# Cyber security and the politics of time

Stevens, Timothy Charles

*Awarding institution:*
King's College London

# Cyber Security
## and the
# Politics of Time

**Timothy Charles Stevens**

*Thesis submitted in accordance with the requirements for the degree of*

*Doctor of Philosophy*

King's College London

Department of War Studies

November 2013

## Abstract

Time is an under-represented topic in security studies and International Relations (IR). The development and implementation of security measures are often justified as necessary responses to the contemporary rate of global change yet little attention is granted time and temporality as factors influencing the politics and practices of security. This thesis proposes that security can be understood within the framework of a 'politics of time' (chronopolitics), in which collective perceptions of time and temporality are constitutive of security politics and practices. Its principal object is cyber security, which aims to regulate and exploit complex sociotechnical systems of networked and interdependent information technologies. The thesis examines how cyber security actors imagine time and temporality in (post)modernity and the implications of these temporal biases for the politics of cyber security. It explores how cyber security actors imagine the accelerating present and the relative deceleration of political decision-making; how apocalyptic narratives of imminent catastrophe illustrate concerns about the immanent dangers of technology; how the past is mobilised through historical analogies to understand dystopian futures; how the future is metaphorically inhabited through preparedness exercises and simulations, and literally populated through education, training and recruitment. These 'chronotypes' inform the cyber security imaginary and disclose a manifold of deeper chronopolitical tendencies, theorised here as the logics of assemblage, real time, event, and eschaton. The thesis makes an original contribution to IR by promoting the interdisciplinary analysis of time to help understand the politics and practices of contemporary security.

## Contents

***Acknowledgements***

I would like to thank David Bhowmik, Daniel Cordle, Kathryn Marie Fisher, Chris Fryer, Mike Innes, Jo Kovacik, Sean Lawson, Sam Liles and Jan Nederveen Pieterse for sharing ideas and research materials. I have benefited greatly from the collegiality and wisdom of my colleagues at King's College London, particularly Neville Bolt, Peter McBurney, Nick Michelsen, Richard Overill, Thomas Rid and John Stone. My supervisors deserve particular gratitude: David Betz marshalled this project to completion and my debt to him is immeasurable; Theo Farrell has long been an encouraging voice without whom this thesis would not have been possible. My examiners, Christopher Coker and Andrew Hoskins, provided comments and insights I am fortunate to be able to incorporate into this work. I acknowledge the financial support of the Economic and Social Research Council (ES/H022678/1) and Charles Wolfson Townsley. I cannot thank my parents and family enough for their support and encouragement. To Lu, who makes all things possible, and Stanley, from whom I have already learnt more than he will ever know, my eternal love, thanks and appreciation.

# 1 INTRODUCTION

For tribal man space was the uncontrollable mystery.

For technological man it is time that occupies the same role.[1]

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'.[2] 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. As Hobbes states elsewhere, 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'.[3] Security is always 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 or foundational of politics.[4] 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

[1] Marshall McLuhan, The Mechanical Bride: Folklore of Industrial Man (Corte Madera, CA: Gingko Press, 2002/1951), 85.
[2] Thomas Hobbes, Leviathan, ed. Richard Tuck, rev. edn. (Cambridge: Cambridge University Press, 1996/1651), XII.52.
[3] Thomas Hobbes, On the Citizen, eds. Richard Tuck and Michael Silverthorne (Cambridge: Cambridge University Press, 1998/1642), 11.
[4] Respectively, Ken Booth, Theory of World Security (Cambridge: Cambridge University Press, 2007); Michael Dillon, Politics of Security: Towards a Political Philosophy of Continental Thought (London: Routledge, 1996).

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'.[5] 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'.[6] 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 similarly retrospective, mining the past to frame the narratives of identity and destiny that legitimise and justify its interventions. The tenses of time are both the friend and enemy of security: the threat of time and the ungoverned processes of change are the reasons provided for the necessary enactments of security whilst 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 effect 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 thesis addresses these questions through an examination of a particular form of security that has emerged in the late 20th and early 21st centuries, that of cyber security. Cyber security is a response to the perceived risks and threats arising from the modern, global information-technological infrastructure most commonly glossed as 'the Internet' and is concerned with anyone or anything that communicates through digital, electronic means. The aim of this thesis is to establish how cyber security communities produce a 'politics of time', in which their

[5] Talcott Parsons, The Structure of Social Action, 2nd. edn. (Glencoe, IL: The Free Press, 1949/1937), 45.
[6] Philip Graham, 'Space: Irrealis Objects in Technology Policy and Their Role in a New Political Economy', Discourse & Society 12, no. 6 (2001): 765.

temporal perspectives are fundamentally constitutive of the political behaviours that enable the policies and practices of cyber security.

