

This chapter extends a key concept in Aradau and van Munster’s model. Rather than peer helplessly at the uncertain future or speculate as to its possibilities, people are encouraged to ‘inhabit the future’ through tangible and intelligible means that prepare them for when the future – often catastrophic – actually arrives (Aradau and van Munster 2011).

This chapter explores the ways in which cyber security futures are 'inhabited', beyond the category of catastrophe to the field of future cyber security events in general. It also develops the concept of inhabitation in a novel direction. 'To inhabit' a place, figuratively or otherwise, is to be the subject that takes the transitive verb: one always dwells or lives in somewhere or something. If I inhabit the future, in some way I act as if I am residing in that temporal register, even if my physical person can only exist in the present. There is an additional older, if now obsolete, meaning of the transitive verb, 'to inhabit', which speaks to the more active connotations of 'to people with' or 'to furnish with inhabitants'. Inhabiting is not just passive dwelling within a space but the active colonisation of the space that enabled the dwelling; it is the 'becoming' of the inhabitation that complements its 'being'. This enables us to think more fully about how security processes go about actively 'populating' as well as inhabiting the future and augments Aradau and van Munster's acknowledgement of the capitalist 'colonisation' of the future in modernity through credit, insurance and risk management (Aradau and van Munster 2011: 10). By doing so, we might more fully account for the role of the corporeal political subject in the anticipatory practices of cyber security, while illuminating further the chronotypical imagination of cyber security communities.

This chapter develops these themes in three stages. In the first section, cyber security exercises and simulations are examined which bear little resemblance to preparedness activities in any other field. Conducted through information-technological means away from the public view, these abstracted and bloodless simulations of future cyber security events are meaningful to participants yet unintelligible to outsiders on account of their primarily virtual, hidden and technical nature. An epistemological problem is encountered when attempting to communicate the outcomes and findings of these to the general public, who have no way of accessing and understanding these phenomena for themselves and must rely on the statements of security professionals, journalists and policymakers, an asymmetric relationship potentially fraught with distrust. The second section argues that in order to mitigate this situation, an increasing number of exercises and simulations *are* communicated to the public. This entails attempts to 'materialise the virtual' – a concept briefly introduced in Chapter 5 – including by demonstrating the possible physical effects of cyber attacks on infrastructure. These make the previously intangible tangible and draw the public into cyber security preparedness in ways analogous to older public information campaigns that aimed to translate distant threats into something immediate and actionable. This shift towards the public mediation of cyber security exercises includes the televised Cyber ShockWave exercise (2010), which demonstrated the deliberate construction of an aesthetic sensorium of crisis in the public domain, allowing observers to inhabit the unfolding simulated events through their own mediated experience. The third section examines how recruitment campaigns bring people directly into cyber security preparedness, a situation enabled by a perceived lack of skills and personnel in this field of security. There is often a competitive element to these recruitment campaigns, in which people enter contests to catch the attention of government and industry. These activities are directed at professionals and university students and at children through education and skills training. The chapter concludes with a discussion of how these various security practices contribute in various ways to the inhabitation of the uncertain future.

Exercise and simulation

In June 1997, the US government undertook one of the earliest large-scale cyber security exercises, couched in terms of the then-fashionable 'information warfare'. 'Eligible Receiver' imagined a military crisis on the Korean Peninsula requiring the rapid deployment of US forces in support of its South Korean ally. Several dozen staff of the National Security Agency (NSA) were cast as North Korean hackers, who, with no prior intelligence and using only code freely available on the internet, were tasked with disrupting US military operations, a situation which would assist in the 'softening' of Washington's stance towards Pyongyang. Over a two-week period, the NSA 'red team' compromised enough systems that official sources professed the outcome 'frightening': not only could the 'North Korean' red team have seriously affected US command-and-control structures in the Pacific theatre, but it was also in a position to inflict 'crippling damage' on urban power grids on the American mainland (Gertz 1998).

In the absence of unclassified data, it is difficult to confirm the veracity of these claims, and they have long been subject to scrutiny and scepticism. More significant than the plausibility of the exercise scenario is how Eligible Receiver quickly became the standard by which to judge other exercises. Chapter 4 noted that Eligible Receiver is one of many events interpreted as a 'sign' of 'cyber apocalypse'. The official conclusion drawn from Eligible Receiver – that US military capability and domestic infrastructures were at grave risk from adversarial hackers floating 'effortlessly through global cyberspace' (Gertz 1998) – has become almost the default 'lesson' of subsequent US exercises. This lesson was apparently corroborated by events occurring shortly thereafter. A year later, the US

Department of Defense experienced a series of cyber attacks, although what damage was caused – if any – is still classified. The FBI/Joint Chiefs of Staff investigation became known as 'Solar Sunrise' and Iraq was initially suspected due to ongoing US military operations there. Two Californian high school students and a teenaged Israeli hacker were eventually identified as responsible and prosecuted (Power 2000).

A US government training video later circulated on the internet captured 'lessons learned' from Solar Sunrise: 'Though no hostile government or group was behind these intrusions, [Solar Sunrise] clearly demonstrates the vulnerability of the nation's complex information systems to terrorist assault' (National Infrastructure Protection Center 1999). Specifically, Solar Sunrise, as a report to Congress concluded, 'confirmed the findings of Eligible Receiver: US information systems are vulnerable' (Hildreth 2001: 5). 'Everything we learned in Eligible Receiver, we relearned in Solar Sunrise', said Deputy Defense Secretary John Hamre, but 'there's nothing like a real-world experience to bring the lessons home' (Graham 1998). The temporal dynamic is one in which exercises and simulations are validated and legitimised by later events, presumably a source of both relief and concern. This is despite the minimal similarity between simulation and event. Eligible Receiver was preoccupied with cyber terrorism and inter-state conflict dynamics; Solar Sunrise investigated what turned out to be exuberant juvenilia, which even the US Department of Justice claimed had not compromised classified data (US Department of Justice 1998).

George Smith, an outspoken critic of US government information warfare rhetoric in the late 1990s, described what he felt, in the case of Eligible Receiver, was a 'jump from alarming scenario to done deal' (Smith 1998). Smith held that the continued classification of information pertaining to these exercises disbarred external, objective evaluation of the claims made for the vulnerability or otherwise of information infrastructures to attack, subversion and degradation. This is the persistent core of cyber security narratives – 'confusion over what is real and what is not' – an epistemological problem that can only begin to be resolved by government disclosure, in the absence of which the published findings of exercises like Eligible Receiver 'must be treated with a high degree of skepticism' (Smith 1998). The 'done deal' to which Smith referred is the logical conclusion to which the public is drawn in the absence of credible, verifiable information: these exercises will expose vulnerabilities that can only be addressed by increasing the activities of the national security state. It is not that security problems do not exist but that we are in no position as external observers to judge for ourselves whether they do or not. Nor can we be content with the increased public expenditure on cyber security these exercises facilitate, in the absence of verifiable data by which to evaluate budgetary claims.

In 2009, John Arquilla asserted that exercises subsequent to Eligible Receiver – Black Ice (2000), Blue Cascades (first held, 2002), Silent Horizon (first held, 2005), Cyber Storm (first held, 2006) – ‘have confirmed beyond doubt that huge vulnerabilities to cyber disruption do exist’ (Arquilla 2009: 212). This is not equivalent to arguing that ‘huge’ cyber disruptions *will* occur, but it does presume that vulnerabilities can be exploited such that they *might*. There remains a sense that these large-scale exercises confirm the already known: that an adversary might exploit vulnerabilities, resulting in the serious degradation of a world power’s ability to protect itself from cyber attack (Dunn Cavelty 2008: 82).

The official public reports of exercises like Cyber Storm – run by the US Department of Homeland Security – are, by contrast, often quite circumspect, preferring to concentrate on processual and procedural aspects of the institutions and organisational structures under stress, rather than on the future probability of the ‘Significant Cyber Incident’ simulated.[1] Nevertheless, the singular and destructive event is still the benchmark against which the mettle of these institutions is tested, be they the North Atlantic Treaty Organization (NATO), the European Union or any one of the dozens, if not hundreds, of other commercial, national and multilateral exercises conducted annually across the globe (ENISA 2012). Cyber exercises are also conducted in preparation for large-scale, ‘non-cyber’ events that definitively will happen, like the Olympic Games and other public spectacles (Institute of Engineering and Technology 2013).

Like counter-terrorism exercises conditional on a terrorist ‘event’, these cyber exercises demand from participants that they can imagine future scenarios in order to assist the process of preventing them from happening. More important still is their function in getting participants ‘to inhabit, rehearse and exercise the event in order to devise adequate responses should the event ever materialize’ (Aradau and van Munster 2011: 22). This requires a ‘world’ for participants to inhabit, and cyber security has long created its own simulated environments, circumscribed by technology and the demands of the exercise. Cyber Storm I (2006) and its subsequent biennial iterations have ‘provided government, private sector, and international participants with a neutral and controlled environment in which to exercise their response procedures to a significant and

[1] Reports on Cyber Storm I (2006), II (2008) and III (2010) are available from www.dhs.gov/cyber-storm-securing-cyber-space. Official reports of Cyber Storm IV (2013) have yet to be released.

coordinated cyber attack' (National Cyber Security Division 2006: 14). Baltic Cyber Shield 2010 was conducted entirely 'within the confines of a virtual battlefield', which could, if necessary, be accessed from anywhere in the world (Geers 2010: 6). These environments are isolated from the wider internet, in order that malware and other forms of code do not escape and create problems elsewhere, but they are inherently incapable of replicating all the conditions pertaining in a real crisis. They are, by comparison with the information infrastructures affected in a live situation, very localised and often represent few of the interdependencies between systems that exist outside the simulation. In military exercises, these highly simplified simulations cannot hope to correspond to 'full-scope' operations that deploy a wide range of political resources and military capabilities in addition to computer network operations (Geers 2010: 4). The responses to this inevitable shortcoming are either to run more simulations or to increase the computing power of the simulation. In the former category, the two large 'technical rehearsals' in March and May 2012, ahead of the London Olympics, examined 'the performance of people, process and systems in different situations selected from a playbook of over 1000 different technology scenarios built up over previous Games' (Institute of Engineering and Technology 2011: 23). Organisers also ran repeated simulations for months prior to the Games.

In the second category, there have been notable attempts to build truly impressive simulation environments, generally known as cyber ranges or testbeds (Davis and Magrath 2013; Siaterlis and Genge 2014). One of the most ambitious is the US Department of Defense's National Cyber Range (NCR), development of which began in 2008. This scale model of the global internet is a 'representative network environment', used as a test-bed for developing and deploying 'revolutionary cyber testing capabilities', including exercises of a military nature (DARPA 2008a). Secretary of Homeland Security Michael Chertoff informed a security conference that the Comprehensive National Cybersecurity Initiative (CNCI) (White House, n.d.), of which the NCR would be part, would be 'like a Manhattan project to defend our cyber networks' (Chertoff 2008b). Since 1996, there have been many calls for a 'cyber' Manhattan Project and at least one public–private initiative has taken that name. One prominent legal scholar wrote: 'We need a latter-day Manhattan project, not to build a bomb but to design the tools and conventions by which to continually defuse one' (Zittrain 2008: 173). A defence insider was quoted similarly, claiming of the NCR, 'Congress has given DARPA a direct order; that's only happened once before – with the Sputnik program in the '50s', the launch of which led directly to the founding of DARPA's forerunner in 1958 (Weinberger 2008). Cold War and nuclear analogies are common with respect to the NCR: ‘the Cyber Range is to the digital age what the Bikini Atoll [was] to the nuclear age’, claimed *The New York Times* (Sanger *et al.* 2009). Again, sponsors and commentators search for metaphors through which to frame and understand the historical significance of these new initiatives.

The historical import of the NCR is for others to discern, particularly as it only went ‘live’ in 2012, when operational responsibility for the $130 million project was transferred from DARPA to the testing and evaluation arm of the Department of Defense. The DARPA press release announcing the handover noted the diversity of network states that could be simulated, the speed at which the NCR could be re-configured and its operational flexibility (DARPA 2012). The NCR is able to simulate the behaviour not only of complex assemblages of code and machines (‘nodes’) but of people (‘users’) too, designated in the original design proposals as ‘basic human replicants’ (DARPA 2008b), a term which owes, but does not acknowledge, its debt to the science fiction movie *Blade Runner* (dir. Ridley Scott, 1982). The more exuberant online news providers seized upon the opportunities offered by this form of popular culture intertextuality, the United Kingdom’s *The Register* declaring, ‘DARPA Wants *Matrix*-Style Virtual World for Cybergeddon’ (Page 2008).[2]

The replicants of *Blade Runner* are genetically engineered creatures which impersonate human form and behaviour. They are different from the simulated corporeality of the inhabitants of the Matrix, whose physical bodies are held in laboratory stasis elsewhere. Both are different again from the NCR replicants which are non-sentient, non-corporeal informational constructs. They have limited agency governed by complex algorithms and no persistent existence outside of the software configuration of the moment. Each time the test-bed is repurposed for the next simulation, the NCR replicants cease to be. They maintain no identity across programs or environments and only exist temporarily to simulate limited aspects of human–computer interaction relevant to the task at hand. They differ also from the denizens of computer-generated virtual reality (VR) simulations for military training purposes, descendants of video game aliens and monsters, whose bodies exist on the virtual battlefield only in order to be killed. Each of these simulated environments is a ‘kill-box’ where body counts matter most and ‘kinetic exchanges’ are the ‘order of the day’ (Coker 2013: 128).

For the real human participants, these ‘virtual’ environments are still experienced physically. James Der Derian’s description of playing a

[2] The reference is to *The Matrix* (dirs. Lana Wachowski and Andy Wachowski, 1999).

version of the 'first-person shooter' computer game *Doom* created by the US Marine Corps underscores further that physical affect persists even in these environments, 'especially if accelerated heartbeat is any measure' (Der Derian 2009a: 90; see also, Smith 2010). In the case of cyber simulations and exercises like those at the NCR, we can assume a similar physiological and emotional response to sensory stimuli, even if the nature and character of these stimuli are quite different from the more visual and visceral experiences of battlefield simulations. In the absence of public information about the conduct of NCR, it is unwise to speculate overly about the experience of being involved in these activities, but from other sources we can develop a basic picture of the environment (e.g. Lockheed Martin 2012). Video footage from NATO's 'Locked Shields' cyber exercises shows teams of operators sitting at rows of desks typing code and commands into laptops, upon the screens of which are displayed technical information decipherable only by the specialist and on which individual nodes and actors are reduced to stylised icons. The dynamism of this ever-changing 'battlefield' is discernible only through scrolling text, blinking colour bars, the pan-continental maps of pulsing network flows on large wall-mounted screens, the attentiveness of the circulating team leaders and through the subdued yet occasionally animated body language of subordinates entangled with the artefactual trinity of screen, keyboard and mouse.[3] This is a sensory assemblage far removed from the adrenalinised physicality of the traditional theatre of war, but it is still one experienced sensorily, physiologically and emotionally by its human participants.

The majority of cyber exercises probably provide similar experiences, where informational rather than physical terrain is the resource over which participants attempt to establish control. Whether military or civilian, or public–private hybrids, the environments that run simulations are characterised by a distinct lack of the sensory stimuli and semiotic markers that ordinarily define the field of conflict. Engagement is facilitated by translating bits of codified information back into visual forms intelligible to the human senses, enabling coherent and appropriate responses by the participants. Within the confines of the exercise room – and from the perspective of the non-technical observer – nothing much seems to change, even as the balance of defeat and victory shifts from one side to the other. In time, one team emerges victorious by achieving a predetermined defensive or offensive goal, a victory only sensible to the outsider through the congratulatory intercourse of the winning team.

[3] See, 'CDX Locked Shields 2013', http://vimeo.com/65305608.

Future cyber conflicts will be played out in these abstracted informational battlespaces, but their simulations are not the only way in which to imagine and rehearse the future. Epistemological uncertainty makes 'lessons learned' difficult to communicate to the public and there are inherent difficulties with 'materialising the virtual', as identified in previous chapters. Attempts to overcome or at least mitigate these problems resort to aesthetic modalities of a more established nature than the deployment of hi-tech apparatus like cyber test-beds and the impenetrability of cyber defence exercises. These activities serve to generalise an aesthetic of future cyber disruption – and, often, catastrophe – that aims to make the 'virtual' material and facilitate the metaphorical inhabitation of the future, especially by the public.

The public sensorium

In September 2007, a CNN video began circulating on the internet, purporting to be Department of Homeland Security footage of an experiment conducted earlier that year at the Department of Energy's research and development facility, the Idaho National Laboratory. In the video, dated 4 March 2007 and lasting barely a minute, a close-up shot shows a large section of industrial plant juddering and shaking before belching out clouds of white and black vapour; a second shot from distance shows what may be the same equipment ejecting similar gaseous emissions.[4] According to sources, in the experiment, codenamed Aurora, 'a 21-line package of software code sent from 100 miles away caused a $1-million commercial electrical generator to generate self-destructive vibrations by rapidly recycling its circuit breakers' (Fulghum 2010). The experiment was widely considered the first proof that hackers could enter a sophisticated industrial control system and cause a physical device to self-destruct.[5] This, suggested experts, showed that electrical infrastructure components were vulnerable to exogeneous interference and destruction in unexpected and worrisome ways (Meserve 2007). From this premise, a narrative of ever-greater threat was developed. CNN reported expert opinion that the attack scenario could be replicated across the US electrical grid in coordinated fashion, causing damage that would take months to repair (Meserve 2007). For an oddly specific investment of

[4] The video is no longer available from CNN but is accessible at www.youtube.com/watch?v=fJyWngDco3g

[5] Although, see the Maroochy Shire sewage system incident in 2000 (Rid and McBurney 2012: 10). There are also earlier press reports of INL tests resulting in physical destruction of infrastructure components (e.g. Blum 2005).

time and money – 'about $5 million and between three and five years of preparation', according to one expert – an adversary could mount a plausible strategic assault against the United States which, if successful, could cost the country hundreds of billions of dollars (Meserve 2007). One government economist offered this dramatic perspective: 'It's equivalent to 40 to 50 large hurricanes striking all at once. It's greater economic damage than any modern economy ever suffered . . . It's greater than the Great Depression. It's greater than the damage we did with strategic bombing on Germany in World War II' (Meserve 2007).

Some of the reporting may have been hyperbolic and some of the expert scenarios a little fanciful or exaggerated, but much of the commentary by public officials was quite circumspect. They identified and accepted the existence of a vulnerability, gave assurances that it was being addressed and stressed that the destruction imagined by some was possible, if highly unlikely. Later still, another simulation at Idaho National Laboratory, this time attended by journalists, showed how a red team could access a chemical plant mock-up and take control of the water-pumping system (Ahlers 2011). 'If this mock facility were an actual chemical plant, hazardous liquids could be spilling', reported Tom Gjelten of National Public Radio. 'If it were an electric utility, the turbines could be spinning out of control. If it were a refinery, the tanks could be bursting or pipelines could be blowing up' (Gjelten 2011). In a non-simulated situation, Stuxnet showed how code could be introduced into a closed supervisory control and data acquisition (SCADA) system, resulting in real physical damage to industrial plant, in that case to several hundred nuclear centrifuges. Journalists and analysts later found, however, that it took substantial investment of time and resources to bring about these results (e.g. Sanger 2012), and it is doubtful if Stuxnet even achieved its desired strategic effect (Barzashka 2013).

If industrial plant is obscure to the average observer, subsequent simulations attempted to illustrate the effects of cyber attacks on the urban infrastructures with which we are more familiar. In November 2012, a press release hit news desks from its source in Bethesda, Maryland, heart of the US defence sector, detailing the inauguration of NetWars CyberCity, a 'small-scale city' in New Jersey, replete with 'bank, hospital, water tower, train system, electric power grid, and a coffee shop' (SANS Institute 2012). The purpose of the development was to teach and train US soldiers to defend urban infrastructures by showing them 'how online actions can have kinetic effects' (SANS Institute 2012). The trainees were tasked with various different missions, lasting from a few hours to a few days. These included hacking the traffic management system to inhibit the flight of terrorists; preventing a train loaded with weaponised radiological material from entering the city; and disarming a rocket launcher aimed at the hospital (Badger 2012; BBC News 2012b).

The rationale for creating an urban mock-up was to stress the linkages and interdependencies of the 'cyber' and the physical. A SANS instructor explained how the military sponsors wanted 'to see physical things'. The aim of the simulation was to demonstrate how you could cause 'physical damage or change in a city environment entirely using computers' (Badger 2012). Again, the emphasis is on making the 'virtual' threat material and more readily comprehensible. In a statement of the banal – yet profound on account of being frequently overlooked – 'all of cyberspace comes to ground somewhere' (Goodman *et al.* 2007: 196–7). CyberCity is an example of how the sociomateriality of information technology networks and their imbrication with the urban fabric can be brought into the realm of aesthetic experience.

There is a long heritage of bridging the gap between practice and reality through the use and construction of simulated battlespaces. One expert alluded to this history, noting that CyberCity was equivalent to the 'deserted villages' of the British military training range of Salisbury Plain; like them, CyberCity would not prevent attacks but would teach soldiers how to 'defend and respond to a situation' (BBC News 2012b). From the Wiltshire villages first hollowed out by national need during World War II (Sawyer 2001) to the post-Iraq US training grounds for 'military operations on urban terrain' (MOUT), urban conditions have frequently been simulated as part of military preparedness exercises (e.g. Der Derian 2009a: 274ff.; Watson 2011). What is remarkable about CyberCity is that it is not physically navigable. At a scale of 1:87, CyberCity is a model city contained within less than fifty square feet; no infantry boots can ever set foot on this particular ground and there is no way the city can in a literal sense be inhabited, even for a short period of time. However, this would be to miss the point of the simulated city, as *The Atlantic* identified, reminding its readers of the 'psychic effect' of the model city, 'a reminder of the kinetic effects of cyberwar' which expose 'the many vulnerabilities in the places we take most for granted' (Garber 2013).

SANS Institute director Eric Bessel asserted, when 'you lose control of cyberspace, you lose control of the physical world' (BBC News 2012b). Through illustrations of this argument, these simulations serve to raise awareness and concern, while agitating for increased political action and resource allocation to various government departments and contractors. We should not be surprised that this genre of 'cyber-physical' simulation acts in this way, but there is a deeper logic at work, which aims to restore the 'real' to the 'virtual'. By connecting 'cyber' to the visually comprehensible world of machines, by representing the results of cyber attacks in the language of physical destruction rather than of data ‘breach’ or ‘exfiltration’, these simulations serve to meld the abstracted virtuality of ones and zeroes with the tangibility of pistons and pumps, bricks and concrete. Rather than rely on spatial or martial analogies to demonstrate the realness of the threat to critical infrastructures, this form of representation draws audiences into a non-metaphorical and physical reality that we already recognise from our industrial and urban experience.

In recent years, military exercises have extended controversially into existing urban and peri-urban areas, combining imagined military scenarios with urban ‘realism’, virtuality with physicality. A large-scale exercise on the California littoral in 1999 was described by James Der Derian as ‘a strange beast, a chimera of *Matrix* chips-and-code and *Private Ryan* blood-and-guts’ (Der Derian 2009a: 125). Der Derian wrote further that for ‘one week, on spectacular display, the mother matrix of war spread her wings, revealing the military-industrial-media-entertainment network in all its glory’ (Der Derian 2009a: 125). This ‘MIME-NET’ thesis stresses the convergence of the institutions of (post)modernity, together geared towards simulating, justifying and prosecuting a state of more-or-less permanent war. We might look even further back for exercises with a distinctly public face and mediated aspect that foreshadow the MIME-NET assemblage. Consider Operation Cue, a 5 May 1955 civil defence exercise intended to assess how a ‘typical’ US community would fare after a twenty-nine-kiloton nuclear blast (Federal Civil Defense Administration 1955a). Joseph Masco describes how this settlement was ‘rendered down to the last detail of consumer desire’, from urban amenities to household furnishings to fresh food, with human mannequins ‘posed with domestic theatricality – at the dinner table, cowering in the basement, or watching television’ (Masco 2004: 353–4).

The US Federal Civil Defense Administration recorded the event and its preparations and made available a public information film in which a female journalist – a possibly fictitious ‘Joan Collin’, her name excised from later versions – and male narrator together wove a tale of technoscientific complexity and national solidarity (Federal Civil Defense Administration 1955b). The damage from the blast was predictably extensive but as ‘ritual sacrifice, Operation Cue made visible for a US audience the terror of a nuclear assault while attempting to demonstrate the possibility of survival’ (Masco 2004: 354). Masco identifies the public message of Operation Cue: that surviving nuclear war was ‘a matter of emotional preparation and mental discipline . . . the postnuclear environment would be only as chaotic as citizens allowed’ (Masco 2008: 375–6). This emphasis on ‘survivability’ and the continuing productive agency of the citizen was a reflection of contemporary US nuclear strategy, which for the next decade or so was dominated by a belief in its nuclear superiority and its consequent ability to win a nuclear war.

By the mid-1960s, this unilateral deterrence strategy would give way to the more even-tempered but existentially challenging problems of 'mutual assured destruction' and bilateral deterrence, the refinement of which would form the basis for all subsequent nuclear strategy (Freedman 1981). In 1983, when the television movie *The Day After* (dir. Nicholas Meyer, 1983) was viewed by an audience of 100 million Americans – roughly the same figure that had watched the Operation Cue broadcast – President Reagan's Strategic Defense Initiative threatened to destabilise the hard-won nuclear standoff, and movies had moved into a significantly more pessimistic register that questioned the illusion of survivability.[6] In Britain, *Threads* (dir. Mick Jackson, 1984) abandoned this pretence entirely, being one of the bleakest portrayals of war and its aftermath ever seen on television (Cordle 2013). The great power politics that led to the holocaust of *Threads* are replaced by a 'politics of vulnerability' that lay bare, through its own apocalyptic revelation, the failure of deterrence and the utter dereliction by the state of its responsibility to protect its citizens (Cordle 2013; see also, Garrison 2006).

Studies of the public reception of movies like *The Day After* assess their emotional and political effects differently, but these imagined futures doubtless served at some minimum level to raise awareness of the nuclear issues presented (Feldman and Sigelman 1985; Schofield and Pavelchak 1989). A similar argument might be made of the cyber security exercises above, with respect to the increasing level of public mediation. In the case of the Idaho test-bed, for example, only senior officials were invited to a demonstration of cyber-physical destruction in 2005. In 2007, a test was filmed and presumed leaked to CNN. By 2011, journalists were embedded in the simulation environment from the start. This implies a deliberate media engagement strategy on the part of the Department of Energy, possibly in conjunction with other agencies like the Department of Homeland Security. Government could thereby communicate through professional intermediaries the essential message about critical infrastructure vulnerabilities and the need for political intervention.

In 2010, CNN screened possibly the most elaborate attempt yet to enrol the public in a cyber security simulation. A two-hour special, 'We Were Warned: Cyber ShockWave', hosted by CNN lead anchor Wolf

[6] For an account of Reagan's response to the movie, see Braund (2010).

Blitzer, broadcast highlights of a simulation developed by the Bipartisan Policy Center in Washington, DC, which was played out before a live audience on 16 February 2010 (CNN 2010).[7] The event simulated the effects of malware propagating through the US cellphone network and the cascading failures that subsequently spread through the ICT infrastructure. As the problems piled up, internet traffic slowed, financial markets buckled, transport and power networks failed, public panic rose and, with the news that the attacks appeared to originate from a Russian server, the president did not know whether to adjudge the attacks worthy of a strategic, perhaps even military, response. In the absence of definitive information regarding the perpetrators, with the problem extending beyond national borders, and with domestic pressure increasing, the president charged the assembled mock National Security Council to advise on available courses of action. The participants – all of whom were former White House, Cabinet, military, intelligence or legal officials – concluded emphatically that the United States was insufficiently prepared for cyber attacks and that more administrative powers were required to control national communications networks in times of emergency (Bipartisan Policy Center 2010). These findings echoed the 'lessons learned' of a hundred prior simulations, which is not to dismiss them, but the difference on this occasion was the level of public exposure deliberately built into the exercise.

Blitzer prefaced the programme with the words, 'What you are about to see is not real but the threat is very real indeed', and concluded by saying, 'This fictional scenario we have just seen is certainly frightening, but what is even more frightening is the danger of it potentially becoming reality.' Making people afraid of the threat, however many layers of simulation we excavate from this exercise, seems to have been an important aim. Former Clinton press secretary Joe Lockhart, who played a presidential adviser in the simulation, opined that it would be 'a good thing' if people were discomfited by the exercise, as it would be the only spur to Congressional action (Nakashima 2010). John McLaughlin, formerly acting director of the Central Intelligence Agency, who also took part in the exercise, stated openly: 'People have trouble understanding warnings . . . It was only after September 11 that people could visualize what was possible. The usefulness of the simulation is it will help people visualize [the threat]' (Nakashima 2010). The public were assisted in this by the production itself, a

[7] A transcript is available at http://transcripts.cnn.com/TRANSCRIPTS/1002/20/se.01.html.

mainstream approximation of what a 'hi-tech' situation room might look like, one not too dissimilar from the cyber exercise environments discussed previously. The CNN version differed in its television-friendly appearance, with added futuristic graphics, dramatic overlays, non-stop portentous music and the presence of a real news anchor 'playing' himself.

Cyber security simulations have become more public-facing as the perceived need for public awareness and political action has increased and are an attempt to communicate risk and threat through representations of material damage and destruction more readily accessible to the public – and policymakers – than talk of abstracted 'information security' might on its own achieve. National Geographic Channel's *American Blackout* (2013) dramatised the effects of a cyber attack on the United States, a ten-day electrical blackout accompanied by civil unrest and the collapse of public services. Channel 4's *Blackout* (2013) trod similar ground in the United Kingdom. In their use of film clips from real blackouts, fictional cellphone and handheld camera 'found footage', first-person narratives and unspecified sense of menace, the production values of these movies pay homage to horror films like *The Blair Witch Project* (dirs. Daniel Myrick and Eduardo Sanchez, 1999) and *Cloverfield* (dir. Matt Reeves, 2008).

Media events like these envelop audiences in a sensory world created by the confluence of information technology, media, politics and security. That the real and the irreal, the actual and the virtual, might no longer be separated with certainty is illustrated by CNN's keeping the word 'SIMULATION' permanently on overlay throughout the Cyber ShockWave broadcast. Perhaps mindful of the famous *War of the Worlds* radio drama controversy (1938), in which simulated news bulletins duped millions of Americans into believing they were under alien attack (Cantril 2005), CNN was probably wise to do so. In the absence of research calibrated to doing so, however, it is difficult to assess the effects of these activities on the public imagination or in political outcomes, but this is not the intention of the present claim. Rather, a dynamic has been identified in which there are reasons for suspecting that this increased attention to public intelligibility of threat is manifest in a growing emphasis on attempts to enrol non-specialists into the aesthetic sensorium of cyber security, even if its substantive effects are, admittedly, presently unknown. In the next section, we identify a further dynamic in the relations between people and the state, one that aims to populate cyber security futures through a variety of recruitment and educational tactics that play upon the aesthetics of cyber security.

Recruitment and education

The *UK Cyber Security Strategy* (2011) noted that keeping up with the 'relentless' pace of technological change 'will require people who have a deep understanding of cyberspace and how it is developing', a cadre of professionals it observed was 'a scarce resource across Government and in business' (Cabinet Office 2011: 29).[8] A key component of the £650 million National Cyber Security Programme announced in the document was to remedy this skills shortfall through a variety of government-sponsored programmes, public–private partnerships and new funding streams for academic research into cyber security (see also, Office of Cyber Security and Information Assurance 2012). A year later, speaking at the London Conference on Cyberspace 2012, junior minister Chloe Smith stated even more concisely why these activities were necessary: '[o]ur ability to defend ourselves in cyberspace depends upon a strong skills and knowledge base' (Smith 2012). In the first comprehensive government review of UK cyber security, the National Audit Office reported in 2013 that the 'shortage of ICT skills hampers the UK's ability to protect itself in cyberspace', a situation that might persist for at least two decades (National Audit Office 2013: 26). These and many other statements make a direct link between the national security of the United Kingdom and skills shortages in technical cyber security and allied fields, a situation one government cyber security official described as 'wholly inadequate' (Satter 2012).

In the United States, the dearth of cyber security specialists has become an even more prominent political issue. Both the Pentagon and the Department of Homeland Security (DHS) have stated publicly that the recruitment situation is deleterious to national security. In 2009, DHS announced it would hire 1000 new cyber security personnel, an aspiration subsequently revised down to 400 in the absence of suitable candidates (Beidel and Magnuson 2011). One senior DHS official told conference delegates in a keynote address in March 2013 that his department simply 'can't find enough people to hire . . . we do not have enough people in the pipeline to protect our private sector organizations, critical infrastructure, or the nation' (*InfoSecurity* 2013). As if to prove the veracity of his statement, he left his post shortly afterwards for a private-sector consultancy run by ex-DHS chief Michael Chertoff. The Pentagon's Cyber Command, which became operational in 2010, with responsibility for protecting national and Department of Defense

[8] This statement hides the fact that government had no idea how many people were working in government cyber security at this point (House of Commons Committee of Public Accounts 2011: 10).

networks and for prosecuting offensive ‘cyber’ operations, announced in early 2013 that it was seeking a five-fold increase in its cadre of cyber security personnel from 900 to 4900. It confirmed that this task would be very difficult because of the recruitment situation (Bumiller 2013). The Pentagon recognised that defence budget cuts would compound these problems, not only in making new appointments, but also in retaining existing staff, whether soldiers or civilians. In the short term, then head of Cyber Command General Keith Alexander admitted before Congress that he would find it difficult to staff the forty support and operational ‘cyber’ teams he was committed to providing across the US military by autumn 2015 (Nakashima 2013). Given that thirteen of these teams were, as Alexander pointed out, ‘offensive’, this was a tacit admission not only that the protective functions of national cyber security might be affected by the recruitment situation but that the US military’s capacity to conduct warfighting operations in the ‘cyber domain’ might also be impacted negatively. In the event, even the controversial US defense sequestration of the current decade left federal cyber security relatively unscathed (Collins 2013), although this did not allay concerns about a general cyber security ‘skills gap’.

One of the largest global surveys of information security professionals across the public and private sectors identified three principal drivers of this apparent deficit in skills and personnel. The first was ‘business conditions’ demanding greater attention to information security across enterprise and the public sector; the second insufficient executive-level understanding of information security needs; and the third a lack of appropriately skilled and educated information security professionals (Frost and Sullivan 2013: 12–14). This last factor is a result of a decrease in the volume of computer science graduates and of skills gaps in the existing workforce due to the divergence between the rapid evolution of the ‘threat landscape’ and the capabilities necessary to counter it. For governments, this situation is compounded by the founding of new and expanded public-sector institutions requiring substantial volumes of new hires and the persistent inability to retain or recruit staff because of a substantial wage disparity with the private sector. This has put government departments into competition for skilled personnel with the private sector and with one another. In 2012, for instance, GCHQ told Parliament that these considerations meant it was losing suitably trained and experienced staff at three times the rate of the corporate sector (Intelligence and Security Committee 2012: 67).

These labour market conditions are not especially new, nor are they restricted to cyber security. Governments have long recognised that fast-moving scientific and technological fields provide great opportunities for employment and economic growth but are hindered by the inability to fill these positions (e.g. House of Lords Select Committee on Science and Technology 2012). In 1968, the UK Committee on Manpower Resources for Science and Technology reported to Parliament on the relations between emerging computer technologies and the labour market. The Committee noted that it was common for technicians to struggle to adjust to 'more modern ideas' as they aged. The novelty of the situation lay in the 'considerable intellectual strain' put upon the managerial class by the computing revolution; their education had given them 'no hint of what the future held for them' (Committee on Manpower Resources for Science and Technology 1968: 101). When that cohort of professionals was in education, such was the pace of scientific and technological change that the basic intellectual foundations of some fields did not form part of it. This has changed since the 1960s, with far more people graduating with computer science degrees and professional information security qualifications now than would have been imaginable then, but recruiting enough skilled people is still a challenge. Government-driven initiatives to rectify this situation are key aspects of national cyber security policies. Three categories of activity concentrate on particular types of individuals potentially amenable to careers in cyber security: respectively, existing professionals, 'hackers' and young people still in education.

The first category is an attempt to populate the emerging cyber security landscape by recruiting mid-career professionals from related fields or by retraining people interested in technical careers or any number of support roles in 'project management, law enforcement, training and development, risk analysis, policy and business' (Office of Cyber Security and Information Assurance 2012: 33; HM Government 2014a). New certification schemes underwritten and administered by GCHQ support this recruitment drive by providing 'cyber professionals' with a clear sense of personal progress along their chosen career paths (CESG 2012). Open competitions, like Cyber Security Challenge UK (CSCUK), and the US Cyber Challenge (USCC) initiative after which it is modelled, aim to raise awareness of cyber security as a career option, while providing training, bursaries, work placements and, sometimes, job offers to those who win the various classes and categories of competitions held each year.[9] These public–private partnerships present a strong sense of civic responsibility and engagement. The CSCUK, for example, intends to satisfy the

[9] As of March 2013, only 40 of the approximately 7,000 participants across four iterations of CSCUK had been offered employment in cyber security. CSCUK stresses its role in raising awareness of cyber security, as much as its direct impact on recruitment (Shah 2013).

national demand for a larger and more dynamic cyber security workforce to defend cyberspace, which is 'integral to our economy, our communities and our security'.[10] The aim of the USCC is 'to find 10,000 of America's best and brightest to fill the ranks of cybersecurity professionals where their skills can be of the greatest value to the nation'.[11]

This civic renewal is prominent in the second category of activity, which in its desire to 'rehabilitate' hackers is one of the more unconventional aspects of the search for cyber security 'talent'. In 1999, IBM's head of corporate security stated that his company would never hire hackers, no matter how 'reformed' they might be: 'It would be like hiring a burglar to institute [*sic*] a burglar system on your house. You wouldn't do it' (National Infrastructure Protection Center 1999). This reflected a common perception of hackers as 'anti-social, possibly dangerous individuals. ... the new enemy of the Information Age' (Nissenbaum 2004; Halbert 1997). Ten years later, UK security minister Lord West articulated a different perspective on hackers and their misdemeanours. 'If they have been slightly naughty boys, very often they enjoy stopping other naughty boys', West said, hinting that this might be sufficient for them to be considered appropriate recruits to the new Cyber Security Operations Centre at GCHQ (Gardham 2009). West suggested that government would not recruit any 'ultra, ultra criminals', but his comments elicited a predictably negative reaction from the information security community, ranging from outright derision to incredulity. One chief executive wondered if this were not just 'some kind of huge joke ... Putting these amateurs, who have no formalised knowledge or training, in charge of national security beggars belief' (Chapman 2009).

We might perhaps expect these reactions, given the long and ongoing struggle between the computer security industry and the 'computer underground' of hackers and crackers, and their divergent understandings of what constitutes acceptable behaviour in computer networks (Taylor 1999). Despite their similar skill-sets and fields of knowledge, there is an antagonism between the two 'communities' – as loosely defined – that frequently crystallises around the 'moral certainties' of 'us' and 'them', echoing the binary language of computing itself (Taylor 1999: 137). Hackers may have 'potentially useful knowledge', writes Athina Karatzogianni, but this does not coincide with business and the academy's preference for 'ethically unproblematic and rigorously researched knowledge' (Karatzogianni 2006: 98). This has not prevented governments from

[10] http://cybersecuritychallenge.org.uk/about-us/overview/.
[11] www.uscyberchallenge.org/our-mission/.

attempting to recruit ‘hackers’, and Lord West’s suggestion is consistent with other governmental efforts in this regard (Libicki *et al.* 2014).

Every year since 1993, the DEFCON convention in Las Vegas has been one of the largest meetings of hackers in the world and for most of its history has run a ‘Spot the Fed’ competition, in which delegates win prizes for alerting conference organisers to the presence of persons thought to be federal agents (Holt 2007: 193–4; Urbelis 2005: 976). Observers have long suspected that hacker groups have been infiltrated by government agents and that hackers themselves have provided sensitive and legally actionable information on their colleagues’ activities to law enforcement and the FBI, sometimes under duress (Pilkington 2011). ‘Spot the Fed’ was in part a reaction to this situation and also served to reinforce the boundaries between the ‘black hats’ of the hacker community and the ‘white hats’ working for government.

DEFCON attendees still play the game, but it has lost some of its piquancy, particularly since DEFCON 7 in 1999, which hosted a ‘Meet the Fed’ panel for the first time.[12] This popular event allowed government security personnel to address the hacker community directly, informing them of their work for government and making open recruitment pitches to the good-natured – if boisterous – audience. The author attended a DEFCON panel in 2009 with speakers from the Department of Defense, Department of Homeland Security, NASA, National Security Agency, Treasury, US Postal Service and others.[13] These overt activities intend to turn ‘black’ into ‘white’ in the interests of national cyber security, not an unreasonable goal considering their skills and knowledge. We cannot yet determine the success of this initiative, but we can suggest it has some efficacy given the willingness of federal employees to attend DEFCON and other conferences year after year in this capacity, including, in 2012, the head of the National Security Agency and US Cyber Command General Keith Alexander (Colon 2012). The well-publicised transformation of, inter alia, Kevin Mitnick from America’s ‘most wanted’ hacker to jailbird to security consultant and public speaker also provides role models for those considering a switch to ‘legitimate’ careers in government and commercial cyber security (Mitnick and Simon 2011). This might prove to be a harder sell after Edward Snowden’s uncovering of federal surveillance programs, to which DEFCON organisers responded by suggesting ‘the feds’ stay away from the conference for a while (Stevens 2013b).

[12] DEFCON 7, Las Vegas, NV, 9–11 July 1999, www.defcon.org/html/links/dc-archives/dc-7-archive.html.

[13] DEFCON 17, Las Vegas, NV, 30 July–2 August 2009, www.defcon.org/html/links/dc-archives/dc-17-archive.html.

The key issue of legitimacy is expressed through the current attention to ‘ethical hacking’, the development of which is an aim of the 2011 *UK Cyber Security Strategy* (Cabinet Office 2011: 29). It is even possible to obtain professional certification as a ‘Certified Ethical Hacker’, although one leading computer security specialist dismissed this nomenclature as a ‘contradiction in terms’ equivalent to ‘ethical rapist’ (D’Ottavi 2003). In June 2013, the United States held its first National Day of Civic Hacking, organised by ‘Code for America’ and supported by a range of public- and private-sector organisations. This event encouraged people to address civic challenges through ‘data, code and technology ... to do what is most quintessentially American: roll up our sleeves, get involved and work together to improve our society’.[14] The organisers were keen to distance themselves from the negative connotations of hacking, a hacker being instead ‘someone who uses a minimum of resources and a maximum of brainpower and ingenuity to create, enhance or fix something’. This is broadly in agreement with long-established self-perceptions of hackers, but what is different in these discourses of ‘ethical’ and ‘civic’ hacking is that the parameters and aims of ‘hacking’ are decided not by ‘hackers’ but by government and commercial interests which fix and patrol its ethical and legal boundaries. This is an appropriation of the term in its technical dimensions and a deliberate excision of much of the spirit of hacking as an exercise in personal autonomy and political agency (e.g. Taylor 1999).

The third category includes attempts by organisations like CSCUK to engage schoolchildren and students through educational initiatives and other means through which cyber security is presented to young people as a valuable career path and ‘life skill’. In May 2012, the UK government’s special representative to business for cyber security told delegates at an IT security conference, ‘[t]here are far too many people over 40 working in this area and not nearly enough in their twenties’ (Nguyen 2012). This observation is supported by survey data, with only 7% of cyber security professionals aged between twenty and twenty-nine years old (e-Skills UK 2013: 13). Echoing the concerns of the Committee on Manpower Resources for Science and Technology some forty-five years previously, she articulated government worries about the prospect of Britain being unable to defend itself in future due to a lack of young people channelled into the cyber security employment ‘stream’. ‘If we want to get people interested, it needs to start in schools’, she said; people ‘need to know this activity has a future and a framework’ (Nguyen 2012). This emphasis on educating children and young adults in cyber security is a distinct feature

[14] http://hackforchange.org/about.

of UK cyber security policy and provides not only a framework and a future for cyber security careers but a framework for the future of cyber security itself.

Through its 'University Cipher Challenge', CSCUK already engages with universities and colleges, pitting computer science departments against one another as a way to showcase their skills and build their reputations.[15] Several of its sponsors are well-respected computer science departments at major British universities. This complements new government funding of doctoral candidates, the naming of eleven Academic Centres of Excellence in Cyber Security Research at British universities and new training programmes in cyber security at major universities (HM Government 2014b). In April 2013, CSCUK announced its intention to extend its competition format into secondary schools, citing the search for 'raw talent' and the need to raise awareness of cyber security as a career path, particularly among young women. A pilot programme starting in autumn 2013 would target 2000 secondary schools, before expanding it across England and Wales in 2014 (Hopkins 2013). The BBC described the scenarios encountered by these youthful participants, which would be familiar to existing cyber security professionals:

> In one scenario, they are told that they face a nuclear threat. They are split into two teams and are told to break into the IT systems of each other's nuclear plant. People frantically tap at their keyboards trying to stay one step ahead. When a team loses, sirens go off and TV footage shows their nuclear plant in flames. (Ostroff and Taylor 2012)

The 2014 Cyber Security Challenge was launched by Cabinet Office Minister Francis Maude, who invoked the need to 'get ahead in the global race' (Ashford 2014), thereby linking cyber security firmly with the Conservative mantra of a time of national reckoning. In April 2012, the Minister for Universities and Science noted a 'decade-long decline' in IT and computer science education in British schools and universities and confirmed that Government was committed to making these fields once again the 'exciting, cutting-edge' subjects they should be (Watson 2012). In September 2014, the existing national ICT curriculum was replaced by 'Computing', to allow schools to choose more innovative and creative ways of teaching ICT, an announcement stressing economic competitiveness and the need for public–private partnerships (Department for Education 2012).[16]

[15] https://cybersecuritychallenge.org.uk/education.php.

[16] The term 'ICT' was discarded, as it carried 'negative connotations of a dated and unchallenging curriculum that does not serve the needs and ambitions of pupils' (Department for Education 2013).

Moving away from a teaching model centred on office software packages, the reinvigorated computing syllabus emphasises the desirability of online training programmes, a more interactive pedagogical environment and the need and opportunities for programming and application development. It reflects the changing ICT environment outside the classroom and in the homes and future workplaces of a new generation of schoolchildren, although it has been criticised as too focused on computer science at the expense of more creative computer use and general digital literacy (e.g. Marshall 2013). This reorientation of ICT teaching is still in its early stages and it is presently unclear to what extent cyber security will form part of the emerging curricula, although government references to improving 'cyber security education at all levels' suggest that it may yet become formally integrated into ICT education (Cabinet Office 2011: 31). There are, however, indications that cyber security is already being taught, or at least addressed, at both secondary and primary levels of education.

A 2012 report by the Information Assurance Advisory Council in conjunction with the Cabinet Office recorded that police had been in schools talking to seven- and eight-year-olds about cyber security, although no details were provided that corroborated this claim (Information Assurance Advisory Council 2012: 8). The same report advised that information security should be built into teacher training qualifications, informed by the need to 'spread security metaphors without making people scared'. The analogy is drawn between cyber security and road safety: 'Appropriate education at all levels is like a kerb drill for cyber security.' The government-sponsored body charged with developing technology skills for business, e-skills UK, developed 'Behind the Screen', a project preliminary to the development of a general secondary certificate in computing.[17] Cyber security is one of the topics directed at fourteen- to sixteen-year-olds through free online resources developed in conjunction with multiple industry partners:

> The 'Cyber Ninjas' project allows students to progress through seven challenges collecting belts as they go, and foiling the machinations of Nemesis and his Henchman as they try to breach the security of Cyber City School. Supported by infographics, games, comic books and audio guides, the content covers awareness and planning; cyber crime and computer forensics; security practices and principles; safety, privacy and ethics and online interaction . . . Score too little and you go to the Dark Side! (e-skills UK n.d.)

There are many other informal, private sector and civil society-led initiatives beginning to engage with schoolchildren of all ages, although there is

[17] This scheme is now known as TechFuture Classroom, www.techfutureclassroom.com/.

little formal coordination of these activities at present. The emphasis on 'safety' rather than 'security' is an existing facet of ICT education, and 'child internet safety' has been part of the National Curriculum for some time. Organisations like the Child Online Exploitation and Protection Centre (CEOP) and the UK Council for Child Internet Safety (UKCCIS), and initiatives like Get Safe Online, already provide outreach to schools and communities, maintain online information resources and run helplines for concerned pupils and parents. Lest these be thought excluded from the purview of cyber security, all three are mentioned in the most recent *UK Cyber Security Strategy* (2011) as models of progressive child online safety and protection and categorised as an aspect of cyber security concerned with personal internet safety. Government public information campaigns to raise awareness of online fraud and other crime, safe browsing and general advice on internet safety are an important category of state action, but space precludes their discussion here.

What we cannot yet tell is how the relations between 'safety' and 'security' evolve in cyber security practices and policies aimed at children. At what point does the emphasis shift from children learning how to protect themselves and their friends to them being enlisted in a wider project to protect society? Older pupils have demonstrated their willingness to use their skills and enthusiasm for the public good, and surveys indicate there is no shortage of university students wanting to work for intelligence agencies. In 2012, MI5, MI6 and GCHQ all appeared in the top ten of employers for whom IT graduates would like to work (Savvas 2012). Through the practices outlined in this section, cyber security is presented not only as a potential career but as a social need and as the foundation of a secure nation, the responsibility for which is being increasingly shifted 'downwards', in demographic terms (Stewart 2014). We can read attempts to look ever earlier in the education system for cyber security 'talent' as part of a renewed privileging of science, technology, engineering and mathematics (STEM) subjects across the educational spectrum. However, the emphasis on security raises questions about who exactly is being asked to be an agent of security and what their responsibilities might be.

What to make, for instance, of a partnership between CSCUK and defence contractor Northrop Grumman, dubbed CyberCenturion, aimed at channelling secondary pupils into careers in the defence sector (Curtis 2014)? The competitive format, using software developed by the US Air Force for its CyberPatriot programme, offers internships to the winners and free passes to industry conferences. Is this just a recruiting drive, or a more problematic imbrication of national security and youth education? This is a pertinent issue given the potential recruitment of children unable to give their consent in other fields of social life and connects to deeper issues about the delegation of security responsibilities from state to citizen in related practices like resilience, what David Chandler has termed the biopolitical ‘societalization’ of security (Chandler 2013). When press reports of the cyber security industry sending ‘recruiting officers’ into schools begin, ‘[a]t a school in south London, a class of 15-year-olds has been told that the future of online defences is in their hands’ (Warrell 2014), we should perhaps begin to question more vigorously this process and its ethical implications.

Inhabiting the future

This chapter has outlined practices that attempt in various ways to ‘inhabit the future’ as a way of preparing for the unpredictable and the unknowable. This emphasis on the human serves to reinforce the fundamental insecurity of computer networks. As the global survey quoted earlier emphasises, human factors are far more important to information security than technical aspects, with suitably qualified security professionals being adjudged almost twice as important as hardware, for instance (Frost and Sullivan 2013: 10). This underscores both the socio-technical nature of IT networks and their insecure design: if ‘perfect’ cyber security were possible, or a satisfactorily high level of security were attainable, the human factor would probably be diminished as technical security increased in efficacy. That governments and businesses actively attempt to populate the cyber security assemblage is a function both of the illusion of technical security and of the sociality of information infrastructures. People are not mere additions to information systems but active participants in wider social, economic and political systems that find expression through cyber security practices.

This chapter drew attention to high-level simulations and exercises that operate beyond public view and which drive and corroborate narratives of cyber insecurity while preparing personnel for future eventualities, catastrophic or otherwise. They serve important institutional functions in training professionals to respond efficiently and effectively while identifying organisational and technical issues that can be rectified through further systems development and training. These practices allow people and organisations to rehearse future events and bring the future into the present as something that can be experienced and inhabited in a metaphorical register. This is enabled by the creation of simulated worlds that replicate situations and scenarios through a variety of aesthetic modalities involving a wide range of senses. In this way, the 'imagined' crisis becomes the 'believable' crisis, as is the intention of all training environments.

These rarefied and highly technical environments and the lessons drawn from them are often difficult to communicate to the non-specialist – including policymakers – and to the public. In order to foster greater public and political awareness of cyber security issues, it has become necessary to find other ways to represent cyber security issues, particularly through translating the 'virtual' into physical and material terms appealing to the non-technical observer. Journalistic media are an integral part of this process, invited to attend demonstrations of the physical effects of cyber attacks and acting as the principal conduit through which to communicate the sense and outcomes of exercises like Cyber ShockWave. These operations are obviously simulations, but they engage the public through televisual media that deliberately blur the boundaries between the real and the imagined, presented not only as 'believable' but also perhaps 'likely'. Under these conditions, cyber security may be more readily identified as a valid object of politics and public policy. We are all asked to inhabit these simulated futures through the mediated present, an enrolment into a complex assemblage of media, technology, politics and security.

Both these forms of preparatory practice bring the future into the present. The third form of practice discussed in this chapter augments the logic of securing the future with a different temporal dynamic – that of projecting the present into the future. In contrast to the metaphorical inhabitation of the future in our lived present, recruitment and education mean to populate – in a literal sense – the future with cyber security personnel. By starting people onto cyber security career paths ever earlier in the education system, there emerges a class of practice that both prepares *for* the future and prepares the future itself. The persons enlisted into cyber security are those people who will have agency in the future, rather than just experience simulations of the future in the present. We might make a similar argument of existing cyber security personnel, in that they too will act in the future, but the political emphasis is on constructing children and young people not only as future agents of state and commercial cyber security but as the future itself. As the cliché goes, children *are* the future, a future that we can only partly share and shape, a generational issue that finds expression in cyber security as much as it does in almost every other field of social action (White 2013).

However, this is a political operation in another important sense. We are not attempting so much to control the future of children as to cast them in our own image, or at least to project our politics of the present into the future. Walter Benjamin observed of education:

> [W]ho would trust a cane wielder who proclaimed the mastery of children by adults to be the sense of education? Is not education, above all, the indispensable ordering of the relationship between generations and therefore mastery, if we are to use this term, of that relationship and not of children? (Benjamin 1979: 104)

We cannot predict or control what the young will do in the future, but we can try to shape the conditions in which they will live, based upon our own suppositions and preoccupations. Cyber security presumes a rather dark future unless we channel our children into cyber security now. In this sense, as Benjamin suggests, we attempt to 'master' our relations with children, rather than the children themselves. British newspaper *The Guardian* traced the line from the present to the future in reporting on James Millican, a first-year university student crowned the United Kingdom's 'Cyber Security Champion' after winning the Cyber Security Challenge in 2012:

> And though he may not recognise it yet, Millican has become a small player in a global game. There is a dotted line that links him to an ideological battle over the future of the internet, and the ways states will use it to prosecute conflicts in the 21st century. (Hopkins 2012)

The implication is that although Millican might be unaware of the future trajectory of cyber security or of the historical dynamics of inter-state warfare, we are more worldly and have chosen to place him in a position to do in the future what we cannot in the present. We cannot control him in the future, but we are creating the conditions through which he may act in our image and in our name. Yet we are impatient with youth, the Office of Cyber Security and Information Assurance (2012: 33) stating: 'We cannot afford to wait until further generations of graduates are trained and ready to take up employment.' For this reason, we seek to recruit from our own generation but only as a stopgap while the young are trained and developed.

In conclusion, in common with all fields of security, cyber security communities enact various forms of preparedness, anticipatory forms of security governance that seek to envelop participants in an aesthetic sensorium that allows them to inhabit believable simulations of imagined futures. This chapter has described some of these practices, their aesthetic characteristics and organisational logics, and it has proposed some possible future developments. Importantly, it has extended our understanding of what inhabitation might mean in non-metaphorical terms, through the active population of the future by recruitment and education. We cannot tell what events and insecurities will emerge, but these modes of inhabiting and populating the future serve to construct the future not only as something which will happen and for which we must be prepared but as something over which cyber security communities can exert some limited agency. However, this is only by devolving responsibility to a future generation we cannot control but whose potentialities cyber security communities can attempt to constrain through practices that accord with their imagination as to what the future holds and requires.

7 Cyber security and the politics of time

Logics and chronopolitics

Chapter 2 introduced the concept of chronotype as a way of approaching the social epistemology of time. Social epistemology is concerned with the intersubjective construction of knowledge in human collectivities, including communities of cyber security practice. Chronotypes are the 'models or patterns' expressed by communities 'through which time assumes practical or conceptual significance' (Bender and Wellbery 1991: 4). Previous chapters have addressed diverse chronotypes of cyber security, the ways in which past, present, future and other aspects of temporality like speed, acceleration and history are imagined and expressed by members of cyber security communities. These chronotypes, further understood as narratives expressing how given communities imagine time and temporality, are not mutually exclusive and together comprise the complex heterogeneity of the sociotemporality of cyber security. This sociotemporality, as the framework of emergent temporality implies, emerges in human cognition and includes the temporalities of nonhumans, matter, energy and information. As narrative strands, however, these are principally stories that cyber security communities tell about themselves and their worlds. Our discussions have explored the political implications of each chronotypical imagining, but one more analytical step is necessary to look in more detail at the chronopolitical logics of cyber security.

In the present context, what do we mean by invoking the term 'logics'? For Richard Grusin, logics are 'tendencies that emerge from and within particular historical practices and assemblages', and from which 'competing or contradictory logics or illogics' can also be recovered (Grusin 2010a: 5). The logics of chronopolitics are those 'tendencies' that derive from the chronotypes we have previously identified and discussed as elements of the cyber security imaginary. They reflect those aspects of these chronotypes that are common to all or that emerge most strongly from the chronotypical assemblage that together informs the chronopolitics of cyber security. They are the dominant logics identified through analysis, rather than a complete model of the chronopolitical logics of cyber security.

Logics are organising principles through which cyber security assemblages coalesce and persist and that together shape the chronopolitics of cyber security. In this way, they are semi-stable forms that are themselves extensible in time. These logics enable the political pursuit of cyber security as a condition and a process, as a state of order and the techniques through which to achieve it, and reveal the fissures and inconsistencies in cyber security in which further political energies arise. It is the task of this chapter to identify, discuss and critique these logics with respect to the larger cyber security assemblage and within the broader contexts of politics and security. The four logics – assemblage, real time, event, *eschaton* – complement and contest one another in various ways but together comprise one interpretation of the chronopolitical manifold of cyber security. The chapter concludes with a discussion of the importance of recognising the heterogeneous nature of the chronopolitics of security.

The logic of assemblage

Cyber security is an assemblage, a dynamic web of human and nonhuman entities, entangled in multiple ways and from which particular temporal tendencies emerge. The logic of assemblage displays distinct temporal characteristics of relevance to the chronopolitics of cyber security. The first temporal aspect of assemblage is closely bound with its etymological origins. An assemblage is not a mere 'thing' that just *is* but an assemblage of things, both human and nonhuman, that *becomes*. The dynamism of this concept is not wholly captured in the modern English noun 'assemblage', a sense that passed from English with the early modern obsolescence of 'assemblance', whose active inflections better represent the nature of the object it described. 'Assemblage' was reintroduced into English from French social theory in the late twentieth century, as a ready translation of *agencement*. Again, many of the active connotations of the root verb *agencer*, 'to arrange, to fit up, to combine, to order', have been somewhat lost in transition (Law 2004: 41; Phillips 2006).

In Deleuze and Guattari, we read of the condition of *agencement* as a 'state of intermingling of bodies in a society, including all the attractions and repulsions, sympathies and antipathies, alterations, amalgamations, penetrations, and expansions that affect bodies of all kinds in their relations to one another' (Deleuze and Guattari 2004: 99). 'Assemblage' implies more than its standard usage in English and its relatively recent theoretical resurgence reconnects with its linguistic heritage to describe an aggregate entity in a state of permanent change, a distinctly

Heraclitean temporality of perpetual Becoming. Change is a condition of the existence of an assemblage, whose identity is necessarily historically contingent and under constant renewal. The cyber security assemblage with which we are concerned exists in a temporality of continual change, but it is insufficient to assert this without enquiring further as to the nature and character of this temporality.

To invoke Heraclitus is to reflect upon the caricatures of his original, admittedly often cryptic, philosophy of flux. Plato reported of Heraclitus that 'you cannot step into the same river twice' (Ademollo 2011: 203). Not only is the river different when you revisit it – the waters you previously touched have long passed – but so are you: you are altered and changed since the last time you stood upon the riverbank. This has been taken erroneously to mean that there is no correspondence between the 'two rivers' and the 'two yous' and is therefore logically absurd and an affront to common sense. Against these criticisms, Heraclitus proposes a deeper truth: that change and permanence co-exist – you and the river are both different and the same at each temporal remove. No object retains all its characteristics and properties from one moment to the next, but many of its aspects persist across time, including human identity, which vexed the ancient philosophers greatly.

We should read Heraclitus not as an assertion of the opposition of constancy and change but as a paradoxical unity of the two: change as the condition of constancy. The human body – from Aristotle to Deleuze and beyond – only exists by dint of its continuous metabolism, just as stars only remain stars through the continuous violence of thermonuclear fusion. For Heraclitus, writes Nicholas Rescher, 'reality is at bottom not a constellation of things at all but one of processes' (Rescher 1996: 10). Rather than subscribing to a post-Platonic perversion of perpetual flux, in which processes portend Heraclitean change and transformation as agents only of disintegration and instability, we should understand change as a process also of formation and stabilisation. Manuel DeLanda, a prominent interpreter of Deleuzean ontology, describes how an assemblage 'can have components working to stabilize its identity as well as components forcing it to change or even transforming it into a different assemblage' (DeLanda 2006: 12). Jane Bennett, too, speaks of assemblages as 'living, throbbing confederations' of humans and nonhumans that are 'able to function despite the persistent presence of energies that confound them from within' (Bennett 2010b: 23–4). An assemblage exists in a temporality expectant of change and contingent upon change, which serves to maintain and to modify its character. This does not imply, however, that it must always be in flux, or at risk of losing its identity, even as no assemblage can be said to be eternal either.

In thinking about cyber security, we need to consider how the cyber security assemblage changes and, most importantly, how it maintains its identity and extends itself beyond its present configuration. Calls for ‘more’ and ‘better’ cyber security imply both an extension of its components and ameliorative changes in its values. Both can be explored through the ways in which assemblages (re)produce themselves in space and time, as they must in order to fulfil their ontological obligation of continuity through change. Latour points out that it is insufficient to explain the workings of political phenomena like cyber security by simplistic recourse to ‘power’ as a unitary social force that somehow explains these phenomena, an ‘endless and mystical task’ that obscures as much as it reveals (Latour 1990: 56). ‘Power’ is only effective anyway through endless ‘complicities, connivances, compromises and mixtures’, none of which is explained by power itself (Latour 1988: 175). For Latour, the logic of assemblage – or, in his related formulation, the ‘actor-network’ – is how it extends its scale through the addition of human and nonhuman actors and maintains its continuity of identity through the repeated ‘performance’ of the links between these agentic nodes in his networks.

The cyber security assemblage extends itself continually, not least because of changes in the information-technological networks that comprise one of its principal referent objects. As the information infrastructure grows daily, as increasing numbers of consumers, businesses and institutions are connected by it, as more services are provided across it and as unimaginable volumes of information are created and transmitted through these interactions, the global ‘landscape’ that influential actors wish to regulate through cyber security practices grows larger and more complex. Cyber security lays claim to this global environment as its field of responsibility, but it is clear that when ‘the spatial domain is conceived as being global in reach, this suggests indeterminate spaces somehow defiant of order and control, transcendent of space and time [and] a source of risk and danger’ (Jabri 2006: 57). Cyber security actors cannot rest while these ‘indeterminate spaces’ exist, particularly as the emergence of the ‘global’ means ‘that which constitutes the internal is now rendered in terms of humanity at large’ (Jabri 2006: 59). The ‘ubiquitous’ cyber threat so often referred to is ubiquitous in the sense that information technologies, even if they do not make the internal/external dichotomy quite as irrelevant as sometimes supposed, at least construct threats emanating from anywhere in the world as national security issues due to their possible effects on domestic assets or populations. It is also the case that threats arising internally may become globalised rapidly, an additional burden upon any state keen not to attract opprobrium from the international community. Governments are required to respond and extend the cyber security assemblage in the hope of regulating both the 'indeterminate spaces' from which these risks emerge and the global flows of information that mediate these dangers.