For instance, cyber security self-identifies with a particular periodization of the world. The concept of the 'Information Age' is not unique to cyber security but how does this inform cyber security and what political work does this concept perform? 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 are implemented in attempts to regulate it? The answers to each of these questions reveals 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. The task of this thesis is to describe, analyse and theorise this chronopolitical manifold and to locate it within the broader politics of cyber security. The chronopolitical lens is not the only one through which to view cyber security, however, and the pluralist instincts of this enquiry respect the importance of space, place, information, matter, energy and time in studies of the political. However, in a world 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 such a 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.

## 1.1 Cyber Security

Security has attained an unprecedented constitutive role 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.[7] Over the intervening decades and, particularly, since the end of the Cold War, conceptions of security have been 'widened' and 'deepened' commensurate with a range of worldviews and theoretical orientations.[8] Widening involves the application of security logics beyond military conflicts and the security of states and nations to a plurality of securities: human, energy, food, environment, water, to name but a few. Deepening shifts emphasis from the state 'down' to the level of the person and the citizen and 'up' to the international and the global. In this double move, security has been 'defined and redefined …. revisioned, re-mapped, gendered, refused', but the logic of security itself exerts a firm grip on the 'contemporary social and political imagination', which is 'dominated by the lexicon of security and the related idea that we are living in an increasingly insecure world'.[9]

The study of security is complicated by, but not always mindful of, a fundamental distinction between the different meanings of the word 'security' itself, which 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'.[10] Security is not merely a condition to be achieved but has a performative function, in that it serves to order the social world rather than merely being an accurate description of any external or objective reality: security transforms social relations into 'security relations'.[11] For some scholars, the infiltration of

[7] Joseph J. Romm, Defining National Security: The Nonmilitary Aspects (New York: Council on Foreign Relations Press, 1993), 1-8.
[8] Barry Buzan, People, States and Fear: The National Security Problem in International Relations (Chapel Hill, NC: University of North Carolina Press, 1983); Steve Smith, 'The Increasing Insecurity of Security Studies: Conceptualizing Security in the Last Twenty Years', Contemporary Security Policy 20, no. 3 (1999): 72-101; Barry Buzan and Lene Hansen, The Evolution of International Security Studies (Cambridge: Cambridge University Press, 2009), 187-225.
[9] Mark Neocleous, Critique of Security (Edinburgh: Edinburgh University Press, 2008), 2-3.
[10] Nils Bubandt, 'Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds', Security Dialogue 36, no. 3 (2005): 278.
[11] Jef Huysmans, 'Security! What Do You Mean? From Concept to Thick Signifier', European Journal of International Relations 4, no. 2 (1996): 226-255.

security logic and practice into contemporary life is so pervasive that, as Michael Dillon suggests, security is not only a pillar of modern politics and society but a key signifier of modernity itself.[12] 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 counterterrorism policy on the same publics it professes to protect, 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?"'[13]

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.[14] The logic of security extends to architecture, with security 'designed in' to everything from airports and sports stadia to nightclubs and shopping centres.[15] No major public event can be undertaken without planners demonstrating their commitment to both visible and invisible security measures,[16] for which costs escalate as much in line with clients' fears and consultants' imaginations as they do with the existence of any credible threat. Fawaz and Bou Akar write that security in the city has been normalised, 'stripped of its political significance': 'threats are taken at face value and generalized in the name of an hypothesized common good, without much recognition of their historical, geographical and social

[12] Dillon, Politics of Security.
[13] Langdon Winner, 'Trust and Terror: The Vulnerability of Complex Socio-Technical Systems', Science as Culture 13, no. 2 (2004): 162.
[14] This is a process through which the 'security industry aims to turn the feelings associated with (in)security into the consumption of commodities'; Neocleous, Critique of Security, 154. Aso, Elke Krahmann, 'Security: Collective Good or Commodity?', European Journal of International Relations 14, no. 3 (2008): 379-404.
[15] Jon Coaffee, Paul O'Hare and Marian Hawkesworth, 'The Visibility of (In)Security: The Aesthetics of Planning Urban Defences Against Terrorism', Security Dialogue 40, nos. 4-5 (2009): 489-511; Jon Coaffee, 'Protecting Vulnerable Cities: The UK's Resilience Response to Defending Everyday Urban Infrastructure', International Affairs 84, no. 4 (2010): 939-954.
[16] Philip Boyle and Kevin D. Haggerty, 'Spectacular Security: Mega-Events and the Security Complex', International Political Sociology 3, no. 3 (2009): 257-274; Philip Boyle and Kevin D. Haggerty, 'Planning for the Worst: Risk, Uncertainty and the Olympic Games', The British Journal of Sociology 63, no. 2 (2012): 241-259.