Characterising 'cyberspace' as a global 'domain' establishes the legitimacy of the state to extend control over this environment (Stevens 2013a), but there are multiple methods through which this is attempted. New software is created to effect change in information systems, either through protecting one's own or by creating insecurity in others'. New modes and doctrines of warfare are explored, tested and refined. New laws, treaties, memoranda of understanding, policies and regulatory instruments are drafted, discussed and implemented. New institutions arise and gather to themselves material and immaterial resources for the prosecution of civil, industrial, intelligence and military activities. New buildings are erected to house them. Through these actions, new links are created and through their repeated performance the boundaries of the cyber security assemblage are extended and stabilised, however temporarily. Through these processes, too, the identity of cyber security is reaffirmed and reinscribed in political discourses of security. Crucially, humans are enfolded into the cyber security assemblage through their existing professions, positions and responsibilities and through the forms of recruitment narrated in Chapter 6. These are responses to the problems of increasing cyber insecurity caused both by the changing information-technological landscape and the activities facilitated by it, including war, crime, terrorism and espionage. In sociological terms, people are 'recruited', 'mobilised' and 'enrolled' into the cyber security assemblage (Latour 2005: 218; Callon 1986).

In the recruitment of humans to causes like cyber security, language is an important catalyst, either through the articulation of reasons, 'exemplified by traditional values or personal emotions', or motives, 'a special kind of reason involving explicit choices and goals' (DeLanda 2006: 22). These act as cognitive triggers to the behaviour of others, in which they decide to adopt a particular course of action aligned with those reasons or motives or not. In cyber security, the reasons are straightforward and expressed in terms of national security: the information systems on which our societies depend are under threat and we need *your* help to maintain *our* way of life. Appeals to history and national memory are deployed to spark social conscience and citizens are presented with a choice: whether to exercise their civic duty or not. To use one's abilities in the national interest is to be 'ethical'. To elect otherwise is to invite one's motives to be questioned. Many people answer these calls, as shown by their willingness to compete for selection by industry and governments, both in situations framed as 'contests' and 'competitions' and through the systemically competitive job market. The inability to convince or coerce people into the cyber security assemblage is a serious issue for cyber security actors, states especially, who are increasingly disposed to seeing themselves as being unable 'to go it alone' (Dunn Cavelty 2008: 137). The cyber security assemblage and its effectiveness in achieving the ends for which it exists can only be maintained by continuing to 'enrol' actors into its networks, and the sometimes unproductive nature of discursive catalysis helps to explain why securitisation moves often fail.

However, actors do more than situate themselves in the spatial topologies of the cyber security assemblage. Everyone enrolled in cyber security gives their skills, experience and labour but also their time. While this is frequently consensual, or at least contractual, this relationship is one in which an assemblage attempts to extend itself through the 'appropriation of the time of others', a key facet of chronopolitics (Rutz 1992: 7). The standardisation and increased commodification of time as a necessary condition of global capitalism are matters of substantial intellectual attention, and although the precise dynamics are disputed there is general consensus, as Anthony Giddens observes, that the discipline of human affairs 'can proceed only via the manipulation of time and of space' (Giddens 1984: 145). The logic of the assemblage and the logic of capital coincide in their reproductive aspects, especially as cyber security is promoted by governments and businesses as a driver of economic growth. In this respect, the time of labour is inevitably appropriated by cyber security interests.

Cyber security actors also attempt to appropriate the time of those who cannot yet offer their labour in exchange for economic compensation. Claims are made on the time of young people in secondary education, for example, who will be identified, inspired and enabled in order to help Britain get ahead in the 'global race' (Brewster 2012). The language of 'digital natives' and 'digital immigrants' frequently serves as a crude proxy for differentiating between, respectively, younger and older generations' abilities to live with and understand contemporary and emerging information technologies (Prensky 2001; Bennett *et al.* 2008). Younger 'digital natives' are perceived as better placed to instinctively engage with 'cyber' issues, a characteristic desirable to government and industry. The younger generation becomes 'the next generation of cyber professionals' (Chertoff 2008a: 482), through which the future will be shaped. In order to shape the future, the time of young people must be appropriated now, through the various constraints and opportunities created on their behalf (King 2010). As concerns grow about future cyber insecurity, the cyber security assemblage reaches further into the education system, from tertiary to secondary to primary, finding new modalities through which to extend itself, temporally and spatially.

The logic of assemblage is a fundamental aspect of the sociomateriality of cyber security. Assemblages are in a state of constant renewal as a mode of existence, a purposive logic that presupposes the intent to reproduce. Cyber security communities seek to continue their existence through many different means. They achieve this not only through the enrolment of ever-greater numbers of actors into their networks but also through the absorption of multiple temporalities into these networks. The sociotemporality of cyber security communities is itself a temporal assemblage, an assemblage of the times of humans and machines, of energy and information. The logic of assemblage propels this heterogeneous collectivity forwards in time: it is ultimately a temporal imperative to survive.

The logic of real time

In the chronotypes expressed by cyber security communities, several claims about the temporality of the contemporary world emerge. For instance, they stress the uniqueness of the present time in world-historical terms. We are in the early stages of a radical transformation in the structures of global life and as a species we are experiencing the natal spasms of a new ‘information age’, a revolution on a par with the prehistoric agrarian revolution and the Industrial Revolution of the eighteenth and nineteenth centuries. Cyber security identifies speed as the ontology of revolutionary postmodernity, a source of socioeconomic opportunity and political advantage, and hence also the object of desire. Speed is also a globalised vector of risk and threat, to be feared and countered. The acceleration of the rate of technological change intensifies these opportunities and problems, causing a relative deceleration in decision-making capabilities, making timely political effort all the more necessary and also potentially ineffectual or unachievable. Caught in a schizophrenic temporality of acceleration and deceleration, cyber security actors are permanently anxious in the knowledge that politics and practice cannot match the pace of sociotechnical change. The near-future comes to dictate all political actions and cyber security becomes obsessed with the present, cutting itself off from the past and the longer-term future in its increasingly desperate attempts to regulate that which cannot be regulated, existing in an extended present in which the future beyond the now is increasingly unimaginable and unrealisable (Nowotny 1994). Its temporal horizons become foreshortened and the politics of cyber security threaten to dissolve in a temporality of pure and inertial ‘nowness’, in which humans are no longer able to exercise political agency in a world of unimaginably fast technological decision-making and action.

This deep concern with speed and acceleration closely resembles the ‘real time’ of Paul Virilio. Virilio posits the existence of a tyrannical regime of technological temporality in which democratic politics is replaced by ‘dromopolitics’, the automated exercise of the political resource of speed, in which place, identity and ethics erode through the paralysis caused by ‘the real-time conductivity of images and information’ (Virilio 2000: 76). We can plausibly propose that the politics of cyber security are not yet so in thrall to speed and acceleration that there remains no space for the exercise of ethical judgement and meaningful politics. ‘Politics’ in this context is not necessarily Western liberal democracy but political systems in which government is at the very least non-violently responsive to public needs and desires. However, the increased automation of technical defence and offence, the possible shift of cyber security political decision-making from legislature to executive and a general sense that existing political structures and institutions are inadequate in the face of sociotechnical acceleration mean that the logic of real time is appreciable in the ongoing political development of cyber security.

The logic of real time is not something that necessarily wholly reflects empirical reality but a tendency that emerges from the cyber security assemblage and acts as one organising principle in the politics of cyber security. It is as much socially constructed as any aspect of chronopolitics, albeit one that plays close attention to the temporalities of nonhumans. The perspective of real time cleaves to a narrative that prioritises the temporalities of information technologies, principally registered through the high speeds of information transmission in computer networks. The time of human actors, therefore, is not the only temporality appropriated by the cyber security assemblage. In contrast with recruitment and education activities, which are still at an early stage of becoming institutionalised, the temporalities of machines are appropriated by cyber security but also internalised and reproduced in distinctly political and problematic ways.

At the root of real time is a radical technological determinism in which the emergence of a global temporality of speed and acceleration maps directly onto developments in information technology. There is great variation in the deterministic arguments deployed within the broad field of IR, but most resolve to a fundamental argument that ‘technology develops according to a single linear rationale which causes outcomes of social development’ (McCarthy 2013: 473). The teleological endpoint to which information technologies rush is the ultimate erasure of space by time in the global ‘now’ of ‘real time’, a perspective that exemplifies the common ground of technological deterministic accounts in their effective erasure of human agency from history. Reading history in these terms confounds attempts to trace causality through humans as well as nonhumans. Importantly, the promotion of a worldview that subscribes to this interpretation of history forecloses the possibilities of democratic politics. Cyber security communities often stress the variety and heterogeneity of 'cyberspace' or 'the internet', but their conceptions of 'the time of cyberspace' or 'the time of the internet' take the opposite stance, adopting a deterministic 'real-time' reading of the global information-technological environment as the baseline for their views of the world and what needs to be done about it.

We should, in the first instance, recognise the genealogy of real time in the histories of Western modernity that stress the standardisation of 'clock time' as a precondition for the 'time-discipline' of industrial capitalism and the subsequent triumphal 'hegemony' of this temporal regime through the processes of colonialism and globalisation (Hom 2010). The canonical example of this genre is often held to be historian E.P. Thompson's 1967 article 'Time, Work-Discipline and Industrial Capitalism'. Thompson described the replacement in the eighteenth century of the 'natural' rhythms and tempos of life with the standardised and mechanised 'clock time' of early industrial capitalism, changes which permeated and radically altered the structures of modern life (Thompson 1967). In 1884, the International Meridian Conference formalised Greenwich as the prime meridian and divided the globe into twenty-four time zones, effectively institutionalising the first unified public global time (Palmer 2002). Almost exactly a century later, the Network Time Protocol (NTP) became the standard global protocol for aligning the system clocks in all computing devices to Coordinated Universal Time (UTC) (Mills 2006). In these developments, we may perceive the emergence of technological time as the global *chronos*, the always-synchronised time of life, society and world history.

Real time is the apotheosis of this interpretation of historical process, in which instantaneity replaces duration and spatial distances collapse almost to irrelevance. For Virilio, the condition of postmodernity is a temporal one, in which 'the "world space" of geopolitics is gradually yielding its strategic primacy to the "world time" of a chronostrategic proximity without any delay and without any antipodes' (Virilio 1997: 69). In lock-step with the imperatives of war and capital, postmodern humanity cannot escape the eternal now, a pessimism that stalks the cyber security imaginary too, in its adherence to speed and acceleration as the defining characteristics of contemporary temporality. This narrative sees clock time – technological *chronos* – as 'an intruder whose adaptations pervert natural time . . . [as] omnipotent and omnicompetent: an adaptable, flexible monster making its way into every area of human life, producing all manner of time-based obsessions and perversions' (Glennie and Thrift 2009: 50). Time is the enemy in theories of temporal hegemony and in cyber security, but in both it is also the seducer: the temporality of machines is the object of their critique, but it becomes the principal concern of their narratives, the horizon beyond which other temporalities are obscured, if not totally ignored.

The totalising nature of these exclusive conceptions of time is at odds with the empirical findings of diverse disciplines, from which we learn that 'what we call time is an ungainly mixture of times – unfolding at different speeds in different spaces – which intersect and interact in all manner of ways' (Glennie and Thrift 2009: 66). The internet, for example, might appear to impose a homogeneous global time, but in its empirical detail it is an assemblage of multiple temporalities deriving from the relations between its numerous elements, both technical and subjective (Lee and Liebenau 2000; Leong *et al.* 2009). This is expressive of Ulrich Beck and Daniel Levy's claim that after traditional, religious and political 'epochs', we are entering a fourth temporal epoch, 'characterized by fragmented times and the absence of a dominant, let alone hegemonic, conception of temporality and attendant views of futurity', or of history (Beck and Levy 2013: 9). The linear and teleological account of the shaping of *chronos* through technological means is an account of world time that in the shift from modernity to postmodernity loses its privileged position as an explanatory metanarrative. It is not abandoned but becomes one element of the heterotemporal assemblage of world politics, 'a shifting and unpredictable conjunction of times', in which 'the theorist's own complex structure is implicated in and with that which he or she seeks to describe, explain and judge' (Hutchings 2008: 176). This perspective refuses totalising narratives of the temporal present propounded by mainstream political actors and by more critical voices.

The logic of real time facilitates the political construction of the information-technological environment as one of risk, threat and negative social transformation, but those who reproduce these narratives are beholden to a peculiar paradox. Why would anyone promote a perspective on the world that diminishes the possibilities of politics while also pursuing politics to regulate that world? The answer lies in the fallacy of real time itself. Robert Hassan (2007) suggests that when Virilio speaks of real time 'killing' subjective time, when sociologist Manuel Castells theorises 'timeless time' as a sort of 'nontime' and when others interpret global simultaneity as an absolute condition rather than as the subjective impression of instantaneity, they are committing to an ontological impossibility. If real time portends the 'surrender of human agency to digital technology', this end-state is rendered 'unrealizable because imperfect humans constantly get in the way of perfect systems' (Hassan 2007: 51). Because of the innate friction of being human, to be human is always to possess the agency to act politically, regardless of technological milieu, even if we cannot necessarily change the conditions of the material environment. This realisation is at the root of critiques of speed that recognise its dangers but embrace the political and emancipatory possibilities of speed and acceleration (Connolly 2000; McIvor 2011; Glezos 2012). It registers in Christopher Coker's assertion that, until the technological singularity at least, 'humans will be easing themselves out of the [decision-making] loop at every level *except the political*: strategy will still be a human monopoly' (Coker 2013: 149, added emphasis; also, Cunningham and Tomes 2004). In a more negative sense, these dynamics are at work in cyber security, not just in the insistence on responding faster to the speed of the environment but in the metaphorical space that opens up because of the deceleration lag between phenomena and the political responses necessary to counter them. The resulting temporality is precisely that which creates the conditions for politics; without this dislocation – absent in the horizontality of real time – politics would not be possible (Massey 1992).

The logic of real time reduces politics to a figurative singularity, an event, a kairotic moment of supreme timeliness in which action must – impossibly – occur now. This logic emerges from narratives contingent upon highly deterministic interpretations of reality and temporality existing in the minds of observers and critics. Real time is only real insofar as it is socially constructed, an observation which does not diminish its potency as an analytical or political construct. To the contrary, the logic of real time is a powerful one, albeit one at odds not only with empirical reality but also with other aspects of the chronopolitics of cyber security itself. In particular, far from being distributed across a hallucinatory skein of centrifugal nowness suspended precariously at the illusory juncture of posteriority and futurity, reality has temporal depth and texture. This is expressed in cyber security in the continued importance attached to events, the logic of which is the topic of the following section.

The logic of event

To Sir Francis Walsingham, Elizabeth I's 'spymaster', is attributed the watchful maxim 'there is less danger in fearing too much than too little' (Cooper 2011: 53). If we are to judge by their discursive reliance upon dystopian narratives of future cyber insecurity and its existential implications, it would seem that many cyber security actors have adopted Walsingham's words as a mantra guiding their pronouncements and practices. Not only does an absence of credible and effective security portend a generalised state of societal deterioration, but political arguments are frequently contingent on 'knowing' that the darkening future will be shaped by events of great magnitude. Somehow, even as the future turns back upon us within the extended present, and as the nightmarish logic of real time threatens to obliterate the heterotemporality of life and history, the event still manages to hold sway in cyber security narratives of the near future.

In our contemporary 'thickened history', in which events happen with ever-greater frequency, confounding our abilities to understand both them and history, certain types of event are still elevated above others (Beissinger 2002). Catastrophes and crises are the stock events of the cyber security imaginary and the principal means through which to comprehend cyber security futures, prick politicians' consciences and achieve security gains in the present. To the same ends, historical events become powerful analogies for what will happen in the absence of appropriate political behaviour now and act as signs corroborating apocalyptic narratives predicting future catastrophes.

It will be clear from the preceding chapters that these events, historical or speculative, and the narratives in which they are embedded, require mediation. This happens through news organisations and other platforms and institutions in order to reach and potentially persuade their audiences and to anchor cyber security in a more stable and coherent past. This much is established, but why else is this necessary and politically expedient? What logic peculiar to the event operates in the chronopolitics of cyber security? To understand the temporality of the event requires that we move away from understanding the event as a commodity to exchange in the global news ecology, or as a discrete temporal moment, and regard it also as an aesthetic form. Reinhart Koselleck suggests that 'even expectation can be experienced' (Koselleck 2004: 261), by which is meant that hopes and fears of the future are registered intensely by human senses and consciousness. As discussed in Chapter 6, Aradau and van Munster politicise this experience of expectation through their conceptualisation of the 'sensorium of anticipation', which enlists all the senses to create an aesthetic of the future that facilitates security politics in the present (Aradau and van Munster 2011: 85–6).

To illustrate this, consider the specific example of 'cyber war'. It has become something of a cottage industry to argue whether cyber war exists or is ever likely to exist. For present purposes, we can understand it provisionally as a societal conflict conducted through information technologies, in which public and private infrastructures and attendant functionalities are degraded by adversarial cyber attacks. In Chapter 4, this form of conflict is described as a staple of the cyber security imaginary, whether or not it constitutes part or potentially all of the strategic level of war or not. It is difficult to tell where the boundaries of cyber war might be, which reflects a general unease at the difficulties in discerning 'traditional' war from forms of conflict that might be termed 'metaphorical'. In the case of cyber war, authors like Thomas Rid affirm that because cyber war cannot be instrumental, political *and* violent – his reading of the Clausewitzian criteria that must be met for something to qualify as war – cyber war cannot be war (Rid 2013a). 'Cyber war' must therefore be a metaphor or heuristic device, rather than war *proper*. This is an idiosyncratic reading of Clausewitz (Stone 2013), but it does illustrate a contemporary uncertainty over what qualifies as war or not in an age of globalised violence, and the analytical and political problems of demarcating where war begins and ends in space *and* time.

Christopher Coker argues that we struggle to comprehend and represent the nature of contemporary war, so that our attempts to do so err towards the visual rather than the textual. The 'image rather than the word renders war into an experience that can be shared', particularly with respect to the 'extremities of human experience that make war so vivid' for the external observer (Coker 2013: 109–10). This is a problem for our understanding of cyber war. If not inevitable in an increasingly informationalised world, cyber conflicts are at least 'latent', in that they are 'in the world but not experienced as part of the world' (Floridi 2014: 318). Cyber war, or any other form of cyber conflict currently underway, is difficult to describe in either textual or visual form and so requires other discursive strategies to make narratives of cyber war intelligible. Narratives of war – real or imagined – need to engage audiences through emotional and affective stimulation. 'Cyber war' is fought principally on abstracted informational terrain and can only become meaningful in Coker's terms, first, through the 'materialisation' of the virtual and, second, through war's affective embodiment (see also Kaiser 2015). Both are aspects of the chronopolitics of the event, through which the event is politicised in the name of cyber security.

The first dynamic entails the translation of the ones and zeroes of informational conflict into something material with which audiences can identify. The visual grammar of cyber war is not digital, unlike the vehicles of its prosecution – cyber 'weapons', as it were – but analogue. It invokes clichés of planes tumbling from the sky and chemical plants exploding. It requires even more immediate demonstrations of industrial plant malfunctioning to the point of destruction. It manifests as mock cities in defence contractors' office blocks. These material effects express the 'virtual' threat and transform the familiar and mundane into objects of extraordinary subversion and sabotage. Although not exclusively visual, this translation makes these events vivid and 'brings home' to media audiences the experience of 'cyber war' and its extreme effects on society. These narratives are closely tied – in theory, at least – to the military targeting of urban environments, particularly 'urbicide', in which the deliberate destruction of the city is characterised as a distinct form of political violence, intended to eliminate cultural heterogeneity and disrupt the continuity of urban identity and memory (Coward 2009; Bevan 2006). Information infrastructures *in toto* are transnational and global, but they are also local and predominantly urban. Their targeting in cyber war is similar to the urbicidal logic of other forms of war and may also elicit emotive responses to the destruction of assets with social and cultural value (Burgess 2007).

The second dynamic asks audiences and observers to become active participants in countering potential infrastructural degradation under conditions of 'cyber war'. Even with the increased technicisation of war through the widespread adoption of information technologies and 'remote' methods of killing, war is not becoming as disembodied as some observers maintain (e.g. Der Derian 2009a). The commonly cited example is of soldiers controlling drones from outposts in the American Southwest, who are characterised as disengaged operators of lethal hardware flying over foreign battlespaces and who can clock off and re-enter their suburban lives in ways not available to their in-theatre colleagues (e.g. Benjamin 2013). As Coker notes, these servicemen and -women are far from detached from their targets in Afghanistan, Somalia or Yemen, but they are fully 'embodied in the network' of modern war (Coker 2013: 98). Use of 'drones' is ethically problematic, but the cybernetic systems in which this use is embedded are neither autonomous nor 'unmanned'.

Kevin McSorley introduces the concept of 'somatic war' to denote the many ways in which expeditionary and 'remote' war are experienced. This requires the use of information technologies to make war 'perceptible and palpable for a wider audience' (McSorley 2012: 56). Images of war transmit political messages, but they also contribute to the visual culture of war in ways beyond the representational and discursive. They must also be understood in terms of their 'affective logics', which offer 'a seductive enrolment into the wider militarized sensorium' (McSorley 2012: 55). Mediated cyber war narratives do convey specific messages, of course, but they also help to foster an affective aesthetic of future cyber war, through which to further political ends.

The mediated discourses of cyber security, the narratives of physical destruction and the semiotic grammars of news reports and other visual representations of cyber insecurity encourage an ‘affective excess’ beyond their overt political messages alone. This also serves to create ambiguous yet ‘intensive space-times’ (Anderson 2009) that are ripe for political exploitation. The aesthetic significance of a public exercise like Cyber ShockWave lies not only in its ability to instil fear and concern but also in its affective resonance with the corporeal and the mundane, which assists in countering the decorporealising effects of speed and virtuality. In this example and through other ‘awareness-raising’ and ‘education’ activities, the immersion of people in the superficially plausible reality of ‘cyberwar’ – part of the ‘public sensorium’ of cyber security – encourages them to recognise the severity of these future events and to reconnect with their civic-mindedness. Discourses of ‘cyber war’, in which war is fought not only abroad but also on the home front, are an encouragement to citizens to rediscover their inner warriors. While there will always be the need for a professional elite of ‘cyber warriors’, there are clear indications that the development of a ‘whole-nation’ approach to cyber security is considered desirable and the language of civilian ‘cyber warriors’ is never far away (e.g. Klimburg 2010, 2011). Perhaps, if the ‘re-enchantment’ of war relies on ‘putting us back in touch with our humanity’ (Coker 2004: 44), the ‘enchantment’ of cyber security lies in putting us back in touch with our warriorhood. The affective excess of speculative events is one way this is attempted.

Richard Grusin’s concept of ‘premediation’ draws a direct link between affective excess and the future and points towards the chronopolitics of these operations (Grusin 2010a). Premediation involves the persistent and preemptive production of media ahead of future events, so that if these events occur, the public is already in some sense immune to the effects the event might otherwise generate. The politics of premediation aims to sustain a minimal level of popular fear and concern, thus enabling governmental politics in the present. It also intends to minimise the media shock of major events in the future, thereby reducing the level of popular discontent, resistance and rejection of these events and actions. Premediation rehearses catastrophic futures before they irrupt into the present and helps to inure publics to the shocks of future events, an outcome which can be read as increasing resilience to the future event (also, Aradau and van Munster 2011: 46).

Koselleck writes that the ‘unexpected has the power of surprise, and this surprise involves new experience’ (Koselleck 2004: 262). Premediation attempts to exclude as far as possible the element of surprise and tries to minimise future ‘new experiences’, preferring to rehearse them in the present rather than live them in the future. It tries to 'prevent the experience of a traumatic future' by acting as 'a kind of affective prophylactic' (Grusin 2010a: 46). 'Remediation' assists these processes further, repurposing past events like Pearl Harbor and 9/11 in the service of security politics, the principle intention of which is to ensure continuity between the present and the future. At the same time, writes Marieke de Goede, premediation of the future limits the number of possible futures available to the social imaginary and to the business of politics. Privileging one scenario at the expense of another or imagining and visualising one possible future instead of another involves 'profoundly political work that enables and constrains political decision-making in the present' (de Goede 2008b: 171). In so doing, these forms of chronopolitical intervention in affective relations can decrease societal resilience and cause resentment among political constituencies.

It is useful to conceive of cyber security in these terms, but we should also wonder at the actual efficacy of premediation in generating security outcomes. Grusin responded to Cyber ShockWave in a blog, lambasting its simplistic take on government decision-making in time of crisis: 'white guys sitting around a room responding to cable news reports imagines a model of government already outmoded when Kubrick released Dr. Strangelove' (Grusin 2010b). This is a reasonable criticism, but he also suggested the exercise might have 'some small effect on modulating individual and collective affect'. More importantly, Cyber ShockWave was 'part of a continued premediation campaign distributed across print, televisual, and networked media, a campaign that is in full swing and appears to be heating up'. This is certainly the case and there are few days without cyber security appearing in the media, even if the definitional bounds of cyber security often stretch credulity or terminological consistency. The severity of the events and processes reported varies greatly, but their presence ensures that premediation continues and intensifies. Many news reports also include 'what if?' segments that build narrative linkages between past events, reported events and future events. The sources of this premediation are many – government, business, journalism, the academy – but all underline the central logic of the premediated event: 'the generation of possible future scenarios or possibilities which may come true or which may not, but work in any event to guide action (or shape public sentiment) in the present' (Grusin 2010a: 47). We may challenge the efficacy of premediation attempts but their chronopolitical logic is readily apparent and invests in the interpretation of past and future events the ability to shape political behaviours in the present. The logic of event achieves this through aesthetic and pragmatic means.

The logic of *eschaton*

At several points in this enquiry, most notably in Chapters 3 and 4, the issue of finitude has been raised with respect to the foreclosure of future temporal horizons. One argument commonly made for the distinctiveness of postmodernity is its apparent rejection of teleological metanarratives and its inability, in the face of global existential crises, to see for itself a long future. The 'extended present' (Nowotny 1994) is theorised as the manifestation of these deep cultural currents, in which concerns over the near future shape politics in the present, as contrasted with politics attempting to mould the long-term future, as might be identified with Enlightenment thinking and technological modernity in general. These arguments derive principally from Western philosophy of history and help frame political narratives of 'cyber apocalypse', in which catastrophic events are both imminent and immanent to postmodernity. These expressions of secular apocalypticism are not simplistic presentations of 'the end' but portend passage points through which political order is transformed and more 'cyber secure' futures are brought into existence. The logic of premediation goes some way to demonstrating the political utility of these apocalyptic portrayals, generating an aesthetic of anticipatory anxiety that facilitates political action in support of cyber security in the present. The creation of this immanent affective state through premediation is a key chronopolitical aspect of cyber security involving actors across multiple sectors and mediated through the heterogeneous and distributed 'new media ecology' of global postmodernity (Hoskins and O'Loughlin 2010).

'The End' may never arrive, but these narratives disclose a deep concern with finitude. The theologian Bernard McGinn describes apocalypse as only one 'species of the genus eschatology' (McGinn 1998: 3). Eschatology views history as teleology and believes that scripture reveals truth about the purpose of history. In contrast, apocalypticism is 'a particular kind of belief about the last things – the End of history and what lies beyond it' (McGinn 1998: 3–4). This may seem like a trivial distinction, but it demarcates the difference between the eschatological interpretation of current events as adumbrations of the end of history and seeing them apocalyptically as the end times themselves. We can learn much from exploring the secular apocalypticism of cyber security, but we can augment this chronopolitical understanding by locating it more firmly within the logic of eschatology as expressed in political theology. Paul Fletcher argued that liberal modernity has distanced itself from the metaphysics of theology but that its political authority derives ultimately from its theological heritage. Scripture and dogma may not find expression or translation in the creeds of market fundamentalism or neoliberal governance, but 'the mundane political order is dependent on a (now recurrently unavowed) transcendent order of things' (Fletcher 2004: 54).

For Fletcher, the 'war on terror' represents a resurgence of the metaphysical into the political, explicable through the lens of eschatology in its specific *telos*, the triumph of Good over Evil. Michael Dillon proceeds a step further in assigning an eschatological ontology to the politics of security in general. The politics of security is 'politics thought in the light of the last things, the limit situation as a determinable and determining terminus', which articulates both a sense of ending (finitude) and of 'ends' (*telos*, aims and desires) (Dillon 1996: 31). Yet, as we have identified in apocalyptic cyber security narratives, the end is not the End but also a beginning – 'the natality' and the very 'advent of the political' (Dillon 1996: 31). However, there is still more temporal texture than this simple picture suggests. As both Fletcher and Dillon recognise, we must account for the apparent gap between the historical present and the end of history (*eschaton*). This hiatus has a distinctly chronopolitical character that helps to explain, for example, why the cyber apocalypse never seems to arrive. It also assists in explaining how politics are enabled in the 'space' opened up between 'now' and 'then' when we refuse the totality of real time.

Fletcher claims for the 'war on terror' a transformation of political time itself, which defers forever the possibility of tangible victory. The war on terror in its quest for 'infinite justice' requires no specific antagonist but is instead 'a security project that finds its condition of possibility in omnimalevolence' (Fletcher 2004: 57). Under these conditions, there is 'no realizable *telos*' and a 'zone of anomic indistinction' between present and future substitutes for any likelihood of victorious consummation. This is a state of exception in which due legal process is suspended and all manner of 'emergency powers' can be enacted (Fletcher 2004: 59). This would include the nascent practices of executive centralisation discussed in Chapter 3, which were identified with the logic of real time.

Dillon expands upon this formulation through his identification of this 'zone of anomic indistinction' with the *katechon*. In Christian eschatology this denotes the 'impetus to resist, restrain, or otherwise defer' the messianic *eschaton* (Dillon 2011). Where Dillon and Fletcher differ is in the latter's insistence on the exceptionality of this temporality, which Dillon treats as entirely banal and constitutive of liberal modernity itself. In political philosophy inflected by this metaphysics – notably, the political theology of Carl Schmitt – the *katechon* becomes, as in Fletcher's anomic zone, that which prevents the end of the present temporal order, the political status quo. The *katechon* is that which maintains order in the face of eschatological fervour for apocalyptic transformation (Ostovich 2007). As McGinn notes of apocalypticism understood as a form of political rhetoric, it is 'as often designed to maintain the political, social, and economic order as to overthrow it' (McGinn 1998: 30). Therefore, as Dillon notes, *eschaton* and *katechon* are in continuous tension, particularly as maintenance of the *katechon* becomes its own form of 'messianic mission' (Dillon 2011: 784).

With respect to cyber security, we can locate the various formulations of 'cyber apocalypse' more concretely within this eschatological framework of Western political philosophy. An initial distinction is necessary between those discourses that make explicit reference to apocalypse and those in which we can discern an apocalyptic sensibility. It is quite possible to belong to the latter category and not the former, as demonstrated by the many examples of cyber security actors whose narratives rely upon the construction of catastrophic end-points but which do not openly evoke 'cybergeddon', 'cyber apocalypse' or other terms loaded with Judaeo-Christian millennial connotations. In both cases, the apocalypse never arrives: the cyber apocalypse is 'inevitable and imminent but perpetually postponed' (Barnard-Wills and Ashenden 2012: 188). The apocalypse is frequently portrayed as something desirable and necessary for political transformation in the name of cyber security but it is not coterminous with the *eschaton*, which would be the 'catastrophic threat of the dissolution of the order of things' (Dillon 2011: 782). This, in fact, is precisely *not* what cyber security actors want. They do not desire the end of the temporal order but the transformation of select elements of the present order in line with their own desires and those of the national security state, congruent with the logics of global capital.

This is not to deny the potency of secular apocalypticism or its utility as an analytical heuristic, but it does challenge cyber security actors' own apocalyptic narratives. In the light of political eschatology, cyber security apocalypses do not threaten the political order but support it: they are themselves agents of what Dillon calls 'katechontic securitization' (Dillon 2011: 789). This requires that the *eschaton*, which would announce the end of the state, is constantly deferred, a project that 'demands relentless political and ideological work' (Dillon 2011: 783). Many forms of this have been identified previously, not least through premediation and the generation of anxiety and concern about the future. We can also find statements of the political utility of apocalyptic language, Pentagon officials admitting that although it might be 'overstated', it works 'to put pressure on Congress to pass cybersecurity legislation' (Marcus 2013). These narratives overtly frame legislation, regulation and other forms of governmentality as the methods through which to prevent apocalypse and catastrophe and maintain this katechontic restraint on true political transformation.

At the same time, a perpetual reliance on catastrophic narratives serves to ignore cyber security initiatives already in place and continues to construct ‘cyberspace’ as an ungovernable and dangerously unknowable source of risk and threat, enabling the pursuit and implementation of further cyber security (Barnard-Wills and Ashenden 2012: 118). As in other areas of life, those who incubate an apocalyptic aesthetic are usually the same as those who promise salvation (Swyngedouw 2013). Current government and commercial investment in cyber security would suggest that the continued deferral of ‘cyber apocalypse’ is good business sense in the form of a burgeoning ‘cyber-industrial complex’ (Deibert 2012). The constant deferral of the end creates a hiatus in which the cyber security project can be reworked in perpetuity with respect to an infinite number of future security possibilities and to a future that never arrives.

It is perhaps too easy to pour into the *katechon* the malice and machinations of the national security state and its supporting infrastructure without considering the more positive connotations of eschatological consciousness. The political theology informing the preceding discussion channels Schmitt’s own belief that ‘all genuine political theories presuppose man to be evil’ (Schmitt 1996: 61, in Ostovich 2007: 63). There seems little room in this schema for hope or optimism, both of which founder on pessimistic readings of the human condition. From the perspective of the state, we have already encountered distinctly grim perspectives on the present and the future, the parlous state of each demanding – as does the logic of *eschaton* presented so far – that the political status quo be maintained and preserved through the instigation of ‘more’ and ‘better’ cyber security. Optimism under these conditions seems reduced to keeping the barbarians from the gates and promoting cyber security as a driver of economic growth.

Hope is central to eschatological consciousness in the Western tradition and becomes not only hope for future redemption but also a resource to be used in pursuit of a better life on earth in the present (Moltmann 1993). ‘Progressive’ forms of apocalypse stress the possibilities of cooperation and collaboration in effecting earthly salvation (‘progress’) without the need for the violence of divine justice (Wessinger 1997). Endeavours like eugenics, cryonics and even space exploration share the belief that science and technology can improve the future of the human species (Bozeman 1997). The posthumanist movement is inherently concerned with a fast-approaching ‘technological singularity’, mischievously dubbed the ‘Rapture of the Nerds’ (Doctorow and Stross 2012). It is infused with secular, even scientific, apocalypticism but emphasises the positive social benefits made possible through radical information-technological developments (DeLashmutt 2006). These expressions of a long heritage of technoscientific thought are secular rather than religious in their apocalypticism, although the two are closely related (Hughes 2012).[1]

Many cyber security narratives are in what we might call the 'catastrophic tradition'. However, they also frequently stress the progressive possibilities of cyber security for enabling social progress, strengthening societal resilience, ensuring ontological security and delivering a better future for all. We should not dismiss these aspirations lightly and one can certainly subscribe to them without worrying overly about the problematic aspects of how they might be achieved and what political ends they disclose. Even in the knowledge that much lies beneath the surface of national security discourse, we might adopt the perspective of the imprisoned Antonio Gramsci, who maintained his 'optimism of the will' in the face of 'pessimism of the intellect' (Gramsci 1973: 175). Beyond this duality of what is and is not possible, it is hope that 'energises political agency' due to its 'refusal to rule out the possibility of a better future' (Booth 2007: 179). Given the centrality of hope to eschatology, if not to political theology, it seems sensible not to exclude it from the chronopolitical logic of the *eschaton*. Even if we reject 'hope' as packaged in the trite manifestos of electoral politics, we should perhaps retain it as a condition of temporal, and therefore political, possibility.

Cyber security and the politics of time

This chapter outlined four prominent strands of the chronopolitical manifold of cyber security, the logics, respectively, of assemblage, real time, event and *eschaton*, organising principles or tendencies that emerge from our analysis of the cyber security assemblage. The analysis of these logics looks deeper into the sociotemporality of cyber security communities of practice and begins to show why the temporal aspects of the cyber security imaginary are the way they are. These logics are not mutually exclusive. The logic of assemblage, for example, is one born of the nature of reality itself, in which continuity and change are two sides of the same existential coin; each presupposes and is conditional on the other. This processual ontology requires that an entity characterised as an assemblage, like cyber security, must change in order to persist. This requires that the assemblage extend itself in space – through enrolling more

[1] For an excoriating review of contemporary technological utopianism, see Rieff (2013).

actors – and in time – by appropriating their temporalities – or it will lose its identity and potency.

In this light, all other logics are expressions of the logic of assemblage, in which cyber security finds new ways to extend itself through time and space. Of course, we can make the argument that cyber security expands in order to counter the threat of cyber insecurity, but this would be to graft politics prematurely onto ontological reality. Like all sociomaterial assemblages, cyber security too must 'perform' itself to remain coherent, although any claims that cyber security is a singular entity possessing some limited identity and agency must be underwritten by an appreciation of its necessary mutability and contingency. Cyber security actors appropriate, internalise and reproduce the 'real time' of information technologies; the premediation of cyber security events enrols bodies and emotions in an affective sensorium; eschatology creates additional time to colonise through increased cyber security. The logic of assemblage underpins all actions by cyber security actors, even if it does not necessarily explain them.

The question of the construction of reality is a key consideration when discussing the 'logic of real time'. The preoccupation with real time stems from concerns about speed and acceleration as ontological conditions of postmodernity, particularly as relates to the information-technological collapse of global distance and the globalisation of a single 'real time' (see also Porter 2015). The argument is that real time suppresses the possibilities of political action, as registered in cyber security by concerns over the inability to 'keep up' with technological change and to legislate and regulate sociotechnical environments. The problem with this perspective is not that these are not important facets of postmodernity but that those who adhere to this narrative tend to ignore the empirical and subjective 'heterotemporality' or 'pluritemporalism' (Nowotny 1992) of the world. In its concerns with speed and acceleration, the logic of real time serves to internalise these temporalities and to reproduce them, exacerbating exactly the conditions it sets out to critique. Our model of emergent sociotemporality and the logic of assemblage show how cyber security appropriates the time of machines, but it is also seduced by nonhuman temporalities, closing down the possibilities of politics in so doing. This is a radical technological determinism that enables the continued construction of information technology as a domain of risk and threat. It facilitates the politics of cyber security and the extension of cyber security practices across all information-technological environments, regardless of need or ethics.

Cyber security is not yet wholly seduced by the apocalyptic logic of real time, however. Reality continues to have temporal depth and texture, as shown by the continued discursive investment in the power of the event. Two dynamics are important in the logic of event. The first is the use of historical events as analogies for future speculative events, in which the future is understood with reference to the past. The second is how the possibilities of future events prompt political action in the present and help to generate an affective aesthetic of anxiety of greater duration than the event alone. Past events are remediated and future events are premediated, both of which require that cyber security narratives are communicated through the global 'new media ecology'. This enrolment of media actors into the cyber security assemblage is essential to all forms of mediation and is another example of how an assemblage attempts to extend itself through social and material relations. So too is the intended effect on actors currently outside the cyber security assemblage, who may be recruited into the assemblage through their affective responses to the remediation of historical events and the premediation of speculative ones, which appeal to national memory and identity and to notions of civic responsibility. The premediation of events serves a further political purpose in attempting to reduce the shocks of future events by rehearsing them in the present, although this attempt at resilience is eroded by limiting the number of possible futures and by creating anxieties that might otherwise not exist.

One key area in which premediation works is the construction and maintenance of apocalyptic anxieties that disclose the eschatological nature of the politics of security itself. In the political theology that underpins the Western liberal tradition, the end of history spells the end of the state, which deploys all available techniques to avoid that end. The state seeks to maintain the temporal distance between now and the end, mainly through the implementation of technologies of security framed as measures to avert catastrophe, itself an obvious expression of the existential logic of assemblage. The substantial increase in cyber security spending and the emergence of a cyber-industrial complex can be read as an expression of this desire to prevent the end of the state, especially given wider concerns about the impact of information technologies on traditional notions of sovereignty, territoriality, power and dominion (Betz and Stevens 2011). This hiatus between now and the end is also the 'gap' opened up by the logic of real time. This is the lag between the technologically supercharged speed of postmodernity and the cumbersome bureaucracies of modernity, in which powerful actors can rework and refashion the cyber security assemblage in an almost infinite number of possible configurations.

If we are to define a chronopolitics of cyber security, it is as an assemblage of complementary and competing temporal logics informing and influencing the politics of cyber security. These logics encompass the nature of reality itself, the social construction of reality, ways of seeing the future and ways of interpreting the past, and the experience of living in a world of seemingly unprecedented change. The cyber security imaginary particular to the community of cyber security practice is in part constructed through these ways of perceiving time and temporality (chronotypes), which together constitute the sociotemporality of cyber security. We reconstruct this sociotemporality through the narratives cyber security actors tell about time, about themselves and about their relations with reality. As befits this social epistemological and constructivist approach, we must recognise that actors are not simply interpreting unmediated reality. They are telling stories about the world and acting upon these interpretations of reality. These notions and narratives change through time, in response to internal and external stimuli and processes, as befits any social group or other assemblage we might identify as a suitable unit of analysis. The drivers and discourses identified in this enquiry will change over time and are not static or definitive, nor do they together comprise an exhaustive statement of the chronopolitics of cyber security.

Yet we are thrown back upon the nature of security itself, established at the beginning of this enquiry as an inherently temporal proposition, particularly in its characterisation as a perennial exercise in practical futurism. Do the claims of cyber security or its chronopolitical logics alter this relation with time, or require the modification of the ontology of security with respect to this orientation to the future? I would suggest not, as the eyes and minds of cyber security actors, both by nature and choice, are still firmly fixed on the future and their actions are principally intended to both shape the future and ensure that cyber security itself persists into the future. What does require attention is the nature of the future itself, which has become almost a proxy for the concepts of uncertainty and risk. In contemporary risk society, writes sociologist Frank Furedi, the future 'is seen as a terrain which bears little relationship to the geography of the present' (Furedi 2006: 68). The concept of the 'extended present' expresses this uncertainty, in which existential concerns about the future shape politics in the present, rather than projecting the present into the future. Furedi summarises this pessimism in survey results that show that for the first time since World War II, parents expect that their children's lives will be worse than their own (Furedi 2006: 68). In these perceptions dies the Enlightenment dream and security, through the practices of risk and premediation, is left to 'imagine, harness and commodify' what remains of the uncertain future (de Goede 2008b: 159).

If cyber security is concerned with securing the future, we must also wonder at the future of cyber security itself. As a term, its days are perhaps numbered. The contemporary rush to prefix all nouns with ‘cyber’ is a response to the ‘foreshortening of the horizon of new technologies’, in which scholars, media and politicians are in ‘a breakneck race to enunciate the immediate moment’ (Lunenfeld 1996: 16–18). This is itself reflective of the perceived speed of the contemporary world and we must wonder if these neologisms will last as long as the phenomena to which they adhere. We cannot know but this uncertainty does not detract from the importance attributed to cyber security, whether it retains that moniker or not. Cyber security is not just ‘epiphenomenal, a consequence of the computer and Internet revolution’, as some authors assert (Harknett and Stever 2011: 455). It is, instead, a *condition* of that revolution, a transformation in which state commercial and civil actors have all invested substantial cognitive, material and emotional resources.

Whatever we call it, cyber security or something like it will persist in its attempts to secure the information infrastructures and informational flows upon which societies and economies depend. What we can be much less certain about is the balance of desires that will determine cyber security’s future complexion with respect to appropriate levels of control and authority. A key dimension of this evolution will be how time is politicised. We may succumb to the imperative to act always in the now, seduced by ‘a metaphysics of crisis and its attendant temporality, the mood of which is unequivocally imperative’ (Fletcher 2004: 59). We may convince ourselves that doing something in the name of national security is always better than doing nothing, even if this creates further insecurities through the circumvention of democratic politics and due legal process (Mitzen 2006; Steele 2008). Alternatively, we might recognise the plurality of temporalities that play into the political sphere, allowing us to take stock before embarking on a purely technologised security future. In all cases, however, political practices will continue to evolve and must continue to attract considered and careful attention as they do so. It is my contention that a crucial aspect of this watchful analysis will be how conceptions of time and temporality inform the politics of security.

8 Conclusion

In 1984, it was possible to write an article purporting to cover all of computer security, detailing the 'concepts, techniques, and measures relating to the protection of computing systems and the information they maintain against deliberate or accidental threats' (Summers 1984). In the same year, a British MP's administrative use of an office word processor – 'which I have found to be of enormous benefit' – was sufficient to establish his credentials before a House of Commons Select Committee on parliamentary IT systems (House of Commons 1984). Three decades later, it is inconceivable that either offering would be possible or tolerated, given enormous changes in the nature and distribution of computer networks and their relations with security and politics. Scholars have argued that the perceived risks and threats arising from the uses and abuses of information technologies constitute '*the* central security policy concern today' (Dunn and Mauer 2007: 152, original emphasis). Subjective though this assertion may be, what has become known as 'cyber security' – variations in local priorities aside – occupies a central position in national and international security policy and is a key condition for the transacting of individual and collective economic, social and political life.

The rate of cyber security policy adoption, implementation and change has been very rapid, particularly since the late 2000s, notwithstanding the protestations of those lamenting the opposite, of course. Accordingly, there has been a significant increase in the volume of policy-oriented work in both the academic and popular arenas and it has become difficult, as Barry Buzan remarked of security discourses thirty years ago, not to be 'swept away by the hectic empiricism of the field' (Buzan 1983: 12). This book is not an attempt to resist that tide but an attempt to question this temporality of speed and acceleration and from that starting point to query more expansively the relations between the cyber security assemblage and time and temporality.

The principal task has been to explore how the broad community of cyber security policy and practice conceives and experiences time and temporality. These examinations have been predicated upon a theorisation of the world as socially constructed, a constructivist perspective concerned both with epistemology – how knowledge is socially constructed – and with ontology – how social reality is constructed. This does not deny the existence of material reality but it does privilege human cognition of the world as a means of understanding the world and through which human communities generate knowledge of the world. In this sense, intersubjective epistemology becomes of ontological importance in social reality. The principal way in which we begin to understand how social reality is constructed is through analysing the utterances of actors concerned with, in this instance, cyber security. How cyber security actors articulate their reality and interpret the realities of others constitute discourses that express the aims and intentions of cyber security as a field of practice. Their norms, desires, ethics, expectations and intentions are manifest and stabilised materially through the technical and political actions so encompassed. In this register, the book contributes to the literature on cyber security and its antecedent and related practices within IR and security studies, especially that corpus of constructivist and post-positivist work concerned with cyber security discourses and the securitisation of 'cyberspace'.

I have proposed the existence of a 'cyber security imaginary' as one modality through which the community of cyber security practice negotiates social reality. To paraphrase Joelien Pretorius, the cyber security imaginary is that part of the broader social imaginary specific to society's common understanding and expectations about cyber security that makes practices related to cyber security possible (Pretorius 2008: 112). This enquiry has focused upon three aspects of the cyber security imaginary. First, that which pertains to an identifiable cyber security community, as distinct from wider societal understandings and expectations of cyber security. This has required attention to the statements of politicians, policymakers, military leaders, intelligence officials, journalists, the security commentariat and commercial security professionals. Although internally heterogeneous, as is any community, there are commonalities in the ways in which these actors imagine their roles in the world and, of course, how they imagine that world itself.

The second area of interest has been the shared temporal biases expressed by these actors, the chronotypes that emerge from their intersubjective understanding of time and temporality. In the model of emergent temporality presented here, these chronotypes exist at the level of sociotemporality, the collective knowledge about time that enables social groups to order reality and reproduce themselves over time. Importantly, this level of temporality incorporates within itself the temporalities of entities at all levels of reality, from the atomic to the animal. Our ability to know these nonhuman temporalities is enhanced by reason and by technologies that extend the human senses. In the sense that we can begin to know but never truly inhabit these nonhuman temporalities, sociotemporality is socially constructed, an assembled form of knowledge. The emergent model of temporality provides an important conceptual bridge between human and nonhuman and potentially constitutes a new basis for understanding time in IR and international politics. It augments the idea of 'assemblage' within political studies, which is principally concerned with material entities and topology, by providing temporal texture to the otherwise relatively flat ontologies of assemblage theory and related conceptual schema.

In the present work, chronotypes are closely interwoven with the third area of concern, which shows how chronotypes influence and shape the politics of cyber security. Through exploration of these chronotypes, we have seen how time and temporality attain 'practical or conceptual significance' (Bender and Wellbery 1991: 4), specifically in the politics and practices of cyber security. Thought of as narratives that cyber security communities tell about themselves and their world, these chronotypes guide political action, many examples of which are described and examined in Chapters 3–6. Chronopolitical practices range from the all-consuming belief in the revolutionary nature of the contemporary 'information age' that encourages ahistoricism and the imperative to 'act now', to desires for a cyber apocalypse to offer us a passage point to a more cyber secure future, to the use of history to analogise catastrophic futures, and various means of rehearsing and even populating the future. All these and more have further political and ethical implications that remain to be resolved. Attention to the temporal foundations of political practices – beyond the well-established notion that politics and security are always oriented to the future – is a productive mode of enquiry that contributes to a renewed interest in these matters in IR.

From this manifold of chronotopes and chronopolitical practices are extracted deeper logics, chronopolitical meta-strands which emerge from the cyber security assemblage and which inform and shape the politics of cyber security. I refer to these as the logics of assemblage, real time, event and *eschaton*. These have potential application beyond cyber security, as they are detectable in other forms of security and politics. If the description of a field of security as an 'assemblage' has any validity, for example, we should expect that observations of other forms of security will also yield the temporality characterised here as the 'logic of assemblage': the inherent necessity of these aggregate entities to reproduce themselves in time, as well as in space. Given the ontological pretensions of this characterisation, this must necessarily be so. The logic of real time, too, has aspirations as a global *explanans* for the politics of the 'information age'. It underpins the work of media studies on the politics and practice of news cycles, for instance. The pressures of real-time connectivity and communications have also become of great interest to military and security practitioners, particularly since 9/11 and the commencement of global counter-terrorism and counter-insurgency campaigns. The seduction by real time poses critical questions for the possibilities of democracy in an environment that almost demands less political reflection and deliberation. The impulse to act, for instance, logically presupposes the derogation of bureaucratic process, or at the very least an erosion of democratic transparency. These tendencies are registered in the 2013 revelations by Edward Snowden of the surveillance activities of the NSA and GCHQ, secret undertakings of dubious legal and constitutional basis that share many of the basic technologies and motivations as cyber security.

The logic of event also draws upon a range of theoretical resources to explore how cyber security actors invest events past and future with political significance. With respect to future events – crises, disasters, catastrophes – it has long been recognised, as did Arnold Wolfers six decades ago, that these events 'must always remain a matter of subjective evaluation and speculation' (Wolfers 1952: 485). In cyber security, these future events are substantially premediated and rehearsed to mitigate uncertainty and to prepare state and public entities for their possible occurrence. The forms of premediation, affective engagement and event inhabitation detailed here develop and complement critical work in security studies and media studies, interrogating the foundations of security politics and practices, particularly forms of anticipatory security governance rooted in the contemporary 'risk society'. Although in many ways a subset of events, the discussion of apocalypse and finitude wrapped within the logic of *eschaton* is broadly applicable to questions of political order, as befits the political theology thesis that informs and supports it. In its treatment here, eschatology can also return some hope to security scenarios that are often, as much of this book illustrates, rife with pessimism and truly dark visions of futurity.

Despite the potential contributions of this book to the interrogation and understanding of other forms of security and politics, it would be inappropriate to attempt to extrapolate or apply these findings with uncritical vigour. The overall orientation has been towards the anglophone cyber security communities of the United Kingdom and the United States, and this raises a key issue that future enquiries might address. Much of the discussion of time and temporality has been with reference to Western philosophy of history and, as stated, to anglophone sources in general. This does not allow us to generalise our findings beyond the Western context, although that was not an original aim of this enquiry. This book means to develop a credible narrative of how and why time is important to political behaviour, but non-Western and subaltern perspectives on time and temporality are excluded from that narrative. These are likely to differ on key issues, particularly with respect to national and cultural histories and the philosophy of history itself.

Cyber security makes significant claims to the global and the international and it would be illuminating to see how Western cyber security processes and practices interact with non-Western temporal perspectives and orientations, especially given the warnings offered in this book against adopting totalising conceptions of time. Cyber security is but one aspect of a developing conflict over the global internet, which often divides along 'East–West' or 'North–South' lines, and the resistance of the United States, in particular, to greater multilateralism in the global governance of the internet reflects American insistence on policy that favours American interests above all others (Kiggins 2015; also, Stevens 2012). Accusations of American colonisation of the internet and networked imperialism are a staple of contemporary critique and, in this respect, analyses of cyber security might provide another opportunity for the culturally non-European to 'return the gaze' (Chakrabarty 2000), exploring Western politics of security through non-Western theoretical frameworks, including philosophies of history and time.

An additional charge of exclusion might also be brought against the author. The book cites the multivocality of group formation but then excludes several classes of voice which impact upon the politics and practices of cyber security. Where are the voices of citizens, consumers and voters and of civil society in general? What do they have to say about time and politics? What do they say about cyber security? What are their roles in the cyber security assemblage and what do they think and say about their responsibilities, self-imposed or otherwise? What are their reactions to the forms of premediation and discourse directed at them by cyber security actors? These are important questions that beg answers, without which the foregoing analysis is undeniably partial to a narrow range of particular communities and to their views and opinions. We might venture that all these communities would also be better represented by finer-grained analyses that might emerge from the application of different methods in which direct interlocution is preferred to the analyses of secondary and mediated sources deployed here. This might reveal how conceptions of time differ between groups, both vertically in terms of communities and also horizontally between nations. Future analyses might also adopt ethnographic methods to explore more closely how cyber security practices are informed and structured by temporal assumptions held at the individual and group levels.

In common with other forms of security, the language of cyber security is, as articulated by political elites, a bipartisan idiom that facilitates threat politics and the potential suppression of rights (Robin 2012). Political conflicts tend to arise over the pace and scale of implementation rather than over substantive conceptual matters, which imparts a certain integrity to the elite politics of cyber security. It may be that chronotypes are not substantially contested between elites, but the language of imminent threat, for example, is surely open for contestation by civil society actors and suggests that political opportunities arise from the conflict between differing conceptions of time and temporality. These are tasks for other researchers, but their findings would undoubtedly enhance our understanding of how time and politics inter-relate and would illuminate aspects of the global cyber security imaginary not attended to in this book.

In closing, the principal contribution of this book has been towards the development of chronopolitics as an object of study in IR. Its central contention is that conceptions of time shape political behaviours, a proposition which I hope to have advanced, if not necessarily proven. A central ambition has been to open up the chronopolitics of cyber security and to challenge the dominant readings of time and temporality we find there. The German Romantic philosopher Friedrich Schlegel wrote: ‘No time has ever been so strongly, so closely, so exclusively, and so generally bound up with the future than that of our present’ (Koselleck 2004: 242). That he wrote this in 1828 should remind us that, despite the urgencies thrust upon us by looming crises, there is always time to reflect upon courses of future action. We may be, as Schlegel supposed of his own time, at a critical moment of importance in human affairs, standing upon the cusp of a new era, but this should not dissuade us from questioning dominant conceptions of political time. It is only through bringing time to the forefront of our attention that the ‘invisible is given form’ (Adam 1995: 6). This intuition has guided the present enquiry and I hope that similar impulses will guide subsequent investigations into politics and security, the need for which could not be more timely or, indeed, timeless.

References

Aaron, Chris (2012), ‘The growing cyber-security market’, *RUSI Defence Systems* 15, no. 1: 86–7.

Abbott, Andrew (2004), *Methods of Discovery: Heuristics for the Social Sciences* (New York: W.W. Norton & Company).

Abrahamsen, Rita and Michael C. Williams (2011), *Security Beyond the State: Private Security in International Politics* (Cambridge University Press).

Adam, Barbara (1989), ‘Feminist social theory needs time: Reflections on the relation between feminist thought, social theory and time as an important parameter in social analysis’, *The Sociological Review* 37, no. 3: 458–73.

Adam, Barbara (1995), *Timewatch: The Social Analysis of Time* (Cambridge: Polity Press).

Adam, Barbara (2008), ‘Of timescapes, futurescapes and timeprints’, paper presented at Lüneberg University, 17 June.

Adams, James (2001), ‘Virtual defense’, *Foreign Affairs* 80, no. 3: 98–112.

Ademollo, Francesco (2011), *The Cratylus of Plato: A Commentary* (Cambridge University Press).

Adey, Peter and Ben Anderson (2012), ‘Anticipating emergencies: Technologies of preparedness and the matter of security’, *Security Dialogue* 43, no. 2: 99–117.

Adler, Emanuel (1997), ‘Seizing the middle ground: Constructivism in world politics’, *European Journal of International Relations* 3, no. 3: 319–63.

Adler, Emanuel (2008), ‘The spread of security communities: Communities of practice, self-restraint, and NATO’s post-Cold War transformation’, *European Journal of International Relations* 14, no. 2: 195–230.

Adler, Emanuel (2012), ‘Constructivism in International Relations: Sources, contributions, and debates’, in *Handbook of International Relations*, ed. Walter Carlsnaes, Thomas Risse and Beth A. Simmons, 2nd. edn (Thousand Oaks, CA: Sage), 112–44.

Adler, Emanuel and Peter M. Haas (1992), ‘Conclusion: Epistemic communities, world order, and the creation of a reflective research program’, *International Organization* 46, no. 1: 367–90.

Adler, Emanuel and Vincent Pouliot (2011), ‘International practices’, *International Theory* 3, no. 1: 1–36.

Agamben, Giorgio (2004) [2002], *The Open: Man and Animal*, tr. Kevin Attell (Stanford University Press).

Agamben, Giorgio (2005) [2000], *The Time That Remains: A Commentary on the Letter to the Romans*, tr. Patricia Dailey (Stanford University Press).

Agnew, John (1994), ‘The territorial trap: The geographical assumptions of International Relations theory’, *Review of International Political Economy* 1, no. 1: 53–80.

Agnew, John (1996), ‘Time into space: The myth of “backward” Italy in modern Europe’, *Time and Society* 5, no. 1: 27–45.

Agnew, John (2011), ‘Space and place’, in *Handbook of Geographical Knowledge*, ed. John Agnew and David N. Livingstone (London: Sage), 316–30.

Ahlers, Mike M. (2011), ‘Inside a government computer attack exercise’, *CNN.com*, 17 October, http://edition.cnn.com/2011/10/17/tech/innovation/cyberattack-exercise-idaho.

Aho, James A. (1997), ‘The apocalypse of modernity’, in *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*, ed. Thomas Robbins and Susan J. Palmer (New York: Routledge), 61–72.

Aldrich, Richard J. (2010), *GCHQ: The Uncensored Story of Britain’s Most Secret Intelligence Agency* (London: HarperCollins).

Allan, Stuart (1994), ‘“When discourse is torn from reality”: Bakhtin and the principle of chronotopicity’, *Time and Society* 3, no. 2: 193–218.

Aloisio, Mario (2004), ‘The calculation of Easter Day, and the origin and use of the word *Computer*’, *IEEE Annals of the History of Computing* 26, no. 3: 42–9.

Alterman, Hyman (1969), *Counting People: The Census in History* (New York: Harcourt, Brace & World).

Amoore, Louise (2013), *The Possibilities of Possibility: Risk and Security Beyond Probability* (Durham, NC: Duke University Press).

Andersen, Holly K. and Rick Grush (2009), ‘A brief history of time-consciousness: Historical precursors to James and Husserl’, *Journal of the History of Philosophy* 47, no. 2: 277–307.

Anderson, Ben (2009), ‘Affective atmospheres’, *Emotion, Space and Society* 2, no. 2: 77–81.

Anderson, Ben (2010a), ‘Security and the future: Anticipating the event of terror’, *Geoforum* 41, no. 2: 227–35.

Anderson, Ben (2010b), ‘Preemption, precaution, preparedness: Anticipatory action and future geographies’, *Progress in Human Geography* 34, no. 6: 777–98.

Anderson, Benedict (2006) [1983], *Imagined Communities: Reflections on the Origin and Spread of Nationalism*, rev. edn (London: Verso).

Andrejevic, Mark (2007), *iSpy: Surveillance and Power in the Interactive Era* (St Lawrence, KS: University Press of Kansas).

Andrew, Christopher (2009), *The Defence of the Realm: The Authorized History of MI5* (London: Allen Lane).

Antoniades, Andreas (2003), ‘Epistemic communities, epistemes and the construction of (world) politics’, *Global Society* 17, no. 1: 21–38.

Appadurai, Arjun (1996), *Modernity at Large: Cultural Dimensions of Globalization* (Minneapolis, MN: University of Minnesota Press).

Aradau, Claudia (2010), ‘Security that matters: Critical infrastructure and objects of protection’, *Security Dialogue* 41, no. 5: 491–514.

Aradau, Claudia and Rens van Munster (2007), ‘Governing terrorism through risk: Taking precautions, (un)knowing the future’, *European Journal of International Relations* 13, no. 1: 89–116.

Aradau, Claudia and Rens van Munster (2008), 'Taming the future: The *dispositif* of risk in the "War on Terror"', in *Risk and the War on Terror*, ed. Louise Amoore and Marieke de Goede (London: Routledge), 23–40.

Aradau, Claudia and Rens van Munster (2011), *Politics of Catastrophe: Genealogies of the Unknown* (London: Routledge).

Armitage, John (1997), 'Accelerated aesthetics: Paul Virilio's *The Vision Machine*', *Angelaki: Journal of the Theoretical Humanities* 2, no. 3: 199–209.

Armitage, John (1999), 'From modernism to hypermodernism and beyond: An interview with Paul Virilio', *Theory, Culture and Society* 16, nos. 5–6: 25–55.

Arnold, Bettina (2014), 'Life after life: Bioarchaeology and post-mortem agency', *Cambridge Archaeological Journal* 24, no. 3: 523–9.

Aron, Raymond (1954), *The Century of Total War*, trs. E.W. Dickes and O.S. Griffiths (London: Derek Verschoyle).

Aron, Raymond (1984) [1978], 'The dawn of universal history', *Politics and History*, ed. and tr. Miriam Bernheim Conant (New Brunswick, NJ: Transaction Publishers), 212–33.

Arquilla, John (2009), 'Information wars', in *Globalization and Security: An Encyclopedia*, vol. I, *Social and Cultural Aspects*, ed. G. Honor Fagan and Ronaldo Munck (Westport, CT: Praeger Security International), 206–20.

Arquilla, John (2012), 'Panetta's wrong about a cyber "Pearl Harbor"', *Foreign Policy*, 19 November, www.foreignpolicy.com/articles/2012/11/19/panettas_wrong_about_a_cyber_pearl_harbor.

Arquilla, John and David Ronfeldt (1997), 'Information, power, and grand strategy: In Athena's Camp—Section 1', in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation), 141–71.

Arquilla, John and David Ronfeldt (1999), *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica, CA: RAND Corporation).

Ashford, Warwick (2014), 'London cyber war game in final of Cyber Security Challenge', *Computer Weekly*, 14 March, www.computerweekly.com/news/2240216180/London-cyber-war-game-in-final-of-Cyber-Security-Challenge.

Attali, Jacques (1982), *Histoires du Temps* (Paris: Fayard).

Augé, Marc (1995) [1992], *Non-Places: Introduction to the Anthropology of Supermodernity*, tr. John Howe (London: Verso).

Augustine (1992), *Confessions*, tr. Henry Chadwick (Oxford University Press).

Aurelius, Marcus (2006), *Meditations*, tr. Martin Hammond (London: Penguin Books).

Aymé, Marcel (2012) [1943], 'The problem of summertime', *The Man Who Walked Through Walls*, tr. Sophie Lewis (London: Pushkin Press), 107–37.

Badger, Emily (2012), 'A tiny city built to be destroyed by cyber terrorists, so real cities know what's coming', *Fast Company*, www.fastcoexist.com/1681033/a-tiny-city-built-to-be-destroyed-by-cyber-terrorists-so-real-cities-know-whats-coming#1.

Baker, Thomas (1857), *The Steam Engine; or, The Powers of Steam. An Original Poem in Ten Cantos* (London: J.S. Hodson).

Bakhtin, Mikhail (1981) [1937–1938], 'Forms of time and of the chronotope in the novel: Notes towards an historical poetics', *The Dialogic Imagination: Four*

Essays by M.M. Bakhtin, ed. Michael Holquist, trs. Caryl Emerson and Michael Holquist (Austin, TX: University of Texas Press), 84–258.

Bambauer, Derek E. (2012), ‘Conundrum’, *Minnesota Law Review* 96, no. 2: 584–674.

Barad, Karen (2007), *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning* (Durham, NC: Duke University Press).

Barbour, Julian (1999), *The End of Time: The Next Revolution in Our Understanding of the Universe* (London: Phoenix).

Barkun, Michael (1997), ‘Millenarians and violence: The case of the Christian identity movement’, in *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*, ed. Thomas Robbins and Susan J. Palmer (New York: Routledge), 247–60.

Barnard-Wills, David and Debi Ashenden (2012), ‘Securing virtual space: Cyber war, cyber terror, and risk’, *Space and Culture* 15, no. 2: 110–23.

Barzashka, Ivanka (2013), ‘Are cyber-weapons effective?’, *The RUSI Journal* 158, no. 2: 48–56.