contexts'.[17] Security is notable in that its claims 'have long thrived on a denotative imprecision that has been carefully calibrated', in which there is 'simultaneous appeal to the hard and the vacuous, the precise and the imprecise'.[18] 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.

In the last two decades, the logic of security has found a novel mode of expression, whose material ubiquity and conceptual totalitarianism makes singular claims upon the nature of the modern world and challenges the extent of any previous regime of security. 'Cyber security' is the first attempt to foster an holistic approach to the security issues raised by information technologies, in particular the digital, electronic and networked information technologies of the Internet and 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, and somewhat anachronistically, termed 'cyberspace'—is constructed as 'ungovernable, unknowable, a cause of vulnerability, inevitably threatening, and a home to threatening actors'.[19] It is frequently 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' sensu lato.

Cyber security has proven itself a concept elastic in definition and elusive in practice. Given its concerns with almost anything that communicates digitally and electronically, whether these

[17] Mona Fawaz and Hiba Bou Akar, 'Practicing (In)Security in the City', City & Society 24, no. 2 (2012): 105.
[18] R.B.J. Walker, 'The Subject of Security', in Critical Security Studies: Concepts and Cases, eds. Keith Krause and Michael C. Williams (London: Routledge, 1997), 63.
[19] David Barnard-Wills and Debi Ashenden, 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', Space & Culture 15, no. 2 (2012): 110-123.

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. These 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 and structure—and accusations of adversarial 'cyber espionage' are often blind to friendly states' uses of identical tactics in pursuit of economic and national security ends.[20] 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 really is just 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'.[21]

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 suggest.[22] 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. Simply put, this means that cybersecurity is the security one enjoys in and from cyberspace'.[23] Cyber security is no longer just about the 'security of cyber',

[20] One of the most robust expressions of this argument is provided by Glenn Greenwald, 'Pentagon's New Massive Expansion of "Cyber-Security" Unit is About Everything Except Defense', The Guardian, 28 January 2013.
[21] James A. Lewis, 'Aux Armes, Citoyens: Cyber Security and Regulation in the United States', Telecommunications Policy 29, no. 11 (2005): 821.
[22] For a similar perspective, see Myriam Dunn, 'Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory', in International Relations and Security in the Digital Age, eds. Johan Eriksson and Giampiero Giacomello (London: Routledge, 2007), 85.
[23] Myriam Dunn Cavelty and Manuel Suter, 'The Art of CIIP Strategy: Taking Stock of Content and Processes', in Critical Information Infrastructure Protection, eds. Javier Lopez, Robert Setola and Stephen D. Wolthusen (Berlin: Springer-Verlag), 19.

as it were, but is also 'security through cyber'.[24] From this perspective, information technologies are the material substrate 'upon which all security sectors are destined to converge'.[25] Cyber security is not restricted to the security of information and information technologies, therefore, but is the means through which other forms of security might be pursued and a condition of that greater security.

Cyber security 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. Cyber security is a sociotechnical 'assemblage', understood in its dictionary sense as a collection of 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.[26] 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.[27]

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

[24] Rid admonishes those who treat 'cyber' as a 'noun', a warning heeded in this document wherever possible. 'Cyber' is certainly ambiguous and unsatisfactory but, unfortunately, we have no ready substitute. Thomas Rid, Cyber War Will Not Take Place (London: Hurst & Company, 2013), ix.
[25] Rachel E.D. Yould, '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, 2003), 78.
[26] Colin McFarlane and Ben Anderson, 'Thinking with Assemblage', Area 43, no. 2 (2011): 162-164.
[27] Stephen J. Collier and Aihwa Ong, 'Global Assemblages, Anthropological Problems', in Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems, eds. Aihwa Ong and Stephen J. Collier (Malden, MA: Blackwell, 2005), 3-21; Cynthia Enloe, 'The Mundane Matters', International Political Sociology 5, no. 4 (2011): 447-450.