Baudelaire, Charles (1981), ‘The painter of modern life’, *Selected Writings on Art and Artists*, tr. P.E. Charvet (Cambridge University Press), 390–435.

Baudrillard, Jean (1997), ‘The end of the millennium or the countdown’, *Economy and Society* 26, no. 4: 447–55.

Bauer, Johannes M. and Michel J.G. van Eeten (2009), ‘Cybersecurity: Stakeholder incentives, externalities, and policy options’, *Telecommunications Policy* 33, nos. 10–11: 706–19.

Bazalgette, Joseph W. (1865), *On the Main Drainage of London and the Interception of the Sewage from the River Thames* (London: William Clowes and Sons).

BBC (2012), ‘The One Show’, 13 December, www.youtube.com/watch?v=XvlL2eGohq0.

BBC News (2012a), ‘David Cameron: We must push in “global trade race”’, 12 November, www.bbc.co.uk/news/uk-politics-20304800.

BBC News (2012b), ‘US military train in cyber-city to prepare hack defence’, 28 November, www.bbc.co.uk/news/technology-20525545.

BBC News (2013a), ‘Asteroid 2012 DA14 in record-breaking earth pass’, 15 February, www.bbc.co.uk/news/science-environment-21442863.

Beck, Ulrich (1992), *Risk Society: Towards a New Modernity* (London: Sage).

Beck, Ulrich, Anthony Giddens and Scott Lash (1994), *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Cambridge: Polity Press).

Beck, Ulrich and Daniel Levy (2013) ‘Cosmopolitanized nations: Re-imagining collectivity in world risk society’, *Theory, Culture and Society* 30, no. 2: 3–31.

Beidel, Eric and Stew Magnuson (2011), ‘Government, military face severe shortage of cybersecurity experts’, *National Defense*, www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevere ShortageOfCybersecurityExperts.aspx.

Beissinger, Mark R. (2002), *Nationalist Mobilization and the Collapse of the Soviet State* (Cambridge University Press).

Bell, David E. (2005), ‘Looking back at the Bell-LaPadula model’, Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, AZ, 5–9 December 2005, 337–51.

Belloc, Hillaire (1898), *The Modern Traveller* (London: Edward Arnold).

Bender, John and David E. Wellbery (1991), ‘Introduction’, in *Chronotypes: The Construction of Time*, ed. John Bender and David E. Wellbery (Stanford University Press), 1–15.

Bendrath, Ralf (2001), ‘The cyberwar debate: Perception and politics in US critical infrastructure protection’, *Information and Security* 7: 80–103.

Bendrath, Ralf (2003), ‘The American cyber-angst and the real world—Any link?’, in *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham (New York: The New Press), 49–73.

Bendrath, Ralf, Johan Eriksson and Giampiero Giacomello (2007), ‘From “cyberterrorism” to “cyberwar”, back and forth: How the United States securitized cyberspace’, in *International Relations and Security in the Digital Age*, ed. Johan Eriksson and Giampiero Giacomello (London: Routledge), 57–82.

Beniger, James R. (1986), *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press).

Benjamin, Medea (2013), *Drone Warfare: Killing by Remote Control* (London: Verso).

Benjamin, Walter (1979), ‘One-way street’, *One-Way Street and Other Writings*, trs. Edmund Jephcott and Kingsley Shorter (London: NLB), 45–104.

Bennett, Jane (2010a), ‘A vitalist stopover on the way to a new materialism’, in *New Materialisms: Ontology, Agency, and Politics*, ed. Diana Coole and Samantha Frost (Durham, NC: Duke University Press), 47–69.

Bennett, Jane (2010b), *Vibrant Matter: A Political Ecology of Things* (Durham, NC: Duke University Press).

Bennett, Sue, Karl Maton and Lisa Kervin (2008), ‘The “digital natives” debate: A critical review of the evidence’, *British Journal of Educational Technology* 39, no. 5: 775–86.

Berenskoetter, Felix (2011), ‘Reclaiming the vision thing: Constructivists as students of the future’, *International Studies Quarterly* 55, no. 3: 647–68.

Berger, James (1999), *After the End: Representations of Post-Apocalypse* (Minneapolis, MN: University of Minnesota Press).

Bergson, Henri (1971) [1910], *Time and Free Will: An Essay on the Immediate Data of Consciousness*, tr. J.L. Pogson (London: George Allen and Unwin).

Berinato, Scott (2003), ‘The future of security’, *CIO* 17, no. 6: 71–6, www.cio.com/article/32033/2010_The_Future_of_Security.

Berlant, Lauren (1991), *The Anatomy of National Fantasy: Hawthorne, Utopia, and Everyday Life* (University of Chicago Press).

Betz, David J. and Tim Stevens (2011), *Cyberspace and the State* (London: Routledge).

Betz, David J. and Tim Stevens (2013), ‘Analogical reasoning and cyber security’, *Security Dialogue* 44, no. 2: 147–64.

Bevan, Robert (2006), *The Destruction of Memory: Architecture at War* (London: Reaktion Books).

Bharara, Preet (2012), ‘Asleep at the laptop’, *The New York Times*, 4 June.

Bhaskar, Rahul (2006), ‘State and local law enforcement is not ready for a Cyber Katrina’, *Communications of the ACM* 49, no. 2: 81–3.

Bigo, Didier (2001), ‘The Möbius ribbon of internal and external security(ies)’, in *Identities, Borders, Orders: Rethinking International Relations Theory*, ed. Mathias Albert, David Jacobson and Yosef Lapid (Minneapolis, MN: University of Minnesota Press), 91–136.

Bigo, Didier (2006), ‘Security, exception, ban and surveillance’, in *Theorizing Surveillance: The Panopticon and Beyond*, ed. David Lyon (Cullompton: Willan), 46–68.

Binnick, Robert I. (1991), *Time and the Verb: A Guide to Tense and Aspect* (New York: Oxford University Press).

Bipartisan Policy Center (2010), ‘Cyber ShockWave shows US unprepared for cyber threats’, press release, 17 February, http://bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats.

Birkland, Thomas A. (2006), *Lessons of Disaster: Policy Change After Catastrophic Events* (Washington, DC: Georgetown University Press).

Blank, Stephen (2008), ‘Web War I: Is Europe’s first information war a new kind of war?’, *Comparative Strategy* 27, no. 3: 227–47.

Bliss, Jeff (2010), ‘US unprepared for “cyber war”, former top spy official says’, *Bloomberg Businessweek*, 23 February.

Blum, Justin (2005), ‘Hackers target US power grid’, *Washington Post*, 11 March.

Blumenson, Martin (1999), ‘The emergence of infrastructure as a decisive strategic concept’, *Parameters* 29, no. 3: 39–45.

Bobbitt, Philip (2008), *Terror and Consent: The Wars for the Twenty-First Century* (London: Penguin).

Bobrow, Davis B. (1986), ‘Complex insecurity: Implications of a sobering metaphor’, *International Studies Quarterly* 40, no. 4: 435–50.

Bochel, Hugh, Andrew Defty and Jane Kirkpatrick (2015), ‘“New mechanisms of independent accountability”: Select Committees and parliamentary scrutiny of the intelligence services’, *Parliamentary Affairs* 68, no. 2: 314–31.

Boellstorff, Tom (2008), *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human* (Princeton University Press).

Boin, Arjen (2004), ‘Lessons from crisis research’, *International Studies Review* 6, no. 1: 165–74.

Boin, Arjen and Allan McConnell (2007), ‘Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience’, *Journal of Contingencies and Crisis Management* 15, no. 1: 50–9.

Bolt, Neville (2009), ‘Unsettling networks’, *The RUSI Journal* 154, no. 5: 34–9.

Booth, Ken (1997), ‘Security and self: Reflections of a fallen realist’, in *Critical Security Studies: Concepts and Cases*, ed. Keith Krause and Michael C. Williams (Abingdon: Routledge), 83–119.

Booth, Ken (2007), *Theory of World Security* (Cambridge University Press).

Borgmann, Albert (1999), *Holding On to Reality: The Nature of Information at the Turn of the Millennium* (University of Chicago Press).

Bostrom, Nick and Milan M. Ćirković, ed. (2008), *Global Catastrophic Risks* (Oxford University Press).

Bourbeau, Philippe (2013), ‘Resiliencism: Premises and promises in securitisation research’, *Resilience: International Policies, Practices and Discourses* 1, no. 1: 3–17.

Bousquet, Antoine (2006), ‘Time Zero: Hiroshima, September 11 and apocalyptic revelations in historical consciousness’, *Millennium: Journal of International Studies* 41, no. 2: 739–64.

Bowker, Geoffrey (1993), ‘How to be universal: Some cybernetic strategies, 1943–70’, *Social Studies of Science* 23, no. 1: 107–27.

Boyer, Paul S. (1992), *When Time Shall Be No More: Prophecy Belief in Modern American Culture* (Cambridge, MA: Harvard University Press).

Boyle, Philip and Kevin D. Haggerty (2009), ‘Spectacular security: Mega-events and the security complex’, *International Political Sociology* 3, no. 3: 257–74.

Boyle, Philip and Kevin D. Haggerty (2012), ‘Planning for the worst: Risk, uncertainty and the Olympic Games’, *The British Journal of Sociology* 63, no. 2: 241–59.

Bozeman, John M. (1997), ‘Technological millennialism in the United States’, in *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*, ed. Thomas Robbins and Susan J. Palmer (New York: Routledge), 139–58.

Brandão, Luis Alberto (2006), ‘Chronotope’, *Theory, Culture and Society* 23, nos. 2–3: 133–4.

Brants, Kees (1989), ‘The social construction of the information revolution’, *European Journal of Communication* 4, no. 1: 79–97.

Braund, Simon (2010), ‘How Ronald Reagan learned to start worrying and stop loving the bomb’, *Empire* 257: 134–40.

Brenner, Susan W. (2009), *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press).

Brewster, Thomas (2012), ‘David Cameron welcomes Microsoft UK IT skills initiative’, *Tech Week Europe*, 7 November, www.techweekeurope.co.uk/workspace/david-cameron-microsoft-skills-98570.

Brodie, Bernard (1978), ‘The development of nuclear strategy’, *International Security* 2, no. 4: 65–83.

Bromley, David G. (1997), ‘Constructing apocalypticism: Social and cultural elements of radical organization’, in *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*, ed. Thomas Robbins and Susan J. Palmer (New York: Routledge), 32–45.

Brosnan, Mark (1998), *Technophobia: The Psychological Impact of Information Technology* (London: Routledge).

Brown, Chris (1994), ‘“Turtles all the way Down”: Anti-foundationalism, critical theory and International Relations’, *Millennium: Journal of International Studies* 23, no. 2: 213–36.

Brown, Ian, Lilian Edwards and Christopher Marsden (2009), ‘Information security and cybercrime’, in *Law and the Internet*, 3rd edn, ed. Lilian Edwards and Charlotte Weldes (Oxford: Hart Publishing), 671–92.

Browning, Christopher S. and Matt McDonald (2013), ‘The future of critical security studies: Ethics and the politics of security’, *European Journal of International Relations* 19, no. 2: 235–55.

Bruno, Greg (2008), ‘Backgrounder: The evolution of cyber warfare’, *The New York Times*, 27 February, www.nytimes.com/cfr/world/slot1_20080227.html.

Bubandt, Nils (2005), ‘Vernacular security: The politics of feeling safe in global, national and local worlds’, *Security Dialogue* 36, no. 3: 275–96.

Buchanan, Ben (2014), ‘Speed and asymmetry in cyber operations’, unpublished manuscript.

Buchanan, Brett (2008), *Onto-Ethologies: The Animal Environments of Uexküll. Heidegger, Merleau-Ponty, and Deleuze* (Albany, NY: State University of New York Press).

Budiansky, Stephen (2010), ‘What’s the use of cryptologic history?’, *Intelligence and National Security* 25, no. 6: 767–77.

Buelens, Geert, Harald Hendrix and Monica Jansen, ed. (2012), *The History of Futurism: The Precursors, Protagonists, and Legacies* (Plymouth: Lexington Books).

Bulmer, Martin (1979), ‘Preface’, in *Censuses, Surveys and Privacy*, ed. Martin Bulmer (London: Macmillan), viii–x.

Bumiller, Elisabeth (2013), ‘Pentagon expanding cybersecurity force to protect networks against attacks’, *The New York Times*, 28 January.

Bumiller, Elisabeth and Thom Shanker (2012), ‘Panetta warns of dire threat of cyberattack’, *The New York Times*, 12 October.

Burgess, J. Peter (2007), ‘Social values and material threat: The European Programme for Critical Infrastructure Protection’, *International Journal of Critical Infrastructures* 3, nos. 3–4: 471–87.

Burke, Edmund (1770), *Thoughts on the Cause of the Present Discontents*, 3rd edn (London: J. Dodsley).

Burnet, John (1930) [1892], *Early Greek Philosophy*, 4th edn (London: Adam and Charles Black).

Burnham, David (1983), *The Rise of the Computer State* (London: Weidenfeld and Nicolson).

Buzan, Barry (1983), *People, States and Fear: The National Security Problem in International Relations* (Brighton: Wheatsheaf Books).

Buzan, Barry and Lene Hansen (2009), *The Evolution of International Security Studies* (Cambridge University Press).

Buzan, Barry and Ole Wæver (2009), ‘Macrosecuritisation and security constellations: Reconsidering scale in securitisation theory’, *Review of International Studies* 35, no. 2: 253–76.

Buzan, Barry, Ole Wæver and Jaap de Wilde (1998), *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers).

Byrd, Hugh and Steve Matthewman (2014), ‘Exergy and the city: The technology and sociology of power (failure)’ *Journal of Urban Technology* 21, no. 3: 85–102.

Cabinet Office (2011), *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: Cabinet Office).

Callon, Michel (1986), ‘Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St. Brieuc Bay’, in *Power, Action and Belief: A New Sociology of Knowledge?*, ed. John Law (London: Routledge), 196–233.

Cameron, Craig M. (1994), *American Samurai: Myth, Imagination, and the Conduct of Battle in the First Marine Division, 1941–1951* (Cambridge University Press).

Cameron, David (2012a), speech, Conservative Party Conference, Birmingham, 10 October, www.bbc.co.uk/news/uk-politics-19897855.

Cameron, David (2012b), speech, Confederation of British Industry, London, 19 November, www.number10.gov.uk/news/speech-to-cbi/.

Campbell, David (1998), *Writing Security: United States Foreign Policy and the Politics of Identity*, rev. edn (Minneapolis, MN: University of Minnesota Press).

Campbell, David (2002), 'Time is broken: The return of the past in the response to September 11', *Theory and Event* 5, no. 4: n.p., http://muse.jhu.edu/journals/theory_and_event/summary/v005/5.4campbell.html.

Campbell, David (2010), 'Poststructuralism', in *International Relations Theories: Discipline and Diversity*, 2nd edn, ed. Tim Dunne, Milja Kurki and Steve Smith (Oxford University Press), 213–37.

Camus, Albert (1991) [1955], *The Myth of Sisyphus and Other Essays*, tr. Justin O'Brien (New York: Vintage International).

Canadian Broadcasting Corporation (1967), 'Marshall McLuhan in conversation with Norman Mailer', *The Way It Is*, 26 November.

Canales, Jimena (2009), *A Tenth of a Second: A History* (University of Chicago Press).

Canetti, Elias (1973) [1960], *Crowds and Power* (New York: Farrar, Straus and Giroux).

Cannavò, Peter F. (2012), 'Ecological citizenship, time, and corruption: Aldo Leopold's Green Republicanism', *Environmental Politics* 21, no. 6: 864–81.

Cant, Sue (2003), '"Cyber 9/11" risk warning', *Sydney Morning Herald*, 22 April.

Cantril, Hadley (2005) [1940], *The Invasion from Mars: A Study in the Psychology of Panic* (Princeton University Press).

Carr, Matt (2010), 'Slouching towards dystopia: The new military futurism', *Race and Class* 51, no. 3: 13–32.

Casasanto, Daniel and Lera Boroditsky (2008), 'Time in mind: Using space to think about time', *Cognition* 106, no. 2: 579–93.

Castells, Manuel (2000), 'Urban sustainability in the information age', *City: Analysis of Urban Trends, Culture, Theory, Policy, Action* 4, no. 1: 118–22.

Castells, Manuel (2010) [1996], *The Information Age: Economy, Society, and Culture*, vol. I: *The Rise of the Network Society*, 2nd edn (Chichester: Wiley-Blackwell).

Castoriadis, Cornelius (1991), 'Time and creation', in *Chronotypes: The Construction of Time*, ed. John Bender and David E. Wellbery (Stanford University Press), 38–64.

Cebrowski, Arthur K. (1998), 'Forum', *Issues in Science and Technology* 15, no. 2: n.p., www.issues.org/15.2/forum.htm.

Center for Strategic and International Studies (CSIS) (1998), *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo* (Washington, DC: CSIS).

Center for Strategic and International Studies (CSIS) (2008), *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC: CSIS).

Central Office of Information (1998), *Our Information Age: The Government's Vision* (London: Central Office of Information).

Ceruzzi, Paul E. (1991), 'When computers were human', *Annals of the History of Computing* 13, no. 3: 237–44.

Ceruzzi, Paul E. (2003), *A History of Modern Computing*, 2nd edn (Cambridge, MA: MIT Press).

CESG (2012), 'New certification scheme announced for IA professionals', press release, 24 October, www.cesg.gov.uk/News/Pages/New-IA-Certification-pages.aspx.

Chakrabarty, Dipesh (2000), *Provincializing Europe: Postcolonial Thought and Historical Difference* (Princeton University Press).

Chandler, David (2012), 'Resilience and human security: The post-interventionist paradigm', *Security Dialogue* 43, no. 3: 213–29.

Chandler, David (2013), 'Resilience and the autotelic subject: Toward a critique of the societalization of security', *International Political Sociology* 7, no. 2: 210–26.

Chandler, Ralph Clark (1985), 'Little Boy, Fat Man, and the Rapture: The effects of late twentieth century apostasy on public policy', *Dialogue* 8, no. 1: 1–39.

Chang, Kenneth (2014), 'Automating cybersecurity', *The New York Times*, 3 June.

Chapman, Siobhan (2009), 'Government criticised for plan to hire "naughty boys"', *ComputerWorld UK*, 30 June, www.computerworlduk.com/news/security/15467/government-criticised-for-plan-to-hire-naughty-boys/.

Chertoff, Michael (2008a), 'The cybersecurity challenge', *Regulation and Governance* 2, no. 4: 480–4.

Chertoff, Michael (2008b), 'Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference', San Francisco, CA, 8 April.

Chesneaux, Jean (2000), 'Speed and democracy: An uneasy dialogue', *Social Science Information* 39, no. 3: 407–420.

Childers, Erskine (1995) [1903], *The Riddle of the Sands: A Record of Secret Service* (London: Penguin).

Clark, Katerina and Michael Holquist (1984), *Mikhail Bakhtin* (Cambridge, MA: Harvard University Press).

Clarke, Lee (2006), *Worst Cases: Terror and Catastrophe in the Popular Imagination* (University of Chicago Press).

Clarke, Richard A. (1999), 'Threats to US national security: Proposed partnership initiatives towards preventing cyber terrorist attacks', *DePaul Business Law Journal* 12, nos. 1–2: 33–43.

Clarke, Richard A. and Robert K. Knake (2010), *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco).

Clarke, Roger (2011), 'Cyborg rights', *IEEE Technology and Society Magazine* 30, no. 3: 49–57.

Clayton, Mark (2012a), 'Senate cybersecurity bill fails, so Obama could take charge', *The Christian Science Monitor*, 16 November.

Clayton, Mark (2012b), '"Cyber Pearl Harbor": Could future cyberattack really be that devastating?', *The Christian Science Monitor*, 7 December.

CNN (2010), 'We were warned: Cyber Shockwave', first broadcast, 20 February.

Coaffee, Jon (2010) 'Protecting vulnerable cities: The UK's resilience response to defending everyday urban infrastructure', *International Affairs* 86, no. 4: 939–54.

Coaffee, Jon, Paul O'Hare and Marian Hawkesworth (2009), 'The visibility of (in)security: The aesthetics of planning urban defences against terrorism', *Security Dialogue* 40, nos. 4–5: 489–511.

Cobb, Adam (1999), 'Electronic Gallipoli?', *Australian Journal of International Affairs* 53, no. 2: 133–49.

Coetzee, J.M. (1999), *The Lives of Animals* (Princeton University Press).

Cohen, Julie E. (2007), 'Cyberspace as/and space', *Columbia Law Review* 107, no. 1: 210–56.

Cohen, Tova and Maayan Lubell (2012), 'Nations must talk to halt "cyber terrorism"—Kaspersky', *Reuters*, 6 June.

Cohn, Norman (2004) [1957], *The Pursuit of the Millennium: Revolutionary Millenarians and Mystical Anarchists of the Middle Ages* (London: Pimlico).

Coker, Christopher (2004), *The Future of War: The Re-Enchantment of War in the Twenty-First Century* (Malden, MA: Blackwell Publishing).

Coker, Christopher (2013), *Warrior Geeks: How 21st Century Technology is Changing the Way We Fight and Think About War* (London: Hurst & Company).

Colbaugh, Richard and Kristin Glass, ed. (2012), *Proactive Defense for Evolving Cyber Threats* (Albuquerque, NM: Sandia National Laboratories).

Collier, Stephen J. and Andrew Lakoff (2008), 'The vulnerability of vital systems: How "critical infrastructure" became a security problem', in *Securing 'the Homeland': Critical Infrastructure, Risk and (In)security*, ed. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge), 17–39.

Collier, Stephen J. and Aihwa Ong (2005), 'Global assemblages, anthropological problems', in *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*, ed. Aihwa Ong and Stephen J. Collier (Malden, MA: Blackwell), 3–21.

Collin, Andrew (1993), 'Andrew Booth's computers at Birkbeck College', *Resurrection: The Bulletin of the Computer Conservation Society* 5: 11–16.

Collins, Craig (2013), 'Cybersecurity and sequestration', *Defense Media Network*, 5 May, www.defensemedianetwork.com/stories/cybersecurity-and-sequestration/.

Colon, Marcus (2012), 'Spies recruiting hackers: Gen. Keith Alexander at DefCon', *SC Magazine*, September, www.scmagazine.com/spies-recruiting-hackers-gen-keith-alexander-at-defcon/article/254692/.

Committee on Manpower Resources for Science and Technology (1968), *The Flow Into Employment of Scientists, Engineers and Technologists. Report of the Working Group on Manpower for Scientific Growth* (London: HMSO).

Connah, Graham (2010), *Writing About Archaeology* (Cambridge University Press).

Connolly, Patrick J. (2014), 'Newton and God's sensorium', *Intellectual History Review* 24, no. 2: 185–201.

Connolly, William E. (2000), ‘Speed, concentric cultures, and cosmopolitanism’, *Political Theory* 28, no. 5: 596–618.

Conway, Maura (2008), ‘Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures’, in *Securing ‘the Homeland’: Critical Infrastructure, Risk and (In)security*, ed. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge), 109–29.

Conway, Maura (2011), ‘Against cyberterrorism’, *Communications of the ACM* 54, no. 2: 26–8.

Cook, Martin L. (2004), ‘Christian apocalypticism and weapons of mass destruction’, in *Ethics and Weapons of Mass Destruction: Religious and Secular Perspectives*, ed. Sohail H. Hashmi and Steven P. Lee (Cambridge University Press), 200–10.

Cooper, John (2011), *The Queen’s Agent: Frances Walsingham at the Court of Elizabeth I* (London: Faber and Faber).

Copeland, B. Jack, ed. (2006), *Colossus: The Secrets of Bletchley Park’s Codebreaking Computers* (Oxford University Press).

Copeland, Dale C. (2000), ‘The constructivist challenge to structural realism: A review essay’, *International Security* 25, no. 2: 187–212.

Cordle, Daniel (2013), ‘“That’s going to happen to us. It is”: *Threads* and the imagination of nuclear disaster on 1980s television’, *Journal of British Cinema and Television* 10, no. 1: 71–92.

Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke (2010), *On Cyber Warfare* (London: Chatham House).

Coward, Martin (2009), *Urbicide: The Politics of Urban Destruction* (Abingdon: Routledge).

Cox, Robert W. (1981), ‘Social forces, states and world orders: Beyond International Relations theory’, *Millennium: Journal of International Studies* 10, no. 2: 126–55.

Croft, Stuart (2008), ‘What future for security studies?’, in *Security Studies: An Introduction*, ed. Paul D. Williams (London: Routledge), 499–511.

Crosthwaite, Paul (2011), ‘The accident of finance’, in *Virilio Now: Current Perspectives in Virilio Studies*, ed. John Armitage (Cambridge: Polity), 177–99.

Cunningham, Kevin and Robert R. Tomes (2004), ‘Space-time orientations and contemporary political-military thought’, *Armed Forces and Society* 31, no. 1: 119–40.

Curtis, Sophie (2014), ‘School children to be trained in cyber warfare’, *The Telegraph*, 11 August, www.telegraph.co.uk/technology/internet-security/11025457/School-children-to-be-trained-in-cyber-warfare.html.

Daily Telegraph (2013), ‘Russian meteor exploded with force of 30 Hiroshima bombs’, 16 February.

Dainton, Barry (2010) [2001], *Time and Space*, 2nd edn (Durham: Acumen).

D’Amico, Robert (1989), *Historicism and Knowledge* (New York: Routledge).

Daniel, Lisa (2011), ‘Panetta: Intelligence community needs to predict uprisings’, *American Forces Press Service*, 11 February, www.defense.gov/news/newsarticle.aspx?id=62790.

Davis, Joshua (2007), 'Hackers take down the most wired country in Europe', *Wired* 15, no. 9, www.wired.com/politics/security/magazine/15–09/ff_estonia.

Davis, Mike (1999), *Ecology of Fear: Los Angeles and the Imagination of Disaster* (New York: Vintage Books).

Davis, Jon and Shane Magrath (2013), *A Survey of Cyber Ranges and Testbeds* (Edinburgh, Australia: Defence Science and Technology Organisation).

Davis Cross, Mai'a K. (2013), 'Rethinking epistemic communities twenty years later', *Review of International Studies* 39, no. 1: 137–60.

Debrix, François (2008), *Tabloid Terror: War, Culture and Geopolitics* (London: Routledge).

Deering, Christopher J. and Forrest Maltzman (1999), 'The politics of executive orders: Legislative constraints on Presidential power', *Political Research Quarterly* 52, no. 4: 767–83.

Defense Advanced Research Projects Agency (2008a), 'National Cyber Range proposers' day workshop', Special Notice DARPA-SN08-33, 29 April, www.fbo.gov/index?s=opportunity&mode=form&id=250832bfd8f71f0340ce65767397fb25&tab=core&_cview=0.

Defense Advanced Research Projects Agency (2008b), 'National Cyber Range', Broad Agency Announcement DARPA-BAA-08–43, 5 May, www.fbo.gov/download/c33/c330660f00c9820d05c9f4c54422024b/080505_BAA_National_Cyber_Range_Final.doc.

Defense Advanced Research Projects Agency (2012), 'National Cyber Range rapidly emulates complex networks', press release, 13 November, www.darpa.mil/NewsEvents/Releases/2012/11/13.aspx.

Defense Science Board (2013), *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Department of Defense).

De Goede, Marieke (2008a), 'The politics of preemption and the war on terror in Europe', *European Journal of International Relations* 14, no. 1: 161–85.

De Goede, Marieke (2008b), 'Beyond risk: Premediation and the post-9/11 security imagination', *Security Dialogue* 39, nos. 2–3: 155–76.

De Goede, Marieke and Beatrice de Graaf (2013), 'Sentencing risk: Temporality and precaution in terrorism trials', *International Political Sociology* 7, no. 3: 313–31.

De Goede, Marieke and Samuel Randalls (2009), 'Precaution, preemption: Arts and technologies of the actionable future', *Environment and Planning D: Society and Space* 27, no. 5: 859–78.

Deibert, Ronald J. (1997), *Parchment, Printing, and Hypermedia: Communication in World Order Transformation* (New York: Columbia University Press).

Deibert, Ronald J. (1999), 'Harold Innis and the Empire of Speed', *Review of International Studies* 25, no. 2: 273–89.

Deibert, Ronald J. (2003), 'Black code: Censorship, surveillance, and the militarisation of cyberspace', *Millennium: Journal of International Studies* 32, no. 3: 501–30.

Deibert, Ronald J. (2008), 'Black code redux: Censorship, surveillance, and the militarization of cyberspace', in *Digital Media and Democracy: Tactics in Hard Times*, ed. Megan Boler (Cambridge, MA: MIT Press), 137–62.

Deibert, Ronald J. (2012), 'The growing dark side of cyberspace (. . . and what to do about it)', *Penn State Journal of Law and International Affairs* 1, no. 2: 260–74.

Deibert, Ronald J. and Masashi Crete-Nishihata (2012), 'Global governance and the spread of cyberspace controls', *Global Governance* 18, no. 3: 339–61.

Deibert, Ronald J. and Rafal Rohozinski (2011), 'The new cyber military industrial complex', *The Globe and Mail*, 28 March, www.theglobeandmail.com/commentary/the-new-cyber-military-industrial-complex/article573990/.

DeLanda, Manuel (2006), *A New Philosophy of Society: Assemblage Theory and Social Complexity* (London: Continuum).

DeLashmutt, Michael W. (2006), 'A better life through information technology? The techno-theological eschatology of posthuman speculative science', *Zygon* 41, no. 2: 267–88.

De Leeuw, Karl and Jan Bergstra, ed. (2007), *The History of Information Security: A Comprehensive Handbook* (Amsterdam: Elsevier).

Deleuze, Gilles and Félix Guattari (2004) [1980], *Capitalism and Schizophrenia*, vol. II, *A Thousand Plateaus*, tr. Brian Massumi (London: Continuum).

De Mul, Jos (1999), 'The informatization of the worldview', *Information, Communication and Society* 2, no. 1: 69–94.

Dennett, Daniel C. (2000), 'Making tools for thinking', in *Metarepresentations: A Multidisciplinary Perspective*, ed. Dan Sperber (New York: Oxford University Press), 17–29.

Denning, Dorothy (2003), 'Cyber-security as an emergent infrastructure', in *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security*, ed. Robert Latham (New York: The New Press), 25–48.

Denning, Peter J. and Dennis J. Frailey (2011), 'Who are we—Now?', *Communications of the ACM* 54, no. 6: 25–7.

Department for Culture, Media and Sport (2013), 'Stimulating private sector investment to achieve a transformation in broadband in the UK by 2015', 27 February, www.gov.uk/government/policies/transforming-uk-broadband.

Department for Education (2012), '"Harmful" ICT curriculum set to be dropped to make way for rigorous computer science', press release, 11 January, www.gov.uk/government/news/harmful-ict-curriculum-set-to-be-dropped-to-make-way-for-rigorous-computer-science.

Department for Education (2013) 'Consultation on computing and disapplication of the current national curriculum', 3 May, http://webarchive.nationalarchives.gov.uk/20130904084020/https://www.education.gov.uk/schools/teachingandlearning/curriculum/nationalcurriculum2014/a00224578/consultation.

Der Derian, James (1990), 'The (s)pace of international relations: Simulation, surveillance, and speed', *International Studies Quarterly* 34, no. 3: 295–310.

Der Derian, James (1992), *Antidiplomacy: Spies, Terror, Speed and War* (Oxford: Blackwell).

Der Derian, James (1999), 'The conceptual cosmology of Paul Virilio', *Theory, Culture and Society* 16, nos. 5–6: 215–27.

Der Derian, James (2001), 'Global events, national security, and virtual theory', *Millennium: Journal of International Studies* 30, no. 3: 669–90.

Der Derian, James (2002), 'Virtuous war/virtual theory', *International Affairs* 76, no. 4: 771–88.

Der Derian, James (2003), ‘The question of information technology in International Relations’, *Millennium: Journal of International Studies* 32, no. 3: 441–56.

Der Derian, James (2009a) [2001], *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*, 2nd edn (New York: Routledge).

Der Derian, James (2009b), ‘Paul Virilio’, in *Critical Theorists and International Relations*, ed. Jenny Edkins and Nick Vaughan-Williams (Abingdon: Routledge), 330–40.

Der Derian, James and Jesse Finkelstein (2008), ‘Critical infrastructures and network pathologies: The Semiotics and Biopolitics of Heteropolarity’, in *Securing ‘the Homeland’: Critical Infrastructure, Risk and (In)security*, ed. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge), 84–105.

Derrida, Jacques (1984), ‘No apocalypse, not now (full speed ahead, seven missiles, seven missives)’, *Diacritics* 14, no. 2: 20–31.