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.[28] 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.[29] 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 existence.

We might dispute whether 'society' exists but we can identify and name other relatively stable assemblages as units of analysis through which to describe their composition, function and interactions with others. Although their definition and theorisation remain contested, 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 the whole being is exerted toward accomplishing nothing'.[30] In its complexity, non-linearity and variety, society is already a more daunting object of analysis than the linearities of engineering and ballistics and students of the social contend that it is not the

[28] Manuel DeLanda, A New Philosophy of Society: Assemblage Theory and Social Complexity (London: Continuum, 2006), 10.
[29] Bruno Latour, Reassembling the Social: An Introduction to Actor-Network Theory (Oxford: Oxford University Press, 2005). 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; ibid., 71-72.
[30] Albert Camus, 'The Myth of Sisyphus', The Myth of Sisyphus and Other Essays (New York: Vintage International, 1991/1955), 120.

proverbial rocket science that is difficult but social science.[31] 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'.[32] The taming and constraining of this multivocality enables cyber security to cohere as an assemblage, mediated through communities of knowledge and practice that enable and instantiate the processes of cyber security.

## 1.2 Imagination and Community

Studies of 'digital-age security' have tended to be 'idiosyncratic and policy-oriented, with little or no effort to apply or develop theory'.[33] This is not to say that existing work on cyber security is not informed by theoretical considerations but that the majority of extant research emphasises policy and technical implementation at the expense of theoretical application and development. This is undoubtedly in part a function of the relative novelty of cyber security as an identifiable field of practice and policy, even if its roots lie in cognate forms of security such as critical infrastructure protection and information security.[34] It is only recently that computer science professionals, for example, have felt it necessary or possible to self-identify as practitioners of cyber security.[35] However, most work on cyber security attempts to be

[31] Tony Reichhardt, 'Harder Than Rocket Science', Nature 435, no. 7045 (2005): 1024-1025.
[32] Latour, Reassembling the Social, 31. These voices include those who study these groups, for whom the characterisation of assemblages as X or Y allows for analysis but obscures the inherently 'fuzzy' boundaries of assemblages so circumscribed.
[33] Johan Eriksson, Johan and Giampiero Giacomello, 'Introduction: Closing the Gap between International Relations Theory and Studies of Digital-Age Security', in Eriksson and Giacomello, International Relations, 2.
[34] The earliest reference to cyber security is probably Stephen B. Furber, VLSI RISC Architecture and Organization (New York: Marcel Dekker, 1989), 298.
[35] Peter J. Denning, 'Who Are We?', Communications of the ACM 44, no. 2 (2001): 15-19; Peter J. Denning and Dennis J. Frailey, 'Who Are We—Now?', Communications of the ACM 54, no. 6 (2011): 25-27.

'problem-solving' rather than 'critical'. It 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.[36]

This perspective dominates security studies in general—a managerial approach informed by 'the desire to "do" security better'.[37] Didier Bigo has observed that despite the intra-disciplinary 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'.[38] 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'.[39] The current enquiry finds affinity with work on cyber security that problematizes security itself rather than leaving its ontological and epistemological foundations unexamined.

Scholars working in the constructivist vein constitute the most developed body of small-'c' critical analyses of cyber security.[40] Constructivism, as one of its earliest proponents in disciplinary International Relations (IR) states, 'complements the Enlightenment belief in the power of language to instantiate reason and qualifies the belief in the power of language to

[36] Robert W. Cox, 'Social Forces, States and World Orders: Beyond International Relations Theory', Millennium: Journal of International Studies 10, no. 2 (1981): 126-155.
[37] Neocleous, Critique of Security, 4.
[38] Didier Bigo, 'The Möbius Ribbon of Internal and External Security(ies)', in Identities, Borders, Orders: Rethinking International Relations Theory, eds. Mathias Albert, David Jacobson and Yosef Lapid (Minneapolis, MN: University of Minnesota Press, 2001), 95.
[39] Dillon, Politics of Security, 18.
[40] On critical theory in IR, see Chris Brown, '"Turtles All the Way Down": Anti-Foundationalism, Critical Theory and International Relations', Millennium: Journal of International Studies 23, no. 2 (1994): 213-236. On critical security studies in IR, see recent discussions in Christopher S. Browning and Matt McDonald, 'The Future of Critical Security Studies: Ethics and the Politics of Security', European Journal of International Relations 19, no. 2 (2013): 235-255; Nik Hynek and David Chandler, 'No Emancipatory Alternative, No Critical Security Studies', Critical Studies on Security 1, no. 1 (2013): 46-63.