Devji, Faisal (2005), *Landscapes of the Jihad: Militancy, Morality, Modernity* (London: Hurst & Company).

Díaz-Andreu, Margarita (1996), ‘Constructing identities through culture: The past in the forging of Europe’, in *Cultural Identity and Archaeology: The Construction of European Communities*, ed. Paul Graves-Brown, Siân Jones and Clive Gamble (London: Routledge), 48–61.

Dietrich, Rainer, Wolfgang Klein and Colette Noyau (1995), *The Acquisition of Temporality in a Second Language* (Amsterdam: John Benjamins Publishing Company).

Dillon, Michael (1996), *Politics of Security: Towards a Political Philosophy of Continental Thought* (London: Routledge).

Dillon, Michael (2002), ‘Network society, network-centric warfare and the state of emergency’, *Theory, Culture and Society* 19, no. 4: 71–9.

Dillon, Michael (2003a), ‘Virtual security: A life science of (dis)order’, *Millennium: Journal of International Studies* 32, no. 3: 531–58.

Dillon, Michael (2003b), ‘Intelligence incarnate: Martial corporeality in the digital age’, *Body and Society* 9, no. 4: 123–47.

Dillon, Michael (2004), ‘The security of governance’, in *Global Governmentality: Governing International Spaces*, ed. Wendy Larner and William Walters (Abingdon: Routledge, 2004), 76–94.

Dillon, Michael (2011), ‘Specters of biopolitics: Finitude, *eschaton*, and *katechon*’, *South Atlantic Quarterly* 110, no. 3: 780–92.

Dillon, Michael and Luis Lobo-Guerrero (2009), ‘The biopolitical imaginary of species-being’, *Theory, Culture and Society* 26, no. 1: 1–23.

Dillon, Michael and Julian Reid (2001), ‘Global liberal governance: Biopolitics, security and war’, *Millennium: Journal of International Studies* 30, no. 1: 41–66.

Dillon, Michael and Julian Reid (2009), *The Liberal Way of War: Killing to Make Life Live* (London: Routledge).

Dimitrov, Radoslav S. (2010), ‘Inside Copenhagen: The state of climate governance’, *Global Environmental Politics* 10, no. 2: 18–24.

Doctorow, Cory and Charles Stross (2012), *The Rapture of the Nerds* (New York: Tor Books).

Dodge, Martin and Rob Kitchin (2004), 'Charting movement: Mapping internet infrastructures', in *Moving People, Goods, and Information in the 21st Century: The Cutting-Edge Infrastructures of Networked Cities*, ed. Richard E. Hanley (New York: Routledge), 159–85.

D'Ottavi, Alberto (2003), 'Firewall pioneer: Security needs integration', *Zone-H*, 4 February, www.zone-h.org/news/id/2058.

Dover, Robert and Michael S. Goodman, ed. (2011), *Learning from the Secret Past: Cases in British Intelligence History* (Washington, DC: Georgetown University Press).

Duncan, James (1993), 'Sites of representation: Place, time and the discourse of the other', in *Place/Culture/Representation*, ed. James Duncan and David Ley (London: Routledge), 39–56.

Dunn, Myriam (2007), 'Securing the digital age: The challenges of complexity for critical infrastructure protection and IR theory', in *International Relations and Security in the Digital Age*, ed. Johan Eriksson and Giampiero Giacomello (London: Routledge), 85–105.

Dunn, Myriam and Victor Mauer (2006), 'Towards a global culture of cyber-security', in *The International CIIP Handbook 2006*, vol. II: *Analyzing Issues, Challenges, and Prospects*, ed. Myriam Dunn and Victor Mauer (Zurich: Swiss Federal Institute of Technology), 189–206.

Dunn, Myriam and Victor Mauer (2007), 'The role of the state in securing the information age—Challenges and prospects', in *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, ed. Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel (Aldershot: Ashgate), 151–62.

Dunn Cavelty, Myriam (2007), 'Cyber-terror—Looming threat or phantom menace? The framing of the US cyber-threat debate', *Journal of Information Technology and Politics* 4, no. 1: 19–36.

Dunn Cavelty, Myriam (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge).

Dunn Cavelty, Myriam (2013), 'From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse', *International Studies Review* 15, no. 1: 105–22.

Dunn Cavelty, Myriam (2014), 'Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities', *Science and Engineering Ethics* 20, no. 3: 701–15.

Dunn Cavelty, Myriam and Jennifer Giroux (2015), 'The good, the bad, and the sometimes ugly: Complexity as both threat and opportunity in the vital systems security discourse', in *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life*, ed. Emilian Kavalski (Albany, NY: SUNY Press), 209–27.

Dunn Cavelty, Myriam and Kristian Søby Kristensen (2008), 'Introduction: Securing the homeland: Critical infrastructure, risk and (in)security', in *Securing 'the Homeland': Critical Infrastructure, Risk and (In)security*, ed. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge), 1–14.

Dunn Cavelty, Myriam and Manuel Suter (2012), 'The art of CIIP strategy: Taking stock of content and processes', in *Critical Information Infrastructure*

Protection, ed. Javier Lopez, Robert Setola and Stephen D. Wolthusen (Berlin: Springer-Verlag), 15–38.

Dutil, Patrice (2014), 'Paths, precedents, parallels and pendulums: The uses of the past in public policy and administration', *Canadian Public Administration* 57, no. 3: 419–35.

Dyer, Geoff (2012), 'Panetta warns US of "cyber Pearl Harbor"', *FT.com*, 12 October, www.ft.com/cms/s/0/6c06b03a-1423-11e2-9ac6-00144feabdc0.html#axzz2PsqYDZXx.

Eckler, A. Ross (1972), *The Bureau of the Census* (New York: Praeger Publishers).

Eddington, Arthur S. (1928), *The Nature of the Physical World* (New York: Macmillan).

Edelman, Murray (1964), *The Symbolic Uses of Politics* (Urbana, IL: University of Illinois Press).

Edwards, Paul N. (1996), *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press).

Eliot, T.S. (1971) [1943], 'Burnt Norton', *Four Quartets* (San Diego, CA: Harvest).

Ellis, Stephen (2011), *Season of Rains: Africa in the World* (London; Hurst & Company).

Elzen, Boelie and Donald MacKenzie (1994), 'The social limits of speed: The development and use of supercomputers', *IEEE Annals of the History of Computing* 16, no. 1: 46–61.

English, Richard (2009), *Terrorism: How to Respond* (Oxford University Press).

ENISA (2012), *On National and International Cyber Security Exercises: Survey, Analysis and Recommendations* (Heraklion: ENISA).

Enloe, Cynthia (2011), 'The mundane matters', *International Political Sociology* 5, no. 4: 447–50.

Epstein, Keith (2009), 'Fearing "Cyber Katrina", Obama candidate for cyber czar urges a "FEMA for the internet"', *Bloomberg Businessweek*, 18 February, www.businessweek.com/the_thread/techbeat/archives/2009/02/fearing_cyber_k.html.

Erikson, Kai (1994), *A New Species of Trouble: The Human Experience of Modern Disasters* (New York: W.W. Norton & Company).

Eriksson, Johan (2001), 'Cyberplagues, IT, and security: Threat politics in the information age', *Journal of Contingencies and Crisis Management* 9, no. 4: 211–22.

Eriksson, Johan and Giampiero Giacomello (2007), 'Introduction: Closing the gap between International Relations theory and studies of digital-age security', in *International Relations and Security in the Digital Age*, ed. Johan Eriksson and Giampiero Giacomello (London: Routledge), 1–28.

e-skills UK (n.d.), 'Cyber security in schools: Cyber ninjas keep Cyber City secure', www.infosecurityeurope.com/__novadocuments/28345?v=635018761162070000.

e-skills UK (2013), *Career Analysis into Cyber Security: New and Evolving Occupations* (London: e-skills UK).

Euben, Roxanne L. (1999), *Enemy in the Mirror: Islamic Fundamentalism and the Limits of Modern Rationalism* (Princeton University Press).

Fabian, Johannes (2002) [1983], *Time and the Other: How Anthropology Makes Its Object* (New York: Columbia University Press).

Farrell, Theo (1996), 'Figuring out fighting organisations: The new organisational analysis in strategic studies', *Journal of Strategic Studies* 19, no. 1: 122–35.

Farrell, Theo (2002), 'Constructivist security studies: Portrait of a research program', *International Studies Review* 4, no. 1: 49–72.

Farwell, James P. and Rafal Rohozinski (2011), 'Stuxnet and the future of cyber war', *Survival* 53, no. 1: 23–40.

Fawaz, Mona and Hiba Bou Akar (2012), 'Practicing (in)security in the city', *City and Society* 24, no. 2: 105–9.

Featherstone, Mark (2010), 'Virilio's apocalypticism', *CTheory*, 16 September, www.ctheory.net/articles.aspx?id=662.

Federal Civil Defense Administration (1955a), *Cue For Survival: Operation Cue* (Washington, DC: US Government Printing Office).

Federal Civil Defense Administration (1955b), 'Operation Cue', film, 15 minutes, http://archive.org/details/Operatio1955.

Feldman, Stanley and Lee Sigelman (1985), 'The political impact of prime-time television: "The Day After"', *The Journal of Politics* 47, no. 2: 556–78.

Fink, Glenn A., Jereme N. Haack, A. David McKinnon and Errin W. Fulp (2014), 'Defense on the move: Ant-based cyber defense', *IEEE Security and Privacy* 12, no. 2: 36–43.

Fisher, Kathryn Marie (2013), 'Exploring the temporality in/of British counterterrorism law and lawmaking', *Critical Studies on Terrorism* 6, no. 1: 50–72.

Fletcher, Paul (2004), 'The political theology of the empire to come', *Cambridge Review of International Affairs* 17, no. 1: 49–61.

Floridi, Luciano (1995), 'Internet: Which future for organized knowledge, Frankenstein or Pygmalion?', *International Journal of Human-Computer Studies* 43, no. 2: 261–74.

Floridi, Luciano (2011), *The Philosophy of Information* (Oxford University Press).

Floridi, Luciano (2012), 'Hyperhistory and the philosophy of information policies', *Philosophy and Technology* 25, no. 2: 129–31.

Floridi, Luciano (2014), 'The latent nature of global information warfare', *Philosophy and Technology* 27, no. 3: 317–19.

Folger, Tim (2007), 'Newsflash: Time may not exist', *Discover Magazine*, June, http://discovermagazine.com/2007/jun/in-no-time.

Forsee, Aylesa (1963), *Albert Einstein: Theoretical Physicist* (New York: Macmillan).

Forsyth, James Wood, Jr (2013), 'What great powers make it: International order and the logic of cooperation in cyberspace', *Strategic Studies Quarterly* 7, no. 1: 93–113.

Foucault, Michel (1984), 'What is Enlightenment?', in *The Foucault Reader*, ed. Paul Rabinow (New York: Pantheon Books), 32–50.

Foucault, Michel (1986), 'Of other spaces', *Diacritics* 16, no. 1: 22–7.

Foucault, Michel (2002) [1966], *The Order of Things: An Archaeology of the Human Sciences* (London: Routledge).

Fox, Robin (2001), 'Time out of mind: Anthropological reflections on temporality', *KronoScope* 1, nos. 1–2: 129–37.

Frank, Adam (2011), *About Time* (Oxford: Oneworld).

Fraser, J.T. (1992), 'Human temporality in a nowless universe', *Time and Society* 1, no. 2: 159–73.

Fraser, J.T. (1999), *Time, Conflict, and Human Values* (Urbana, IL: University of Illinois Press).

Fraser, J.T. (2001), 'The extended umwelt principle: Uexküll and the nature of time', *Semiotica* 134, nos. 1–4: 263–73.

Fraser, J.T. (2003), 'Time felt, time understood', *KronoScope* 3, no. 1: 15–26.

Fraser, J.T. (2005), 'Space-time in the study of time: An exercise in critical interdisciplinarity', *KronoScope* 5, no. 2: 151–75.

Freedman, Lawrence (1981), *The Evolution of Nuclear Strategy* (Basingstoke: Macmillan Press).

Friedman, Milton (1961), 'The lag in effect of monetary policy', *Journal of Political Economy* 69, no. 5: 447–66.

Frost and Sullivan (2013), *The 2013 (ISC)^2 Global Information Security Workforce Study* (Mountain View, CA: Frost and Sullivan).

Fulghum, David A. (2010), 'No fingerprints: Culprits in the cyberattack on Iran are still unknown', *Aviation Week and Space Technology* 172, no. 36: 29–30.

Fuller, Steve (2002) [1988], *Social Epistemology*, 2nd edn (Bloomington, IN: Indiana University Press).

Furber, Stephen B. (1989), *VLSI RISC Architecture and Organization* (New York: Marcel Dekker).

Furedi, Frank (2006) [1997], *Culture of Fear Revisited: Risk-Taking and the Morality of Low Expectation*, 4th edn (London: Continuum).

Gable, Kelly A. (2010), 'Cyber-apocalypse now: Securing the internet against cyberterrorism and using universal jurisdiction as a deterrent', *Vanderbilt Journal of Transnational Law* 43: 57–118.

Galison, Peter (2003), *Einstein's Clocks, Poincaré's Maps: Empires of Time* (New York: W.W. Norton & Company).

Galison, Peter and Bruce Hevly, ed. (1992), *Big Science: The Growth of Large-Scale Research* (Stanford University Press).

Gane, Nicholas (2006), 'Speed up or slow down? Social theory in the information age', *Information, Communication and Society* 9, no. 1: 20–38.

Gannon, Charles E. (2009), 'Imag(in)ing tomorrow's wars and weapons', *Peace Review: A Journal of Social Justice* 21, no. 2: 198–208.

Garamone, Jim (2009), 'Lynn calls for collaboration in establishing cyber security', *American Forces Press Service*, 1 October.

Garber, Megan (2013), 'The future of cybersecurity could be sitting in an office in New Jersey', *The Atlantic*, 4 January, www.theatlantic.com/technology/archive/2013/01/the-future-of-cybersecurity-could-be-sitting-in-an-office-in-new-jersey/266849/.

Gardham, Duncan (2009), 'Hackers hired to halt attacks on Britain by cyber terrorists', *The Daily Telegraph*, 26 June.

Garrison, Dee (2006), *Bracing for Armageddon: Why Civil Defense Never Worked* (New York: Oxford University Press).

Gartner (2014), 'Gartner says worldwide information security spending will grow almost 8 percent in 2014 as organizations become more threat-aware', 22 August, www.gartner.com/newsroom/id/2828722.

Geers, Kenneth (2009), ‘The cyber threat to national critical infrastructures: Beyond theory’, *Information Security Journal: A Global Perspective* 18, no. 1: 1–7.

Geers, Kenneth (2010), ‘Live fire exercise: Preparing for cyber war’, *Journal of Homeland Security and Emergency Management* 7, no. 1, article 74.

Gell, Alfred (1992), *The Anthropology of Time: Cultural Constructions of Temporal Maps and Images* (Oxford: Berg).

Gellner, Ernest (1988), *Plough, Sword and Book: The Structure of Human History* (London: Collins Harvill).

Gerovitch, Slava (2008), ‘InterNyet: Why the Soviet Union did not build a nationwide computer network’, *History and Technology* 24, no. 4: 335–50.

Gertz, Bill (1998), ‘Computer hackers could disable military’, *The Washington Times*, 16 April.

Gibbs, Samuel (2014), ‘Eugene Kaspersky: Major cyberterrorist attack is only a matter of time’, *The Guardian*, 1 May, www.theguardian.com/technology/2014/may/01/eugene-kaspersky-major-cyberterrorist-attack-uk.

Gibson, William (1984), *Neuromancer* (London: HarperCollins).

Giddens, Anthony (1984), *The Constitution of Society: Outline of a Theory of Structuration* (Berkeley, CA: University of California Press).

Gill, Stanley (1951), ‘The diagnosis of mistakes in programmes on the EDSAC’, *Proceedings of the Royal Society A* 206, no. 1087: 538–54.

Gjelten, Tom (2011), ‘Stuxnet raises “blowback” risk in cyberwar’, *NPR.org*, 2 November, www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar.

Gjertsen, Derek (1989), *Science and Philosophy: Past and Present* (London: Penguin Books).

Glennie, Paul and Nigel Thrift (2009), *Shaping the Day: A History of Timekeeping in England and Wales 1300–1800* (Oxford University Press).

Glenny, Misha (2011), ‘Virtual warfare in race to avoid “doomsday”’, *The Guardian*, 17 May.

Glenny, Misha and Camino Kavanagh (2012), ‘800 titles but no policy—Thoughts on cyber warfare’, *American Foreign Policy Interests* 34, no. 6: 287–94.

Glezos, Simon (2012), *The Politics of Speed: Capitalism, the State and War in an Accelerating World* (London: Routledge).

Golding, Peter (2000), ‘Forthcoming features: Information and communications technologies and the sociology of the future’, *Sociology* 34, no. 1: 165–84.

Goldman, Alvin I. (1999), *Knowledge in a Social World* (Oxford University Press).

Goldsmith, Jack and Melissa Hathaway (2010), ‘The cybersecurity changes we need’, *Washington Post*, 29 May.

Goodman, Michael S. (2014), *The Official History of the Joint Intelligence Committee*, vol. I: *From the Approach of the Second World War to the Suez Crisis* (Abingdon: Routledge).

Goodman, Seymour E., Jessica C. Kirk and Megan H. Kirk (2007), ‘Cyberspace as a medium for terrorists’, *Technological Forecasting and Social Change* 74, no. 2: 193–210.

Gordon, Uri (2009), ‘Anarchism and the politics of technology’, *WorkingUSA: The Journal of Labor and Society* 12, no. 3: 489–503.

Gould, Stephen Jay (1987), *Time's Arrow, Time's Cycle: Myth and Metaphor in the Discovery of Geological Time* (Cambridge, MA: Harvard University Press).

Government Office for Science (2011), *Blackett Review of High Impact Low Probability Risks* (London: Department of Business, Innovation and Skills).

Graham, Bradley (1998), 'US studies new threat: Cyber attack', *The Washington Post*, 24 May.

Graham, Philip (2001), 'Space: Irrealis objects in technology policy and their role in a new political economy', *Discourse and Society* 12, no. 6: 761–88.

Graham, Stephen and Simon Marvin (2001), *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition* (London: Routledge).

Graham, Stephen and Nigel Thrift (2007), 'Out of order: Understanding repair and maintenance', *Theory, Culture and Society* 24, no. 3: 1–25.

Gramsci, Antonio (1973) [1929], *Letters from Prison* (New York: Harper Row).

Gray, John (2007), *Black Mass: Apocalyptic Religion and the Death of Utopia* (London: Allen Lane).

Gray, John (2012), 'The violent visions of Slavoj Žižek', *New York Review of Books*, 12 July, www.nybooks.com/articles/archives/2012/jul/12/violent-visions-slavoj-zizek/.

Gray, John (2013), 'Ignore at our peril', *The Guardian*, 2 February.

Greenberg, Stanley (1998), *Invisible New York: The Hidden Infrastructure of the City* (Baltimore, MD: Johns Hopkins University Press).

Greene, Brian (1999), *The Elegant Universe: Superstrings, Hidden Dimensions, and the Quest for the Ultimate Theory* (London: Jonathan Cape).

Greenwald, Glenn (2013), 'Pentagon's new massive expansion of "cyber-security" unit is about everything except defense', *The Guardian*, 28 January, www.guardian.co.uk/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet.

Gregory, Donna U. (1989), 'The dictator's furnace', *Peace Review: A Journal of Social Justice* 1, no. 1: 12–6.

Grier, David Alan (2005), *When Computers Were Human* (Princeton University Press).

Gross, Michael Joseph (2011), 'A declaration of cyber-war', *Vanity Fair*, April, www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

Grubesic, Tony H. and Alan T. Murray (2006), 'Vital nodes, interconnected infrastructures, and the geographies of network survivability', *Annals of the Association of American Geographers* 96, no. 1: 64–84.

Grusin, Richard (2010a), *Premediation: Affect and Mediality After 9/11* (Basingstoke: Palgrave Macmillan).

Grusin, Richard (2010b), 'Cyber Shock Wave—Fearmongering on CNN', *Premediation*, 25 February, http://premediation.blogspot.co.uk/2010/02/cyber-shock-wave-fearmongering-on-cnn.html.

Grzymala-Busse, Anna (2011), 'Time will tell? Temporality and the analysis of causal mechanisms and processes', *Comparative Political Studies* 44, no. 9: 1267–97.

Guernsey, Daniel, Mason Rice and Sujeet Shenoi (2012), ‘Implementing novel reactive defense functionality in MPLS networks using hyperspeed signalling’, *International Journal of Critical Infrastructure Protection* 5, no. 1: 40–52.

Guitton, Clement (2013), ‘Cyber insecurity as a national threat: Overreaction from Germany, France and the UK?’, *European Security* 22, no. 1: 21–35.

Gusterson, Hugh (1999), ‘Missing the end of the Cold War in international security’, in *Cultures of Insecurity: States, Communities, and the Production of Danger*, ed. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall (Minneapolis, MN: University of Minnesota Press), 319–45.

Guthrie, W.K.C. (1978), *A History of Greek Philosophy*, vol. V: *The Later Plato and the Academy* (Cambridge University Press).

Guzzini, Stefano (2000), ‘A reconstruction of constructivism in International Relations’, *European Journal of International Relations* 6, no. 2: 147–82.

Haas, Peter M. (1989), ‘Do regimes matter? Epistemic communities and Mediterranean pollution control’, *International Organization* 43, no. 3: 377–403.

Haas, Peter M. (1992), ‘Introduction: Epistemic communities and international policy coordination’, *International Organization* 46, no. 1: 1–35.

Hacking, Ian (1999), *The Social Construction of What?* (Cambridge, MA: Harvard University Press).

Haimes, Yacov Y., Kenneth Crowther and Barry M. Horowitz (2008), ‘Homeland security preparedness: Balancing protection with resilience in emergent systems’, *Systems Engineering* 11, no. 4: 287–308.

Halbert, Debora (1997), ‘Discourses of danger and the computer hacker’, *The Information Society* 13, no. 4: 361–74.

Hall, Wayne M. (2003), *Stray Voltage: War in the Information Age* (Annapolis, MD: Naval Institute Press).

Hansen, Lene and Helen Nissenbaum (2009), ‘Digital disaster, cyber security, and the Copenhagen School’, *International Studies Quarterly* 53, no. 4: 1155–75.

Haraway, Donna (1991), ‘A cyborg manifesto: Science, technology, and socialist-feminism in the late twentieth century’, *Simians, Cyborgs and Women: The Reinvention of Nature* (New York: Routledge), 149–81.

Haraway, Donna (1997), *Modest Witness@Second_Millennium: Female_Man©_Meets Oncomouse*^{TM}*: Feminism and Technoscience* (New York: Routledge).

Harknett, Richard J. (2011), ‘Thinking about how to think about cybersecurity’, *15th Karlsruhe Dialogues: Caught In the Net? Global Google-Cultures*, Karlsruhe Institute of Technology, Karlsruhe, Germany, 11–13 February.

Harknett, Richard A. and James A. Stever (2009), ‘The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen’, *Journal of Homeland Security and Emergency Management* 6, no. 1, DOI:10.2202/1547-7355.1649.

Harknett, Richard A. and James A. Stever (2011), ‘The new policy world of cybersecurity’, *Public Administration Review* 71, no. 3: 455–60.

Harman, Graham (2010a), ‘I am also of the opinion that materialism must be destroyed’, *Environment and Planning D: Society and Space* 28, no. 5: 772–90.

Harman, Graham (2010b), ‘Technology, objects and things in Heidegger’, *Cambridge Journal of Economics* 34, no. 1: 17–25.

Harris, Jose (1993), *Private Lives, Public Spirit: Britain 1870–1914* (London: Penguin Books).

Harris, Paul (2011), ‘Living with 9/11: The anti-terror chief’, *The Guardian*, 6 September.

Hartnett, Stephen John (2011), ‘Google and the “twisted cyber spy” affair: US-Chinese communication in an age of globalization’, *Quarterly Journal of Speech* 97, no. 4: 411–34.

Harvey, David (1990), *The Condition of Postmodernity: An Enquiry Into the Origins of Cultural Change* (Cambridge, MA: Blackwell).

Hassan, Robert (2007), ‘Network time’, in Hassan and Purser (ed.), 37–61.

Hassan, Robert (2009), *Empires of Speed: Time and the Acceleration of Politics and Society* (Leiden: Brill).

Hassan, Robert (2010), ‘Globalization and the “temporal turn”: Recent trends and issues in time studies’, *The Korean Journal of Policy Studies* 25, no. 2: 83–102.

Hassan, Robert and Ronald E. Purser, ed. (2007), *24/7: Time and Temporality in the Network Society* (Stanford, CA: Stanford Business Books).

Hayden, Michael V. (2011), speech, Aspen Security Forum, Aspen, CO, 29 July, www.youtube.com/watch?v=yoWkAVXmSs0.

Healey, Jason (2011), *The Five Futures of Cyber Conflict and Cooperation* (Washington, DC: Atlantic Council).

Healey, Jason (2012), ‘Hazard, outrage and Panetta’s cyber speech’, *New Atlanticist*, 23 October, www.atlanticcouncil.org/blogs/new-atlanticist/hazard-outrage-and-panettas-cyber-speech.

Healey, Jason, ed. (2013), *A Fierce Domain: Conflict in Cyberspace, 1986–2012* (Washington, DC: Atlantic Council).

Heidegger, Martin (1995) [1929–1930], *The Fundamental Concepts of Metaphysics: World, Finitude, Solitude*, trs. William McNeill and Nicholas Walker (Bloomington, IN: Indiana University Press).

Heidegger, Martin (2010) [1927], *Being and Time*, rev. edn, tr. Joan Stambaugh (Albany, NY: State University of New York Press).

Heim, Michael (1993), *The Metaphysics of Virtual Reality* (New York: Oxford University Press).

Hellström, Tomas (2003), ‘Systemic innovation and risk: Technology assessment and the challenge of responsible innovation’, *Technology in Society* 25, no. 3: 369–84.

Hellström, Tomas (2007), ‘Critical infrastructure and systemic vulnerability: Towards a planning framework’, *Safety Science* 45, no. 3: 415–30.

Helm, Bertrand P. (2001), ‘Review: J.T. Fraser, Time, Conflict, and Human Values’, *The Journal of Speculative Philosophy* 15, no. 1: 50–6.

Heywood, Andrew (2000), *Key Concepts in Politics* (Basingstoke: Palgrave Macmillan).

Highland, Harold Joseph (1983), ‘Impact of microcomputers on total computer security’, *Computers and Security* 2, no. 2: 171–83.

Hildreth, Steven A. (2001), *Cyberwarfare* (Washington, DC: Congressional Research Service).

Hindess, Barry (2007), ‘The past is another culture’, *International Political Sociology* 1, no. 4: 325–38.

HM Government (1955), *Annual Report of the Chief of Inspector of Factories for the Year 1954* (London: HMSO).

HM Government (2000), *A New Future for Communications* (London: HMSO).

HM Government (2009a), *Digital Britain: Final Report* (Norwich: The Stationery Office).

HM Government (2009b), *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (Norwich: The Stationery Office).

HM Government (2010a), *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Norwich: The Stationery Office).

HM Government (2010b), *Britain’s Superfast Broadband Future* (London: Department for Business, Innovation and Skills).

HM Government (2013), *The Coalition: Together in the National Interest* (London: Cabinet Office).

HM Government (2014a), *Cyber Security Skills: Business Perspectives and Government’s Next Steps* (London: Department for Business, Innovation and Skills).

HM Government (2014b), *Developing Our Capability in Cyber Security: Academic Centres of Excellence in Cyber Security Research* (London: Department for Business, Innovation and Skills).

Hobbes, Thomas (1996) [1651], *Leviathan*, ed. Richard Tuck, rev. edn (Cambridge University Press).

Hobbes, Thomas (1998) [1642], *On the Citizen*, ed. Richard Tuck and Michael Silverthorne (Cambridge University Press).

Hobsbawm, Eric (2013), ‘The American cowboy: An international myth?’, *Fractured Times: Culture and Society in the 20th Century* (London: Little, Brown), 272–89.

Hobson, John and George Lawson (2008), ‘What is history in International Relations?’, *Millennium: Journal of International Studies* 37, no. 2: 415–35.

Hodder, Ian (2012), *Entangled: An Archaeology of the Relationships between Humans and Things* (Chichester: Wiley-Blackwell).

Hoekstra, Peter and Brian Finch (2013), ‘The looming certainty of a cyber Pearl Harbor’, *Politico*, 19 February, www.politico.com/story/2013/02/the-looming-certainty-of-a-cyber-pearl-harbor-87806.html.

Holquist, Michael (2010), ‘The fugue of chronotope’, in *Bakhtin’s Theory of the Literary Chronotope: Reflections, Applications, Perspectives*, ed. Nele Bemong, Pieter Borghart, Michel de Dobbeleer, Kristoffel Demoen, Koen de Temmerman and Bart Keunen (Ghent: Ginkgo Academia Press), 19–33.

Holt, Thomas J. (2007), ‘Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures’, *Deviant Behavior* 28, no. 2: 171–98.

Hom, Andrew R. (2010), ‘Hegemonic metronome: The ascendancy of Western standard time’, *Review of International Studies* 36, no. 4: 1145–70.

Hom, Andrew R. and Brent J. Steele (2010), ‘Open horizons: The temporal visions of reflexive realism’, *International Studies Review* 12, no. 2: 271–300.

Home Office (2010), *Cyber Crime Strategy* (Norwich: The Stationery Office).

Hoofd, Ingrid M. (2012), *Ambiguities of Activism: Alter-Globalism and the Imperatives of Speed* (New York: Routledge).

Hook, Glenn D (1984), 'The nuclearization of language: Nuclear allergy as political metaphor', *Journal of Peace Research* 21, no. 3: 259–75.

Hopf, Ted (1998), 'The promise of constructivism in International Relations theory', *International Security* 23, no. 1: 171–200.

Hopkins, Nick (2012), 'Militarisation of cyberspace: Why the West fears the threat from China's "cyber jedis"', *The Guardian*, 17 April.

Hopkins, Nick (2013), '"Cyber jedi" schools contest a new hope for Britain's IT empire to strike back', *The Guardian*, 28 April, www.guardian.co.uk/technology/2013/apr/28/cyber-jedi-contest-britain-empire.

Hosein, Ian (2004), 'The sources of laws: Policy dynamics in a digital and terrorized world', *The Information Society: An International Journal* 20, no. 3: 187–99.

Hoskins, Andrew (2006), 'Temporality, proximity and security: Terror in a media-drenched age', *International Relations* 20, no. 4: 453–66.

Hoskins, Andrew (2011), 'Media, memory, metaphor: Remembering and the connective turn', *Parallax* 17, no. 4: 19–31.

Hoskins, Andrew and Ben O'Loughlin (2010), *War and Media: The Emergence of Diffused War* (Cambridge: Polity).

House of Commons Committee of Public Accounts (2011), *Information and Communications Technology in Government: Report, Together with Formal Minutes, Oral and Written Evidence* (London: The Stationery Office).

House of Commons (1984), *Minutes of Evidence*, Select Committee on House of Commons (Services), Computer Sub-Committee, 24 January 1984.

House of Commons Defence Committee (2013), *Defence and Cyber-Security*, vol. I (London: The Stationery Office).

House of Lords (2010) [1862], *Companion to the Standing Orders of and Guide to the Proceedings of the House of Lords*, 22nd edn (Norwich: The Stationery Office).

House of Lords Select Committee on Science and Technology (2012), *Higher Education in Science, Technology, Engineering and Mathematics (STEM) Subjects: Report* (London: The Stationery Office).

Hughes, James J. (2012), 'The politics of transhumanism and the techno-millennial imagination, 1626-2030', *Zygon: Journal of Religion and Science* 47, no. 4: 757–76.

Hughes, Michael and Harry Wood (2014), 'Crimson nightmares: Tales of invasion and fears of revolution in early twentieth-century Britain', *Contemporary British History* 28, no. 3: 294–317.

Hughes, Rex (2010), 'A treaty for cyberspace', *International Affairs* 86, no. 2: 523–41.

Hundley, Richard O. and Robert H. Anderson (1995), 'Emerging challenge: Security and safety in cyberspace', *IEEE Technology and Society* 14, no. 4: 19–28.

Hunt, Edward (2012), 'US government penetration programs and the implications for cyberwar', *IEEE Annals of the History of Computing* 34, no. 3: 4–21.

Huntington, Samuel P. (1968), *Political Order in Changing Societies* (New Haven, CT: Yale University Press).