represent the world as it is'.[41] 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'.[42] 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. There exists a material reality to which we have partial access through human senses and reason but 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 not denying the ontology of material reality.[43] This post-Kantian distinction between human and world might be unsuitable as a basis for categorical metaphysics[44] but it has proven valuable and influential in IR theory and in security studies.[45]

Constructivist studies of cyber security have drawn upon securitisation theory and related approaches that privilege the constitutive role of language to show how cyber threats are

[41] Nicholas Onuf, 'The Constitution of International Society', European Journal of International Law 5, no. 1 (1994): 1-19.
[42] Emanuel Adler, 'Seizing the Middle Ground: Constructivism in World Politics', European Journal of International Relations 3, no. 3 (1997): 322.
[43] As a meta-theory, constructivism in IR is concerned both with the 'social construction of knowledge' (epistemology) and 'the construction of social reality' (ontology); Stefano Guzzini, 'A Reconstruction of Constructivism in International Relations', European Journal of International Relations 6, no. 2 (2000): 147-182.
[44] Graham Harman, 'I Am Also of the Opinion That Materialism Must Be Destroyed', Environment & Planning D: Society & Space 28, no. 5 (2010): 773.
[45] Theo Farrell, 'Constructivist Security Studies: Portrait of a Research Program', International Studies Review 4, no. 1 (2002), 49-72; Emanuel Adler, 'Constructivism in International Relations: Sources, Contributions, and Debates', in Handbook of International Relations, eds. Walter Carlsnaes, Thomas Risse and Beth A. Simmons, 2nd. edn. (Thousand Oaks, CA: Sage, 2012), 112-144.

constructed through cyber security discourses.[46] Securitisation theory emphasises the sociolinguistic construction of security and is constructivist in its emphasis on identifying 'the processes of constructing a shared understanding of what is considered and collectively responded to as a threat'.[47] Myriam Dunn Cavelty's book, Cyber-Security and Threat Politics (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.[48] It has also served as a valuable historically minded addition to a field compromised by ahistoricism.[49]

[46] Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', Information & Security 7 (2001): 80-103; Johan Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', Journal of Contingencies & Crisis Management 9, no. 4 (2001): 211-222; Ralf Bendrath, 'The American Cyber-Angst and the Real World—Any Link?', in Latham, Bombs and Bandwidth, 49-73; Ralf Bendrath, Johan Eriksson and Giampiero Giacomello, 'From "Cyberterrorism" to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace', in Eriksson and Giacomello, International Relations, 57-82; Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly 53, no. 4 (2009): 1155-1175; Sean Lawson, 'Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States', First Monday 17, no. 7 (2012), n.p.; Sean Lawson, 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats', Journal of Information Technology & Politics 10, no. 1 (2013): 86-103; Myriam Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', International Studies Review 15, no. 1 (2013): 105-122; Sean Lawson, '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, eds. Christopher Laing, Atta Badii and Paul Vickers (Hershey, PA: IGI Global, 2013), 168-188.

[47] Barry Buzan, Ole Wæver and Jaap de Wilde, Security: A New Framework for Analysis (Boulder, CO: Lynne Reinner Publishers, 1998), 26. Securitisation is here allied with constructivism despite its roots in the realist IR tradition, against which constructivism is often opposed. This is justified because securitisation theory does not treat security as an objective condition but as intersubjectively constructed; see Michael C. Williams, 'Words, Images, Enemies: Securitization and International Politics', International Studies Quarterly 47, no. 4 (2003): 511-531.

[48] Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008).

[49] Although see Michael Warner, 'Cybersecurity: A Pre-History', Intelligence & National Security 27, no. 5 (2012): 781-799.

Dunn Cavelty draws attention to the important role of collective knowledge in shaping political outcomes, an approach which draws on the concept of 'epistemic communities'.[50] Grounded in Michel Foucault's formulation of episteme,[51] which John Ruggie describes as 'a dominant way of looking at social reality, a set of shared symbols and references, mutual expectations and a mutual predictability of intention', epistemic communities consist of 'interrelated roles which grow up around an episteme; they delimit, for their members, the proper construction of social reality'.[52] In IR, the concept of epistemic communities has narrowed from Foucault's original conception of a form of social knowledge specific to a particular epoch to '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'.[53] This has clear relevance to cyber security, in which computer scientists and computer security professionals are brought into the policy arena to advise on technical issues. The concept of epistemic community has ordinarily been applied to scientific communities but there is a strong case that 'non-scientific knowledge is just as—if not more—influential as scientific knowledge in influencing policy goals'.[54] We can therefore identify other relevant epistemic communities—political, military, intelligence, media—within the national context and other collectivities organised and acting transnationally.