Husserl, Edmund (1964) [1928], *The Phenomenology of Internal Time-Consciousness*, ed. Martin Heidegger, tr. James S. Churchill (The Hague: Martinus Nijhoff).

Hutchings, Kimberly (2007), 'Happy anniversary! Time and critique in International Relations theory', *Review of International Studies* 33, supplement S1: 71–89.

Hutchings, Kimberly (2008), *Time and World Politics: Thinking the Present* (Manchester University Press).

Huysmans, Jef (1996), 'Security! What do you mean? From concept to thick signifier', *European Journal of International Relations* 4, no. 2: 226–55.

Huysmans, Jef (1997), 'James Der Derian: The unbearable lightness of theory', in *The Future of International Relations: Masters in the Making?*, ed. Iver B. Neumann and Ole Wæver (London: Routledge), 361–83.

Huyssen, Andreas (2003), *Present Pasts: Urban Palimpsests and the Politics of Memory* (Stanford University Press).

Hynek, Nik and David Chandler (2013), 'No emancipatory alternative, no critical security studies', *Critical Studies on Security* 1, no. 1: 46–63.

Information Assurance Advisory Council (2012), *Record of a Joint IAAC/Cabinet Office Seminar—UK Cyber Security Strategy* (Swindon: IAAC).

InfoSecurity (2013), 'RSA 2013: As cybersecurity receives more attention, DHS becomes a critical player', 26 February, www.infosecurity-magazine.com/view/30907/rsa-2013-as-cybersecurity-receives-more-attention-dhs-becomes-a-critical-player/.

Innes, Michael, ed. (2007), *Denial of Sanctuary: Understanding Terrorist Safe Havens* (Westport, CT: Praeger Security International).

Institute of Engineering and Technology (2011), *Delivering London 2012: ICT Enabling the Games* (Stevenage: The IET).

Institute of Engineering and Technology (2013), *Delivering London 2012: ICT Implementation and Operations* (Stevenage: The IET).

Intelligence and Security Committee (2012), *Annual Report 2011–2012* (Norwich: The Stationery Office).

Jabri, Vivienne (2006), 'War, security and the liberal state', *Security Dialogue* 37, no. 1: 47–64.

Jackson, Patrick Thaddeus (2011), *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics* (London: Routledge).

Jackson, Richard (2005), *Writing the War on Terrorism: Language, Politics and Counter-Terrorism* (Manchester University Press).

Jagoda, Patrick (2012), 'Speculative security', in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press), 21–35.

Jarvis, Lee (2009), *Times of Terror: Discourse, Temporality and the War on Terror* (Basingstoke: Palgrave Macmillan).

Jeffery, Keith (2010), *MI6: The History of the Secret Intelligence Service* (London: Bloomsbury Publishing).

Jessop, Bob (2009), 'The spatiotemporal dynamics of globalizing capital and their impact on state power and democracy', in Rosa and Scheuerman (ed.), 135–58.

Johnson, Boris (2011), ‘It will take a super-sewer to get London out of this mess’, *Daily Telegraph*, 12 September.

Johnson, Ed (2002), ‘“Cowboy” Blair raises eyebrows’, *Associated Press*, 4 September.

Jordan, Glenn (1995), ‘Flight from modernity: Time, the Other and the discourse of primitivism’, *Time and Society* 4, no. 3: 281–303.

Jungk, Robert (1958), *Brighter Than a Thousand Suns: The Moral and Political History of the Atomic Scientists*, tr. James Cleugh (London: Victor Gollancz).

Kaczynski, Theodore (1995), *Industrial Society and Its Future*.

Kaika, Maria and Erik Swyngedouw (2000), ‘Fetishizing the modern city: The phantasmagoria of urban technological networks’, *International Journal of Urban and Regional Research* 24, no. 1: 120–38.

Kaiser, Robert (2015), ‘The birth of cyberwar’, *Political Geography* 46: 11–20.

Kaldor, Mary (2006) [1999], *New and Old Wars: Organized Violence in a Global Era*, 2nd edn (Cambridge: Polity Press).

Kaminski, Ryan T. (2010), ‘Escaping the cyber state of nature: Cyber deterrence and international institutions’, in *Conference on Cyber Conflict Proceedings 2010*, ed. Christian Czosseck and Karlis Podins (Tallinn: CCD COE Publications), 79–94.

Kamp, Poul-Henning (2011), ‘The one-second war’, *Communications of the ACM* 54, no. 5: 44–88.

Kane, Margaret (2002), ‘US vulnerable to data sneak attack’, *CNet News*, 13 August, http://news.cnet.com/2100-1017-949605.html.

Kant, Immanuel (1998) [1781/1787], *Critique of Pure Reason* (Cambridge University Press).

Karatzogianni, Athina (2006), *The Politics of Cyberconflict* (Abingdon: Routledge).

Kaspersky, Eugene (2012), ‘Cassandra complex … not for much longer’, *Nota Bene*, 17 March, http://eugene.kaspersky.com/2012/03/17/cassandra-complex-not-for-much-longer-2/.

Kaveney, Roz (2013), ‘The meaning of meteors’, *The Guardian*, 15 February, www.guardian.co.uk/commentisfree/2013/feb/15/meaning-of-meteors.

Keane, John (2012), ‘Silence and catastrophe: New reasons why politics matters in the early years of the twenty-first century’, *The Political Quarterly* 83, no. 4: 660–8.

Keep, Christopher (1995), ‘An absolute acceleration: Apocalypticism and the war machines of Waco’, in *Postmodern Apocalypse: Theory and Cultural Practice at the End*, ed. Richard Dellamora (Philadelphia, PA: University of Pennsylvania Press), 262–74.

Kelly, Kevin (2010), *What Technology Wants* (New York: Viking).

Kern, Stephen (1983), *The Culture of Time and Space 1880–1918* (Cambridge, MA: Harvard University Press).

Kesan, Jay P. and Carol M. Hayes (2010), ‘Thinking through active defense in cyberspace’, *Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options*, 10–11 June 2010 (Washington, DC: National Academies Press), 327–42.

Khong, Yuen Foong (1992), *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton University Press).

Kiggins, Ryan David (2015), 'Open for expansion: US policy and the purpose for the internet in the post-Cold War era', *International Studies Perspectives* 16, no. 1: 86–105.

Kilcullen, David (2005), 'Countering global insurgency', *Journal of Strategic Studies* 28, no. 4: 597–617.

Kincanon, Eric (2004), 'Misuses of physical models in understanding time', *KronoScope* 4, no. 1: 70–3.

King, Martin Luther, Jr (1993), 'Letter from Birmingham Jail', *University of California Davis Law Review* 26, no. 4: 835–51.

King, Vera (2010), 'The generational rivalry for time', *Time and Society* 19, no. 1: 54–71.

Kitzinger, Jenny (2000), 'Media templates: Patterns of association and the (re)construction of meaning over time', *Media, Culture and Society* 22, no. 1: 61–84.

Klaver, J.M.I. (1997), *Geology and Religious Sentiment: The Effect of Geological Discoveries on English Society and Literature Between 1829 and 1859* (Leiden: Brill).

Kleinrock, Leonard (2003), 'An internet vision: The invisible global infrastructure', *Ad Hoc Networks* 1, no. 1: 3–11.

Klimburg, Alexander (2010), 'The whole of nation in cyberpower', *Georgetown Journal of International Affairs* 11: 171–9.

Klimburg, Alexander (2011), 'Mobilising cyber power', *Survival* 53, no. 1: 41–60.

Klimburg, Alexander (2013), 'The Internet Yalta', 5 February, Center for a New American Security, http://www.cnas.org/files/documents/publications/CNAS_WCIT_commentary.pdf.

Kline, Ronald R. (2006), 'Cybernetics, management science, and technology policy: The emergence of "information technology" as a keyword, 1948–1985', *Technology and Culture* 47, no. 3: 513–35.

Klinke, Ian (2013), 'Chronopolitics: A conceptual matrix', *Progress in Human Geography* 37, no. 5: 673–90.

Knabb, Richard D., Jamie R. Rhome and Daniel P. Brown (2011), 'Tropical Cyclone Report: Hurricane Katrina', National Hurricane Center, 20 December 2005, updated 14 September 2011, www.nhc.noaa.gov/pdf/TCR-AL122005_Katrina.pdf.

Kohl, Philip L. and Clare Fawcett (1995), 'Archaeology in the service of the state: Theoretical considerations', in *Nationalism, Politics, and the Practice of Archaeology*, ed. Philip L. Kohl and Clare Fawcett (Cambridge University Press), 3–18.

Koselleck, Reinhart (2004) [1979], *Futures Past: On the Semantics of Historical Time*, tr. Keith Tribe (New York: Columbia University Press).

Kragh, Helge S. (2007), *Conceptions of the Cosmos—From Myths to the Accelerating Universe: A History of Cosmology* (Oxford University Press).

Krahmann, Elke (2008), 'Security: Collective good or commodity?', *European Journal of International Relations* 14, no. 3: 379–404.

Kundera, Milan (1997), *Slowness: A Novel*, tr. Linda Asher (New York: HarperCollins).

Kütting, Gabriela (2001), 'Back to the future: Time, the environment and IR theory', *Global Society* 15, no. 4: 345–60.

Lakoff, George and Mark Johnson (1980), *Metaphors We Live By* (University of Chicago Press).

Landes, Richard (1998), *Whilst God Tarried: Disappointed Millennialism and the Genealogy of the Modern West* (New York: Basic Books).

Landy, Marcia (2004), '"America under attack": Pearl Harbor, 9/11, and history in the media', in *Film and Television After 9/11*, ed. Wheeler W. Dixon (Carbondale, IL: Southern Illinois University Press), 79–100.

Latham, Robert (2003), 'Introduction', in *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security*, ed. Robert Latham (New York: The New Press), 1–21.

Latour, Bruno (1988), *The Pasteurization of France*, trs. Alan Sheridan and John Law (Cambridge, MA: Harvard University Press).

Latour, Bruno (1990), 'Drawing things together', in *Representation in Scientific Practice*, ed. Michael Lynch and Steve Woolgar (Cambridge, MA: MIT Press), 19–68.

Latour, Bruno (1992), 'Where are the missing masses? The sociology of a few mundane artifacts', in *Shaping Technology / Building Society: Studies in Sociotechnical Change*, ed. Wiebe E. Bijker and John Law (Cambridge, MA: MIT Press), 225–58.

Latour, Bruno (1993) [1991], *We Have Never Been Modern*, tr. Catherine Porter (Cambridge, MA: Harvard University Press).

Latour, Bruno (2002), 'Morality and technology: The end of the means', *Theory, Culture and Society* 19, nos. 5–6: 247–60.

Latour, Bruno (2005), *Reassembling the Social: An Introduction to Actor-Network Theory* (Oxford University Press).

Law, John (2004), *After Method: Mess in Social Science Research* (London: Routledge).

Lawson, George (2012), 'The eternal divide? History and International Relations', *European Journal of International Relations* 18, no. 2: 203–26.

Lawson, Sean (2011), 'Articulation, antagonism, and intercalation in Western military imaginaries', *Security Dialogue* 42, no. 1: 39–56.

Lawson, Sean (2012a), 'Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States', *First Monday* 17, no. 7, http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.

Lawson, Sean (2012b), 'DHS Secretary Napolitano uses Hurricane Sandy to hype cyber threat', *Forbes*, 1 November, www.forbes.com/sites/seanlawson/2012/11/01/dhs-secretary-napolitano-uses-hurricane-sandy-to-hype-cyber-threat/.

Lawson, Sean (2013a), 'Motivating cybersecurity: Assessing the status of critical infrastructure as an object of cyber threats', in *Securing Critical Infrastructures and Industrial Control Systems: Approaches for Threat Protection*, ed. Christopher Laing, Atta Badii and Paul Vickers (Hershey, PA: IGI Global), 168–88.

Lawson, Sean (2013b), 'Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats', *Journal of Information Technology and Politics* 10, no. 1: 86–103.

Lawson, Sean and Robert W. Gehl (2011), 'Convergence security: Cyber-surveillance and the biopolitical production of security', paper presented at Cyber-Surveillance in Everyday Life: An International Workshop, Toronto, 13–15 May.

Leccardi, Carmen (2007), 'New temporal perspectives in the "high-speed society"', in Hassan, Robert and Ronald E. Purser, ed. (2007), 24/7: Time and Temporality in the Network Society (Stanford, CA: Stanford Business Books), 25–36.

Lee, Heejin and Jonathan Liebenau (2000), 'Time and the internet at the turn of millennium', *Time and Society* 9, no. 1: 43–56.

Lee, Raymond L.M. (2012), 'Global modernity and temporal multiplicity', *KronoScope* 12, no. 1: 31–51.

Leong, Susan, Teodor Mitew, Marta Celletti and Erika Pearson (2009), 'The question concerning (internet) time', *New Media and Society* 11, no. 8: 1267–85.

Levin, Adam (2012), 'How the SEC almost shut down Wall Street' *Huffington Post*, 15 November, www.huffingtonpost.com/adam-levin/did-you-know-the-sec-almo_b_2133962.html.

Lewis, James A. (2003), 'Cyber terror: Missing in action', *Knowledge, Technology and Policy* 16, no. 2: 34–41.

Lewis, James A. (2005), 'Aux armes, citoyens: Cyber security and regulation in the United States', *Telecommunications Policy* 29, no. 11: 821–30.

Lewis, James A. (2010), 'Sovereignty and the role of government in cyberspace', *Brown Journal of World Affairs* 16, no. 2: 55–65.

Lewis, Jeff (2012), *Global Media Apocalypse: Pleasure, Violence and the Cultural Imaginings of Doom* (Basingstoke: Palgrave Macmillan).

Libicki, Martin C. (1997), *Defending Cyberspace and Other Metaphors* (Honolulu, HI: University Press of the Pacific).

Libicki, Martin C. (2007), *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press).

Libicki, Martin C. (2009), *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation).

Libicki, Martin C. (2011), 'The strategic uses of ambiguity in cyberspace', *Military and Strategic Affairs* 3, no. 3: 3–10.

Libicki, Martin C., David Senty and Julia Pollak (2014), *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND Corporation).

Lieberman, Joseph I. and Susan Collins (2012), 'At dawn we sleep', *The New York Times*, 7 December.

Liff, Adam P. (2012), 'Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war', *Journal of Strategic Studies* 35, no. 3: 401–28.

Lindsay, Jon R. (2013), 'Stuxnet and the limits of cyber warfare', *Security Studies* 22, no. 3: 365–404.

Little, Morgan (2012), 'Executive Order on cyber security builds steam amid criticisms', *Los Angeles Times*, 2 October, http://articles.latimes.com/2012/oct/02/news/la-pn-obama-executive-order-cyber-security-20121002.

Little, Richard G. (2002), 'Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures', *Journal of Urban Technology* 9, no. 1: 109–23.

Lockheed Martin (2012), 'National cyber range', presentation, www.ndia.org/Resources/OnlineProceedings/Documents/21M0/MODSIM/03-Defense-Pridmore.pdf.

Lucas, Gavin (2005), *The Archaeology of Time* (London: Routledge).

Lule, Jack (1991), 'Roots of the space race: Sputnik and the language of US news in 1957', *Journalism and Mass Communication Quarterly* 68, nos. 1–2: 76–86.

Lundborg, Tom (2012), *Politics of the Event: Time, Movement, Becoming* (London: Routledge).

Lunenfeld, Peter (1996), 'Theorizing in real time: Hyperaesthetics for the technoculture', *Afterimage* 23, no. 4: 16–18.

Lynn, William J., III (2010), 'Defending a new domain: The Pentagon's cyberstrategy', *Foreign Affairs* 89, no. 5: 97–108.

Lyotard, Jean-François (1987), 'The sign of history', in *Post-Structuralism and the Question of History*, ed. Derek Attridge, Geoff Bennington and Robert Young (Cambridge University Press), 162–80.

McCaney, Kevin (2014), 'Intelligence agency has a cold plan for faster, cheaper supercomputing', *Defense Systems*, 4 December, http://defensesystems.com/articles/2014/12/04/iarpa-cryogenic-exascale-supercomputing.aspx.

McCarthy, Daniel (2013), 'Technology and "the international" or: How I learned to stop worrying and love determinism', *Millennium: Journal of International Studies* 41, no. 3: 470–90.

McConnell, Mike (2010), 'To win the cyber-war, look to the Cold War', *The Washington Post*, 28 February.

McFarlane, Colin and Ben Anderson (2011), 'Thinking with assemblage', *Area* 43, no. 2: 162–4.

McGinn, Bernard (1998) [1979], *Visions of the End: Apocalyptic Traditions in the Middle Ages* (New York: Columbia University Press).

McIvor, David (2011), 'The politics of speed: Connolly, Wolin, and the prospects for democratic citizenship in an accelerated polity', *Polity* 43, no. 1: 58–83.

Mackenzie, Adrian (2002), *Transductions: Bodies and Machines at Speed* (London: Continuum).

MacKenzie, Donald (1996), 'Nuclear weapons laboratories and the development of supercomputing', *Knowing Machines: Essays on Technical Change* (Cambridge, MA: MIT Press), 99–129.

MacKenzie, Donald and Garrel Pottinger (1997), 'Mathematics, technology, and trust: Formal verification, computer security, and the US military', *IEEE Annals of the History of Computing* 19, no. 3: 41–59.

Mackinlay, John (2009), *The Insurgent Archipelago: From Mao to Bin Laden* (London: Hurst and Company).

McLaren, Peter (2002), 'George Bush, apocalypse sometime soon, and the American imperium', *Cultural Studies—Critical Methodologies* 2, no. 3: 327–33.

McLuhan, Marshall (2002) [1951], *The Mechanical Bride: Folklore of Industrial Man* (Corte Madera, CA: Ginkgo Press).

McLuhan, Marshall (2006) [2001], 'The medium is the message', in *Media and Cultural Studies: KeyWorks*, rev. edn, ed. Meenakshi Gigi Durham and Douglas M. Kellner (Malden, MA: Blackwell Publishing), 107–16.

McLure, Helen (2000), 'The wild, wild web: The mythic American West and the electronic frontier', *The Western Historical Quarterly* 31, no. 4: 457–76.

McManners, John (1981), *Death and the Enlightenment: Changing Attitudes to Death Among Christians and Unbelievers in Eighteenth-Century France* (Oxford University Press).

McPherson, James L. and S.N. Alexander (1951), 'Performance of the census UNIVAC system', *Proceedings of the AIEE-ERE Conference*, 10–12 December 1951, 16–22.

McSorley, Kevin (2012), 'Helmetcams, militarized sensation and "somatic war"', *Journal of War and Culture Studies* 5, no. 1: 47–58.

McTaggart, J.M.E. (1908), 'The unreality of time', *Mind: A Quarterly Review of Psychology and Philosophy* 17, no. 4: 457–74.

Magaziner, Ira (1998), 'Democracy and cyberspace: First principles', *Democracy and Digital Media Conference*, Cambridge, MA, 8 May.

Magee, Clifford S. (2013), 'Awaiting cyber 9/11', *Joint Force Quarterly* 70: 76–82.

Maier, Charles S. (1987), 'The politics of time: Changing paradigms of collective time and private time in the modern era', in *Changing Boundaries of the Political: Essays on the Evolving Balance Between the State and Society, Public and Private in Europe*, ed. Charles S. Meier (Cambridge University Press), 151–75.

Malphurs, Ryan (2008), 'The media's frontier construction of President George W. Bush', *The Journal of American Culture* 31, no. 2: 185–201.

Mandiant (2014), *Trends 2014: Beyond the Breach* (Alexandria, VA: Mandiant).

Marcus, Jonathan (2013), 'Are we really facing cyberwar?', *BBC News*, 5 March, www.bbc.co.uk/news/technology-21653361.

Marinetti, Filippo Tommaso (1973), 'The founding and manifesto of Futurism', in *Futurist Manifestos*, ed. Umbro Apollonio (New York: Viking Press), 19–24, originally published in *Gazzetta dell'Emilia*, 5 February 1909.

Markoff, John (2005), 'A new arms race to build the world's mightiest computer', *The New York Times*, 19 August.

Marshall, Rosalie (2013), 'Ofsted, Microsoft and teachers voice concerns with draft DfE computing curriculum', *V3.co.uk*, 1 March, www.v3.co.uk/v3-uk/news/2251555/ofsted-microsoft-and-teachers-worried-dfe-computing-curriculum-not-up-to-scratch.

Martin, Lauren and Stephanie Simon (2008), 'A formula for disaster: The Department of Homeland Security's virtual ontology', *Space and Polity* 12, no. 3: 281–96.

Martin, Thomas (2014), 'Governing an unknowable future: The politics of Britain's Prevent policy', *Critical Studies on Terrorism* 7, no. 1: 62–78.

Marwick, Alice (2008), 'To catch a predator? The MySpace moral panic', *First Monday* 13, no. 6, n.p., http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2152/1966.

Masco, Joseph (2004), 'Nuclear technoaesthetics: Sensory politics from Trinity to the virtual bomb in Los Alamos', *American Ethnologist* 31, no. 3: 349–73.

Masco, Joseph (2008), '"Survival is your business": Engineering ruins and affect in nuclear America', *Cultural Anthropology* 23, no. 2: 361–98.

Massey, Doreen (1992), 'Politics and space/time', *New Left Review* 196: 65–84.

May, Jon and Nigel Thrift (2001), 'Introduction', in *Timespace: Geographies of Temporality*, ed. Jon May and Nigel Thrift (London: Routledge), 1–46.

May, Peter J., Chris Koski and Nicholas Stramp (2014), 'Issue expertise in policymaking', *Journal of Public Policy*, DOI:10.1017/S0143814X14000233.

Mayer, Kenneth R. (2001), *With the Stroke of a Pen: Executive Orders and Presidential Power* (Princeton University Press).

Mellor, D.H. (1993), 'The unreality of tense', in *The Philosophy of Time*, ed. Robin Le Poidevin and Murray MacBeath (Oxford University Press), 47–59.

Merk, Frederick (1995) [1963], *Manifest Destiny and Mission in American History* (Cambridge, MA: Harvard University Press).

Meserve, Jeanne (2007), 'Sources: Staged cyber attack reveals vulnerability in power grid', *CNN.com*, 26 September, http://edition.cnn.com/2007/US/09/26/power.at.risk/.

Miller, Donald F. (1993), 'Political time: The problem of timing and chance', *Time and Society* 2, no. 2: 179–87.

Mills, David L. (2006), *Computer Network Time Synchronization: The Network Time Protocol* (Boca Raton, FL: CRC Press).

Ministry of Defence (2010), *Global Strategic Trends: Out to 2040*, 4th edn, Development, Concepts and Doctrine Centre Strategic Trends Programme.

Minkowski, Hermann (2010), 'Space and time', in *Minkowski Spacetime: A Hundred Years Later*, ed. Vesselin Petkov (New York: Springer), xiv–xli.

Mitchell, William J. (1995), *City of Bits: Space, Place and the Infobahn* (Cambridge, MA: MIT Press).

Mitnick, Kevin D. and William L. Simon (2011), *Ghost in the Wire: My Adventures as the World's Most Wanted Hacker* (New York: Little, Brown and Company).

Mitzen, Jennifer (2006), 'Ontological security in world politics', *European Journal of International Relations* 12, no. 3: 341–70.

Molfino, Emily (2012), 'Viewpoint: Cyberterrorism: Cyber "Pearl Harbor" is imminent', in *Cyberspaces and Global Affairs*, ed. Sean S. Costigan and Jake Perry (Farnham: Ashgate Publishing), 75–82.

Moltmann, Jürgen (1993) [1965], *Theology of Hope: On the Ground and the Implications of a Christian Eschatology*, tr. James W. Leitch (Minneapolis, MN: Fortress Press).

Morson, Gary Saul and Caryl Emerson (1990), *Mikhail Bakhtin: Creation of a Prosaics* (Stanford University Press).

Mueller, John (1995), *Quiet Cataclysm: Reflections on the Recent Transformation of World Politics* (New York: HarperCollins).

Mueller, John (2010), *Atomic Obsession: Nuclear Alarmism from Hiroshima to al-Qaeda* (New York: Oxford University Press).

Mueller, Milton L. (2010) *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press).

Mulrine, Anna (2011), 'CIA chief Leon Panetta: The next Pearl Harbor could be a cyberattack', *The Christian Science Monitor*, 9 June.

Mumford, Lewis (1934), *Technics and Civilization* (New York: Harcourt, Brace and Company).

Münkler, Herfried (2005), *The New Wars* (Cambridge: Polity Press).

Munn, Nancy D. (1992), 'The cultural anthropology of time: A critical essay', *Annual Review of Anthropology* 21: 93–123.

Murphy, Raymond (2001), 'Nature's temporalities and the manufacture of vulnerability: A study of a sudden disaster with implications for creeping ones', *Time and Society* 10, nos. 2–3: 329–48.

Murray, W.H. (1984), 'Security considerations for personal computers', *IBM Systems Journal* 23, no. 3: 297–304.

Mythen, Gabe and Sandra Walklate (2008), 'Terrorism, risk and international security: The perils of asking "what if?"', *Security Dialogue* 39, nos. 2–3: 221–42.

Nakashima, Ellen (2010), 'War game reveals US lacks cyber-crisis skills', *The Washington Post*, 17 February.

Nakashima, Ellen (2012), 'US builds a cyber "Plan X"', *The Washington Post*, 31 May.

Nakashima, Ellen (2013), 'Pentagon plans to add 13 offensive teams to combat online threat', *The Washington Post*, 13 March.

Napolitano, Janet (2013), 'From cyber to immigration, terrorism to disasters: Securing America in the next administration', Wilson Center, Washington, DC, 24 January, www.wilsoncenter.org/event/cyber-to-immigration-terrorism-to-disasters-securing-america-the-next-administration.

National Audit Office (2013), *The UK Cyber Security Strategy: Landscape Review* (Norwich, The Stationery Office).

National Cyber Security Division (2006), *Cyber Storm: Exercise Report* (Washington, DC: Department of Homeland Security).

National Infrastructure Protection Center (and National Counterintelligence Center and Federal Bureau of Investigation) (1999), *Solar Sunrise: Dawn of a New Threat*, video, 18 minutes, www.wired.com/threatlevel/2008/09/video-solar-sun/.

National Public Radio (2010), 'Assessing the threat of cyberterrorism: Interview with James Lewis', *Fresh Air*, 10 February, www.npr.org/templates/story/story.php?storyId=123531188.

Naughtie, James (2005), *The Accidental American: Tony Blair and the Presidency*, rev. edn (London: Macmillan).

Neocleous, Mark (2008), *Critique of Security* (Edinburgh University Press).

Neustadt, Richard E. and Ernest R. May (1986), *Thinking in Time: The Uses of History for Decision Makers* (New York: The Free Press).

Newitz, Annalee and Simon Glezos (2010), 'Digital inflections: Annalee Newitz in conversation with Simon Glezos', *CTheory*, 30 November, www.ctheory.net/articles.aspx?id=673.

Newton, Isaac (1729), *The Mathematic Principles of Natural Philosophy*, vol. I, tr. Andrew Motte (London: Benjamin Motte).

Nguyen, Anh (2012), 'UK cybersecurity professionals are "too old", says Baroness Neville-Jones', *ComputerWorld UK*, 24 May, www.computerworlduk.com/news/careers/3359837/uk-cybersecurity-professionals-are-too-old-says-baroness-neville-jones/.

Nishimura, Kuniyuki (2011), 'Worlds of our remembering: The agent-structure problem as the search for identity', *Cooperation and Conflict* 46, no. 1: 96–112.

Nissenbaum, Helen (2004), 'Hackers and the contested ontology of cyberspace', *New Media and Society* 6, no. 2: 195–217.

Nissenbaum, Helen (2005), 'Where computer security meets national security', *Ethics and Information Technology* 7, no. 2: 61–73.

Nowotny, Helga (1992), 'Time and social theory: Towards a social theory of time', *Time and Society* 1, no. 3: 421–54.

Nowotny, Helga (1994), *Time: The Modern and Postmodern Experience* (Cambridge: Polity Press).

Nye, Joseph S., Jr (2011), 'Nuclear lessons for cyber security', *Strategic Studies Quarterly* 5, no. 4: 18–38.

Obama, Barack (2010), 'Remarks by the President on the economy', Winston-Salem, NC, 6 December, www.whitehouse.gov/the-press-office/2010/12/06/remarks-president-economy-winston-salem-north-carolina.

Office of Cyber Security and Information Assurance (2011), presentation, *London Conference on Cyberspace*, 2 November.

Office of Cyber Security and Information Assurance (2012), 'Cyber security skill shortages', *ITNOW* 54, no. 2: 32–4.

Olivier, Laurent (2011), *The Dark Abyss of Time: Archaeology and Memory*, tr. Arthur Greenspan (Lanham, MD: AltaMira Press).

Omand, David (2010), *Securing the State* (London: Hurst & Company).

Ong, Aihwa (2005), 'Ecologies of expertise: Assembling flows, managing citizenship', in *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*, ed. Aihwa Ong and Stephen J. Collier (Malden, MA: Blackwell Publishers), 337–53.

Onuf, Nicholas (1994), 'The constitution of international society', *European Journal of International Law* 5, no. 1: 1–19.

Orwell, George (1965) [1949], *Nineteen Eighty-Four* (London: Heinemann).

Osborne, Peter (1995), *The Politics of Time: Modernity and Avant-Garde* (London: Verso).

Ostovich, Steven (2007), 'Carl Schmitt, political theology, and eschatology', *KronoScope* 7, no. 1: 49–66.

Ostroff, Natalie and Jim Taylor (2012), 'First boot camp gets young people into cybersecurity', *BBC Newsbeat*, 7 September, www.bbc.co.uk/newsbeat/19515213.

Overy, Richard (2009), *The Morbid Age: Britain Between the Wars* (London: Allen Lane).

Ovid (1916), *Metamorphoses*, vol. II, tr. Frank Justus Miller (London: William Heinemann, Ltd.).

Page, Lewis (2008), 'DARPA wants *Matrix* style virtual world for cybergeddon', *The Register*, 7 May, www.theregister.co.uk/2008/05/07/darpa_cyber_range_rfp/.

Palmer, Allen W. (2002), 'Negotiation and resistance in global networks: The 1884 International Meridian Conference', *Mass Communication and Society* 5, no. 1: 7–24.

Panetta, Leon (2012), 'Remarks by Secretary Panetta on cybersecurity', speech to Business Executives for National Security, New York, 11 October, www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Panetta, Leon (2013), 'Remarks by Secretary Panetta', speech at Georgetown University, Washington, DC, 6 February, www.defense.gov/transcripts/transcript.aspx?transcriptid=5189.

Parkins, Wendy (2004), 'Out of time: Fast subjects and slow living', *Time and Society* 13, nos. 2–3: 363–82.

Pärna, Karen (2010), 'Digital apocalypse: The implicit religiosity of the Millennium Bug scare', in *Religions of Modernity: Relocating the Sacred to the Self and the Digital*, ed. Stef Aupers and Dick Houtman (Leiden: Brill), 239–59.

Parsons, Talcott (1949) [1937], *The Structure of Social Action*, 2nd edn (Glencoe, IL: The Free Press).

Partridge, Chris (1997), 'How to conquer the world ... and never leave the barracks', *The Times*, 27 August.

Patterson, David (2011), *A Genealogy of Evil: Anti-Semitism from Nazism to Islamic Jihad* (Cambridge University Press).

Paz, Octavio (1974) [1969], 'Order and accident', *Conjunctions and Disjunctions*, tr. Helen R. Lane (New York: Viking Press,), 91–139.

Penrose, Roger (1989), *The Emperor's New Mind: Concerning Computers, Minds and the Laws of Physics* (Oxford University Press).

Pepper, David (2010), 'The business of SIGINT: The role of modern management in the transformation of GCHQ', *Public Policy and Administration* 25, no. 1: 85–97.

Perrow, Charles (1981), 'Normal accident at Three Mile Island', *Society* 18, no. 5: 17–26.

Perrow, Charles (1999) [1984], *Normal Accidents: Living with High-Risk Technologies*, 2nd edn (Princeton University Press).

Peters, Bernard (1967), 'Security considerations in a multi-programmed computer system', *Proceedings of the 1967 Spring Joint Computer Conference* 30, 283–86.

Peters, F.E. (1967), *Greek Philosophical Terms: A Historical Lexicon* (New York University Press).

Phillips, John (2006), '*Agencement*/Assemblage', *Theory, Culture and Society* 23, nos. 2–3: 108–9.

Pick, Daniel (1993), *War Machine: The Rationalisation of Slaughter in the Modern Age* (New Haven, CT: Yale University Press).

Pietz, William (1997), 'Death of the deodand: Accursed objects and the money value of human life', *RES: Anthropology and Aesthetics* 31: 97–108.

Pilkington, Ed (2011), 'Fear: The old technology that turned hackers into informers', *The Guardian*, 7 June.

Plotinus (1992), *The Enneads*, tr. Stephen MacKenna (Burdett, NY: Larson Publications).

Pobojewska, Aldona (2001), 'New biology—Jakob von Uexküll's Umweltlehre', *Semiotica* 134, nos. 1–4: 323–39.

Poole, Steven (2012), ‘Invasion of the cyber hustlers’, *New Statesman*, 6 December, www.newstatesman.com/sci-tech/internet/2012/12/jeff-jarvis-clay-shirky-jay-rosen-invasion-cyber-hustlers.

Porter, Patrick (2015), *The Global Village Myth: Distance, War, and the Limits of Power* (Washington, DC: Georgetown University Press).

Portnoy, Michael and Seymour Goodman (2009), ‘A brief history of global responses to cyber threats’, in *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, ed. Michael Portnoy and Seymour Goodman (New York: Springer), 5–10.

Power, Richard (2000), ‘Joy riders: Mischief that leads to mayhem’, *InformIT*, 30 October, www.informit.com/articles/article.aspx?p=19603.

Prensky, Marc (2001), ‘Digital natives, digital immigrants part 1’, *On the Horizon* 9, no. 5: 1, 3–6.

President’s Council of Advisors on Science and Technology (2010), *Report to the President and Congress: Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology* (Washington, DC: White House).

Pretorius, Joelien (2008), ‘The security imaginary: Explaining military isomorphism’, *Security Dialogue* 39, no. 1 (2008): 99–120.

Prewitt, Kenneth (2004), ‘What if we give a census and no one comes?’, *Science* 304, no. 5676: 1452–3.

Prior, Arthur N. (1993), ‘Changes in events and changes in things’, in *The Philosophy of Time*, ed. Robin Le Poidevin and Murray MacBeath (Oxford University Press), 35–46.

Prozorov, Sergei (2011), ‘The other as past and present: Beyond the logic of “temporal othering” in IR theory’, *Review of International Studies* 37, no. 3: 1273–93.

Radcliff, Deborah (2002), ‘More than a game’, *ComputerWorld*, 9 September.

Rämö, Hans (1999), ‘An Aristotelian human time-space manifold: From *chronochora* to *kairotopos*’, *Time and Society* 8, no. 2: 309–28.

Rapoport, David C. (1988), ‘Messianic sanctions for terror’, *Comparative Politics* 20, no. 2: 195–213.

Rashid, Fahmida Y. (2014), ‘Global cybersecurity market to hit $120.1 billion by 2017’, *SecurityCurrent*, 6 March, www.securitycurrent.com/en/news/ac_news/global-cybersecurity-marke.

Rattray, Greg, Chris Evans and Jason Healey (2010), ‘American security in the cyber commons’, in *Contested Commons: The Future of American Power in a Multipolar World*, ed. Abraham M. Denmark and James Mulvenon (Washington, DC: Center for a New American Security), 139–72.

Rawnsley, Gary D. (2009), ‘The laws of the playground: Information warfare and propaganda across the Taiwan Strait’, in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni (London: Routledge), 79–94.

Reichenbach, Hans and Maria Reichenbach (1956), *The Direction of Time* (Berkeley, CA: University of California Press).

Reid, Julian (2009), ‘Politicizing connectivity: Beyond the biopolitics of information technology in international relations’, *Cambridge Review of International Affairs*, 22, no. 4: 607–23.

Rescher, Nicholas (1996), *Process Metaphysics: An Introduction to Process Philosophy* (Albany, NY: State University of New York Press).

Reuters (2014), 'China's Tianhe-2 retains top supercomputer rank', 17 November.

Rid, Thomas (2012), 'Cyber war will not take place', *Journal of Strategic Studies* 35, no. 1: 5–32.

Rid, Thomas (2013a), *Cyber War Will Not Take Place* (London: Hurst & Company).

Rid, Thomas (2013b), 'Cyber fail', *New Republic*, 4 February, www.newrepublic.com/article/112314/obama-administrations-lousy-record-cyber-security.

Rid, Thomas and Ben Buchanan (2015), 'Attributing cyber attacks', *Journal of Strategic Studies* 39, no. 1: 4–37.

Rid, Thomas and Peter McBurney (2012), 'Cyber-weapons', *The RUSI Journal* 157, no. 1: 6–13.

Rieff, David (2013), 'The singularity of fools', *Foreign Policy* 200: 96.

Rifkin, Jeremy (1987), *Time Wars: The Primary Conflict in Human History* (New York: Henry Holt and Company).

Rinaldi, Steven M., James P. Peerenboom and Terrence K. Kelly (2001), 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems* 21, no. 6: 11–25.

Robbins, Thomas and Susan J. Palmer (1997), 'Patterns of contemporary apocalypticism in North America', in *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*, ed. Thomas Robbins and Susan J. Palmer (New York: Routledge, 1997), 1–27.

Roberts, Geoffrey (2006), 'History, theory and the narrative turn in IR', *Review of International Studies* 32, no. 4: 703–14.

Robin, Corey (2012), 'The language of fear: National security in modern politics', in *Fear: Across the Disciplines*, ed. Jan Plamper and Benjamin Lazier (University of Pittsburgh Press), 118–31.

Rogers, Richard (2010), 'Internet research: The question of method—A keynote address from the YouTube and the 2008 Election Cycle in the United States Conference', *Journal of Information Technology and Politics* 7, nos. 2–3: 241–60.

Romm, Joseph J. (1993), *Defining National Security: The Nonmilitary Aspects* (New York: Council on Foreign Relations Press).

Rosa, Hartmut (2005), 'The speed of global flows and the pace of democratic politics', *New Political Science* 27, no. 4: 445–59.

Rosa, Hartmut (2009), 'Social acceleration: Ethical and political consequences of a desynchronized high-speed society', in Rosa and Scheuerman (ed.), 77–111.

Rosa, Hartmut and William E. Scheuerman, ed. (2009), *High-Speed Society: Social Acceleration, Power, and Modernity* (University Park, PA: Pennsylvania State University Press).

Rosenberg, Emily S. (2003), *A Date Which Will Live: Pearl Harbor in American Memory* (Durham, NC: Duke University Press).

Rosenberg, Justin (1994), 'The international imagination: IR theory and "classic social analysis"', *Millennium: Journal of International Studies* 23, no. 1: 85–108.

Rosenzweig, Paul (2013), *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Santa Barbara, CA: ABC-CLIO).

Ruggie, John Gerard (1975), 'International responses to technology: Concepts and trends', *International Organization* 29, no. 3: 557–83.

Ruggie, John (1993), 'Territoriality and beyond: Problematizing modernity in International Relations', *International Organization* 47, no. 1: 139–74.

Russia Today (2013), 'Panetta back at it with "cyber Pearl Harbor" fear mongering', 7 February, http://rt.com/usa/panetta-cyber-pearl-harbor-611/.

Rutz, Henry J. (1992), 'Introduction: The idea of a politics of time', in *The Politics of Time*, ed. Henry J. Rutz (Arlington, VA: American Anthropological Association), 1–17.

Sabin, Philip (2012), *Simulating War: Studying Conflict Through Simulation Games* (London: Continuum).

Saco, Diana (1999), 'Colonizing cyberspace: "National security" and the internet', in *Cultures of Insecurity: States, Communities, and the Production of Danger*, ed. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall (Minneapolis, MN: University of Minnesota Press), 261–91.

Sandywell, Barry (2006), 'Monsters in cyberspace: Cyberphobia and cultural panic in the information age', *Information, Communication and Society* 9, no. 1: 39–61.

Sanger, David E. (2012), *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers).

Sanger, David E., John Markoff and Thom Shanker (2009), 'US plans attack and defense in web warfare', *The New York Times*, 28 April.

SANS Institute (2012), 'SANS launches NetWars CyberCity to train cyber warriors for defense', press release, 27 November, www.sans.org/press/announcement/2012/11/27/1.

Sarkar, Dibya (2002), 'Cybersecurity guide delayed', *Federal Computer Week*, 11 June, http://fcw.com/articles/2002/06/11/cybersecurity-guide-delayed.aspx.

Satter, Raphael (2012), 'Amateurs battle malware, hackers in UK cybergames', *Associated Press*, 11 March.

Savvas, Antony (2012), 'IT students aim for the security services', *ComputerWorld UK*, 17 May, www.computerworlduk.com/news/careers/3358292/it-students-aim-for-security-services/.

Saward, Michael (2011), 'Slow theory: Taking time over transnational democratic representation', *Ethics and Global Politics* 4, no. 1: 1–18.

Sawyer, Rex (2001), *Little Imber on the Down: Salisbury Plain's Ghost Village* (East Knoyle: The Hobnob Press).

Schaefer, Nancy A. (2004), 'Y2K as an endtime sign: Apocalypticism in America at the *fin-de-millennium*', *The Journal of Popular Culture* 38, no. 1: 82–105.

Schafer, Mark and Scott Crichlow (1996), 'Antecedents of groupthink: A quantitative study', *Journal of Conflict Resolution* 40, no. 3: 415–35.

Schaffer, Jonathan (2003), 'Is there a fundamental level?', *Noûs* 37, no. 3: 498–517.

Schell, Bernadette and Clemens Martin (2006), *Webster's New World Hacker Dictionary* (Indianapolis, IN: Wiley Publishing, Inc.).

Scherpe, Klaus R. (1986), 'Dramatization and de-dramatization of "the end": The apocalyptic consciousness of modernity and post-modernity', *Cultural Critique* 5: 95–129.

Scheuerman, William E. (2004), *Liberal Democracy and the Social Acceleration of Time* (Baltimore, MD: Johns Hopkins University Press).

Schieber, Philip (1987), 'The wit and wisdom of Grace Hopper', *The OCLC Newsletter* 167, n.p., www.cs.yale.edu/homes/tap/Files/hopper-wit.html.

Schivelbusch, Wolfgang (1986) [1977], *The Railway Journey: The Industrialization of Time and Space in the 19th Century* (Berkeley, CA: University of California Press).

Schlienger, Thomas and Stephanie Teufel (2002), 'Information security culture: The socio-cultural dimension in information security management', in *Security in the Information Society: Visions and Perspectives*, ed. M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi and Heba K. Aslan (Norwell, MA: Kluwer Academic Publishers), 191–201.

Schmidt, Howard A. (2006), *Patrolling Cyberspace: Lessons Learned from a Lifetime in Data Security* (North Potomac, MD: Larstan Publishing, Inc.).

Schmitt, Carl (1996) [1932], *The Concept of the Political*, tr. George Schwab (Chicago University Press).

Schmitt, Frederick F. (1994), 'Socializing epistemology: An introduction through two sample issues', in *Socializing Epistemology: The Social Dimensions of Knowledge*, ed. Frederick F. Schmitt (Lanham, MD: Rowman and Littlefield Publishers, Inc.), 1–27.

Schmitt, Michael N., ed. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press).

Schneier, Bruce (2000), 'The process of security', *Information Security Magazine*, April, www.schneier.com/essay-062.html.

Schneier, Bruce (2004), *Secrets and Lies: Digital Security in a Networked World*, rev. edn (Indianapolis, IN: John Wiley & Sons).

Schneier, Bruce (2013a), 'Our new regimes of trust', *The SciTech Lawyer* 9, nos. 3–4, www.schneier.com/blog/archives/2013/02/our_new_regimes.html.

Schneier, Bruce (2013b), 'Our security models will never work—No matter what we do', *Wired*, 14 March, www.wired.com/opinion/2013/03/security-when-the-bad-guys-have-technology-too-how-do-we-survive/.

Schofield, Janet W. and Mark A. Pavelchak (1989), 'Fallout from *The Day After*: The impact of a TV film on attitudes relating to nuclear war', *Journal of Applied Social Psychology* 19, no. 5: 433–48.

Schroeder, Paul W. (1997), 'History and International Relations theory', *International Security* 22, no. 1: 64–74.

Schurz, Carl (1913), 'Manifest destiny', *Speeches, Correspondence and Political Papers*, vol. V, ed. Frederic Bancroft (New York: The Knickerbocker Press), 191–214.

Schwaller, Caroline M. (1997), 'Year 2000. A date with destiny. Apocalypse as "the end" or as "revelation"?', *Space and Culture* 1, no. 2: 37–49.

Schwartau, Winn (1991a), *Terminal Compromise—Computer Terrorism: When Privacy and Freedom are the Victims* (Seminole, FL: Interpact Press).

Schwartau, Winn (1991b), 'Fighting terminal terrorism', *Computerworld*, 28 January, 23.

Schwartau, Winn (1994), *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age* (New York: Thunder's Mouth Press).

Schwartau, Winn (2002), *Pearl Harbor Dot Com* (Seminole, FL: Interpact Press).

Sewell, William H., Jr (1990), 'Collective violence and collective loyalties in France: Why the French Revolution made a difference', *Politics and Society* 18, no. 4: 527–52.

Shah, Sooraj (2013), 'Cyber Security Challenge "is not only about recruiting talent", claims CEO', *Computing*, 13 March, www.computing.co.uk/ctg/news/2254243/cyber-security-challenge-is-not-only-about-recruiting-talent-claims-ceo.

Shameli-Sendi, Alireza, Naser Ezzati-Jivan, Masoume Jabbarifar and Michael Dagenais (2012), 'Intrusion response systems: Survey and taxonomy', *International Journal of Computer Science and Network Security* 12, no. 1: 1–14.

Shannon, Claude E. (1949), 'Communication theory of secrecy systems', *The Bell System Technical Journal* 28, no. 4: 656–715.

Shim, Doobo (1998), 'From yellow peril through model minority to renewed yellow peril', *Journal of Communication Inquiry* 22, no. 4: 385–409.

Shostack, Adam (2012), 'The evolution of information security', *The Next Wave: The National Security Agency's Review of Emerging Technologies* 19, no. 2: 6–11.

Siaterlis, Christos and Béla Genge (2014), 'Cyber-physical testbeds', *Communications of the ACM* 57, no. 6: 64–73.

Singer, P.W. and Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press).

Sky News (2013), bulletin, 8 January.

Slack, Jennifer Daryl (1984), 'The information revolution as ideology', *Media, Culture and Society* 6, no. 3: 247–56.

Smith, Chloe (2012), speech to London Conference on Cyberspace, 6 November, www.gov.uk/government/speeches/chloe-smith-speaks-at-cyber-security-summit.

Smith, George (1998), 'An electronic Pearl Harbor? Not likely', *Issues in Science and Technology* 15, no. 1: 68–73.

Smith, John E. (1969), 'Time, times, and the "right time"; *Chronos* and *kairos*', *The Monist* 53, no. 1: 1–13.

Smith, John E. (1986), 'Time and qualitative time', *The Review of Metaphysics* 40, no. 1: 3–16.

Smith, Roger (2010), 'The long history of gaming in military training', *Simulation and Gaming* 41, no. 1: 6–19.

Smith, Steve (1999), 'The increasing insecurity of security studies: Conceptualizing security in the last twenty years', *Contemporary Security Policy* 20, no. 3: 72–101.

Smoke, Richard (1993), *National Security and the Nuclear Dilemma: An Introduction to the American Experience in the Cold War*, 3rd edn (New York: McGraw-Hill).

Solomon, Ty (2014), 'Time and subjectivity in world politics', *International Studies Quarterly* 58, no. 4: 671–81.

Spellman, Frank R. and Melissa L. Stoudt (2011), *Nuclear Infrastructure Protection and Homeland Security* (Lanham, MD: Government Institutes).

Stakhanova, Natalia, Samik Basu and Johnny Wong (2007), ‘A taxonomy of intrusion response systems’, *International Journal of Information and Computer Security* 1, nos. 1–2: 169–84.

Star, Susan Leigh (1999), ‘The ethnography of infrastructure’, *American Behavioral Scientist* 43, no. 3: 377–91.

Starr, Harvey (2013), ‘On geopolitics: Spaces and places’, *International Studies Quarterly* 57, no. 3: 433–39.

Staudenmeier, John M. (1985), *Technology’s Storytellers: Reweaving the Human Fabric* (Cambridge, MA: MIT Press).

Steele, Brent J. (2007), ‘Liberal-idealism: A constructivist critique’, *International Studies Review* 9, no. 1: 23–52.

Steele, Brent J. (2008), *Ontological Security In International Relations: Self-Identity and the IR State* (London: Routledge).

Stephens, Carlene (1989), ‘“The most reliable time”: William Bond, the New England railroads, and time awareness in 19th-century America’, *Technology and Culture* 30, no. 1: 1–24.

Sterling, Bruce (2010), ‘Atemporality for the creative artist’, *Transmediale 10*, Berlin, 6 February, www.wired.com/beyond_the_beyond/2010/02/atemporality-for-the-creative-artist/.

Stevens, Tim (2012), ‘A cyberwar of ideas? Deterrence and norms in cyberspace’, *Contemporary Security Policy* 33, no. 1: 148–70.

Stevens, Tim (2013a), ‘Information warfare: A response to Taddeo’, *Philosophy and Technology* 26, no. 2: 221–25.

Stevens, Tim (2013b), ‘DEFCON to feds: “We need some time apart”’, *Assembling Security*, 11 July, http://assemblingsecurity.wordpress.com/2013/07/11/defcon-feds/.

Stevenson, David (2014), ‘Learning from the past: The relevance of international history’, *International Affairs* 90, no. 1: 5–22.

Stewart, William (2014), ‘Pupils to be taught cyber-security from age 11 to help tackle online crime’, *Times Educational Supplement*, 13 March.

Stibitz, George (1945), ‘Relay computers’, National Defense Research Committee, Applied Mathematics Panel, AMP Report 171.1R.

Stockdale, Liam P.D. (2013), ‘Imagined futures and exceptional presents: A conceptual critique of “pre-emptive security”’, *Global Change, Peace and Security* 25, no. 2: 141–57.

Stone, Deborah A. (1989), ‘Causal stories and the formation of policy agendas’, *Political Science Quarterly* 104, no. 2: 281–300.

Stone, John (2013), ‘Cyber war *will* take place!’, *Journal of Strategic Studies* 36, no. 1: 101–8.

Stronach, Ian, John Clarke and Jo Frankham (2014), ‘Economic “revelations” and the metaphors of the meltdown: An educational deconstruction’, *British Educational Research Journal* 40, no. 2: 319–36.

Sturken, Marita (1997), *Tangled Memories: The Vietnam War, the AIDS Epidemic, and the Politics of Remembering* (Berkeley, CA: University of California Press).

Sulek, David and Ned Moran (2009), 'What analogies can tell us about the future of cybersecurity', in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press), 118–31.

Summers, Rita C. (1984), 'An overview of computer security', *IBM Systems Journal* 23, no. 4: 309–25.

Swyngedouw, Erik (2013), 'Apocalypse now! Fear and doomsday pleasures', *Capitalism Nature Socialism* 24, no. 1: 9–18.

Tapia, Andrea H. (2003), 'Technomillennialism: A subcultural response to the technological threat of Y2K', *Science, Technology and Human Values* 28, no. 4: 483–512.

Taylor, Anthony (2012), *London's Burning: Pulp Fiction, the Politics of Terrorism and the Destruction of the Capital in British Popular Culture, 1840–2005* (London: Continuum).

Taylor, Charles (2004), *Modern Social Imaginaries* (Durham, NC: Duke University Press).

Taylor, Paul (2012), 'Former US spy chief warns on cybersecurity', *Financial Times*, 2 December.

Taylor, Paul A. (1999), *Hackers: Crime in the Digital Sublime* (London: Routledge).

Tegmark, Max and Nick Bostrom (2005), 'Is a doomsday catastrophe likely?', *Nature* 438: 754.

Teske, Roland J. (2000), 'William of Auvergne on time and eternity', *Traditio* 55: 125–41.

Tennyson, Alfred (1971), 'Ode on the death of the Duke of Wellington', *Poems and Plays*, ed. T. Herbert Warren (Oxford University Press).

The Economist (2012), 'Hype and fear', 8 December, 62.

Thibodeau, Patrick (2013), 'Fear of thinking war machines may push US to exascale', *ComputerWorld*, 20 June, www.computerworld.com/s/article/9240230/Fear_of_thinking_war_machines_may_push_U.S._to_exascale.

Thierer, Adam (2013), 'Technopanics, threat inflation, and the danger of an information technology precautionary principle', *Minnesota Journal of Law, Science and Technology* 14, no. 1: 309–86.

Thompson, E.P. (1967), 'Time, work-discipline and industrial capitalism', *Past and Present* 38: 56–97.

Thoreau, Henry David (1888) [1854], *Walden* (London: Walter Scott).

Thrift, Nigel (2008), *Non-Representational Theory: Space, Politics, Affect* (London: Routledge).

Tierney, Kathleen, Christine Bevc and Erica Kuligowski (2006), 'Metaphors matter: Disaster myths, media frames, and their consequences in Hurricane Katrina', *The Annals of the American Academy of Political and Social Science* 604, no. 1: 57–81.

Todorova, Maria (2005), 'The trap of backwardness: Modernity, temporality, and the study of Eastern European nationalism', *Slavic Review* 64, no. 1: 140–64.

Toulmin, Stephen and June Goodfield (1965), *The Discovery of Time* (London: Hutchinson).

Trigger, Bruce G. (1989), *A History of Archaeological Thought* (Cambridge University Press).

Tsouras, Peter G., ed. (2000), *The Greenhill Dictionary of Military Quotations* (London: Greenhill Books).

Tsutsui, William M. (2010), ‘Oh no, there goes Tokyo: Recreational apocalypse and the city in postwar Japanese popular culture’, in *Noir Urbanisms: Dystopic Images of the Modern City*, ed. Gyan Prakash (Princeton University Press), 104–26.

Urbelis, Alexander (2005), ‘Toward a more equitable prosecution of cybercrime: Concerning hackers, criminals, and the national security’, *Vermont Law Review* 29, no. 4: 975–1008.

Urry, John (1994), ‘Time, leisure and social identity’, *Time and Society* 3, no. 2: 131–49.

US Commodity Futures Trading Commission and US Securities and Exchange Commission (2010), *Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues* (Washington, DC: CFTC/SEC).

US Department of Justice (1998), ‘Israeli citizen arrested in Israel for hacking United States and Israeli government computers’, 18 March, www.justice.gov/opa/pr/1998/March/125.htm.html.

US Joint Chiefs of Staff (2013), *Cyberspace Operations*, Joint Publication 3–12 (R), http://fas.org/irp/doddir/dod/jp3_12r.pdf.

Van Creveld, Martin (1989), *Technology and War: From 2000 BC to the Present*, rev. and expanded edn (New York: The Free Press).

Van Creveld, Martin (2013), *Wargames: From Gladiators to Gigabytes* (Cambridge University Press).

Van Loon, Joost (2000), ‘Imminent immanence: The time-politics of speed and the management of decline’, *Time and Society* 9, nos. 2–3: 347–53.

Vatis, Michael (2002), ‘Cyber attacks: Protecting America’s security against digital threats’, *ESDP Discussion Paper 2002–04* (Cambridge, MA: John F. Kennedy School of Government, Harvard University).

Vaughan-Williams, Nick (2005), ‘International Relations and the “problem of history”’, *Millennium: Journal of International Studies* 34, no. 1: 115–36.

Verbeek, Peter-Paul (2004), *What Things Do: Philosophical Reflections on Technology, Agency, and Design* (University Park, PA: Pennsylvania State University Press).

Vieira, Ryan Anthony (2011), ‘Connecting the new political history with recent theories of temporal acceleration: Speed, politics, and the cultural imagination of *fin de siècle* Britain’, *History and Theory* 50, no. 3: 373–89.

Viereck, Peter (1949), ‘The poet in the machine age’, *Journal of the History of Ideas* 10, no. 1: 88–103.

Virilio, Paul (1993) [1976], *L’Insécurité du Territoire*, 2nd edn (Paris: Galilée).

Virilio, Paul (1997) [1995], *Open Sky*, tr. Julie Rose (London: Verso).

Virilio, Paul (2000) [1990], *Polar Inertia*, tr. Patrick Camiller (London: Sage).

Virilio, Paul (2004), ‘The last vehicle’, in *The Paul Virilio Reader*, ed. Steve Redhead (New York: Columbia University Press), 109–20.

Virilio, Paul (2007) [2005], *The Original Accident*, tr. Julie Rose (Cambridge: Polity).

Virilio, Paul (2009) [1980], *The Aesthetics of Disappearance*, tr. Philip Beitchman (Los Angeles, CA: Semiotext(e)).

Virilio, Paul (2012) [2010], *The Great Accelerator*, tr. Julie Rose (Cambridge: Polity).

Virilio, Paul and John Armitage (2011), 'The third war: Cities, conflict and contemporary art: Interview with Paul Virilio', in *Virilio Now: Current Perspectives in Virilio Studies*, ed. John Armitage (Cambridge: Polity), 29–45.

Virilio, Paul, Gérard Courtois and Michel Guerrin (2008), 'Le krach actuel représente l'accident intégral par excellence', *Le Monde*, 18 October.

Virilio, Paul and James Der Derian (1998), '"Is the author dead?"—An interview with Paul Virilio', in *The Virilio Reader*, ed. James Der Derian (Malden, MA: Blackwell Publishers), 16–21.

Virilio, Paul and Philippe Petit (1999) [1996], *Politics of the Very Worst: An Interview by Philippe Petit*, tr. Michael Cavaliere, ed. Sylvère Lotringer (New York: Semiotext(e)).

Von Uexküll, Jakob (1957) [1934], 'A stroll through the worlds of animals and men: A picture book of invisible worlds', in *Instinctive Behavior: The Development of a Modern Concept*, tr. and ed. Claire H. Schiller (New York: International Universities Press, Inc.), 5–80.

Walker, Jeremy and Melinda Cooper (2011), 'Genealogies of resilience: From systems ecology to the political economy of crisis adaptation', *Security Dialogue* 42, no. 2: 143–60.

Walker, R.B.J. (1989), 'History and structure in the theory of International Relations', *Millennium: Journal of International Studies* 18, no. 2: 163–83.

Walker, R.B.J. (1993), *Inside/Outside: International Relations as Political Theory* (Cambridge University Press).

Walker, R.B.J. (1997), 'The subject of security', in *Critical Security Studies: Concepts and Cases*, ed. Keith Krause and Michael C. Williams (London: Routledge), 61–81.

Walpole, Horace (1973), 'Letter to Thomas Walpole the Younger, Saturday 19 February 1785', *Horace Walpole's Correspondence*, vol. XXXVI, ed. W.S. Lewis (New Haven, CT: Yale University), 231–3.

Ward, Koral (2008), *Augenblick: The Concept of the 'Decisive Moment' in 19th- and 20th-Century Philosophy* (Aldershot: Ashgate).

Warrell, Helen (2014), 'Cyber security industry sends recruiting officers into schools', *FT.com*, 22 October 2014, www.ft.com/cms/s/0/ae43a730-5a00-11e4-8771-00144feab7de.html#axzz3MA5xiWh1.

Watson, Julie (2011), 'Mock city rises at Marine base for urban training', *Associated Press*, 25 January.

Watson, Jonathan (2012), 'Getting serious about security', *Business Technology*, April, 9.

Webster, Frank (2006) [1995], *Theories of the Information Society*, 3rd edn (London: Routledge).

Webster, Frank and Kevin Robins (1986), *Information Technology: A Luddite Analysis* (Norwood, NJ: Ablex Publishing Corporation).

Weinberger, Sharon (2008), 'Cyberwarfare: DARPA's new "space race"', *Danger Room*, 1 May, www.wired.com/dangerroom/2008/05/the-pentagon-wa-2/.

Weithman, Paul (2001), 'Augustine's political philosophy', in *The Cambridge Companion to Augustine*, ed. Eleonore Stump and Norman Kretzmann (Cambridge University Press, 2001), 234–52.

Wells, H.G. (1913), *The Discovery of the Future* (New York: B.W. Huebsch).

Wells, H.G. (1934) [1931], *The Work, Wealth and Happiness of Mankind*, new and rev. edn (London: William Heinemann).

Wendt, Alexander (2003), 'Why a world state is inevitable', *European Journal of International Relations* 9, no. 4: 491–542.

Wertheim, Margaret (1999), *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (London: Virago).

Wessinger, Catherine (1997), 'Millennialism with and without the mayhem', in *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*, ed. Thomas Robbins and Susan J. Palmer (New York: Routledge), 47–59.

Wesson, Paul S. (2010), 'Time as an illusion', in *Minkowski Spacetime: A Hundred Years Later*, ed. Vesselin Petkov (New York: Springer), 307–18.

West, Mark and Chris Carey (2006), '(Re)enacting frontier justice: The Bush administration's tactical narration of the Old West fantasy after September 11', *Quarterly Journal of Speech* 92, no. 4: 379–412.

Wheeler, John Archibald Wheeler (1982), 'The computer and the universe', *International Journal of Theoretical Physics* 21, nos. 6–7: 557–72.

White, Jonathan (2013), 'Thinking generations', *British Journal of Sociology* 64, no. 2: 216–47.

Whitehead, Alfred North (1920), *The Concept of Nature* (Cambridge University Press).

White House (2003), *The National Strategy to Secure Cyberspace* (Washington, DC: White House).

White House (2009), *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House).

White House (2011), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House).

White House (2013a), *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636.

White House (2013b), *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21.

Williams, Donald C. (1951), 'The myth of passage', *The Journal of Philosophy* 48, no. 15: 457–72.

Williams, Michael C. (2012), 'The new economy of security', *Global Crime* 13, no. 4: 312–19.

Williams, Stewart (2012), 'Rendering the untimely event of disaster ever present', *Landscape Review* 14, no. 2: 86–96.

Wilson, Clay (2005), *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington, DC: Congressional Research Service).

Wilson, Eric (2012), 'Criminogenic cyber-capitalism: Paul Virilio, simulation, and the global financial crisis', *Critical Criminology* 20, no. 3: 249–74.

Winner, Langdon (2004), 'Trust and terror: The vulnerability of complex socio-technical systems', *Science as Culture* 13, no. 2: 155–72.

Winthrop-Young, Geoffrey (2010), ‘Afterword: Bubbles and webs: A backdoor stroll through the readings of Uexküll’, in Jakob von Uexküll, *A Foray into the Worlds of Animals and Humans: With a Theory of Meaning*, tr. Joseph D. O’Neil (Minneapolis, MN: University of Minnesota Press), 209–43.

Wohlstetter, Roberta (1962), *Pearl Harbor: Warning and Decision* (Stanford University Press).

Wojcik, Daniel (1997), *The End of the World as We Know It: Faith, Fatalism, and Apocalypse in America* (New York University Press).

Wolfers, Arnold (1952), ‘National security as ambiguous symbol’, *Political Science Quarterly* 67, no. 4: 481–502.

Woodcock, George (1977), ‘The tyranny of the clock’, in *The Anarchist Reader*, ed. George Woodcock (Hassocks: Harvester Press), 132–6.

Woodward, Bob (2002), *Bush at War* (New York: Simon & Schuster).

World Economic Forum (2014), *Global Risks 2014*, 9th edn (Geneva: World Economic Forum).

Yeats, William Butler (2008), ‘The second coming’, *The Collected Poems of W.B. Yeats* (Ware: Wordsworth Editions).

Yould, Rachel E.D. (2003), ‘Beyond the American fortress: Understanding homeland security in the information age’, in *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Society*, ed. Robert Latham (New York: The New Press), 74–98.

Zenko, Micah (2013), ‘Most. Dangerous. World. Ever’, *Foreign Policy*, 26 February, www.foreignpolicy.com/articles/2013/02/26/most_dangerous_world_ever.

Zerubavel, Eviatar (1987), ‘The language of time: Toward a semiotics of temporality’, *The Sociological Quarterly* 28, no. 3: 343–56.

Zetter, Kim (2014), ‘Meet MonsterMind, the NSA bot that could wage cyberwar autonomously’, *Wired*, 13 August 2014, www.wired.com/2014/08/nsa-monstermind-cyberwarfare/.

Zimmerman, Rae (2001), ‘Social implications of infrastructure network interactions’, *Journal of Urban Technology* 8, no. 3: 97–119.

Zittrain, Jonathan (2008), *The Future of the Internet—And How to Stop It* (London: Penguin).

Zuccato, Albin (2007), ‘Holistic security management framework applied in electronic commerce’, *Computers and Security* 26, no. 3: 256–65.

Zurbrugg, Nicholas (1999), ‘Virilio, Stelarc and “terminal” technoculture’, *Theory, Culture and Society* 16, nos. 5–6: 177–99.

Index