Together, the epistemic communities of cyber security contribute to an identifiable 'community of practice'. Communities of practice are 'simultaneously "objectified" meanings and discourse that congeal in physical matter' and connote 'activity, as in a state of permanent

[50] John Gerard Ruggie, 'International Responses to Technology: Concepts and Trends', International Organization 29, no. 3 (1975): 557-583; Peter M. Haas, 'Do Regimes Matter? Epistemic Communities and Mediterranean Pollution Control', International Organization 43, no. 3 (1989): 377-403; Peter M. Haas, 'Introduction: Epistemic Communities and International Policy Coordination', International Organization 46, no. 1 (1992): 1-35; Emanuel Adler and Peter M. Haas, 'Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program', International Organization 46, no. 1 (1992): 367-390.

[51] Michel Foucault, The Order of Things: An Archaeology of the Human Sciences (London: Routledge, 2002/1966).

[52] Ruggie, 'International Responses', 569-570, original emphasis.

[53] Haas, 'Introduction', 3.

[54] Mai'a K. Davis Cross, 'Rethinking Epistemic Communities Twenty Years Later', Review of International Studies 39, no. 1 (2013): 148.

becoming; stability within change'.[55] The spread of these communities of security practice is enabled by 'creating alliances, competing for and mobilizing resources and allegiances, and devising interpretations that align interests with negotiated identities—and by the reification of the background knowledge on which practice is based'.[56] As Adler and Pouliot note, these practices in turn structure world politics and security.[57] These communities of practice need not correspond to existing institutional boundaries, 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'.[58] These aggregate entities are 'systems that mix technology, politics, actors in diverse configurations that do not follow given scales or political mappings', identified elsewhere in studies of international politics.[59]

In respect of actors and discourses embedded in and constitutive of assemblages, we cannot neglect the broader Foucauldian conception of the social episteme, the configuration of semiotic and structural elements constitutive of society that allow for the self-imagining of community and society.[60] That is, 'the web of beliefs into which a people are acculturated and through which they perceive the world around them'.[61] Beliefs are often manifest in the ways in which communities imagine themselves and the notion of self-imagination as an essential

[55] Emanuel Adler, '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 (2008): 199.
[56] Ibid., 196.
[57] Emanuel Adler and Vincent Pouliot, 'International Practices', International Theory 3, no. 1 (2011): 1-36.
[58] Rita Abrahamsen and Michael C. Williams, Security Beyond the State: Private Security in International Politics (Cambridge: Cambridge University Press, 2011), 217; also, Rita Abrahamsen and Michael C. Williams, 'Security Beyond the State: Global Security Assemblages in International Politics', International Political Sociology 3, no. 1 (2009): 1-17.
[59] Aihwa Ong, 'Ecologies of Expertise: Assembling Flows, Managing Citizenship', in Ong and Collier, Global Assemblages, 338.
[60] John Gerard Ruggie, 'Territoriality and Beyond: Problematizing Modernity in International Relations', International Organization 47, no. 1 (1993): 157.
[61] Ronald J. Deibert, Parchment, Printing, and Hypermedia: Communication in World Order Transformation (New York: Columbia University Press, 1997), 33.

component of communal identity politics is well-established in international studies.[62] The present study retains this sense but also extends Ruggie's 'mutual predictability of intention' into the related concept of the 'security imaginary'.[63] 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'.[64] For Joelien Pretorius, a security imaginary is not 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'.[65]

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 the community of cyber security practice and within society as a whole. As Pretorius demonstrates, this cultural dimension to security plays an important role in spreading practices and norms of security, such as may be discerned in current attempts to foster a 'global culture of cyber security'.[66] In

[62] For example, Benedict Anderson, Imagined Communities: Reflections on the Origin and Spread of Nationalism, rev. edn. (London: Verso, 2006/1983)
[63] Joelien Pretorius, 'The Security Imaginary: Explaining Military Isomorphism', Security Dialogue 39, no. 1 (2008): 99-120; Sean Lawson, 'Articulation, Antagonism, and Intercalation in Western Military Imaginaries', Security Dialogue 42, no. 1 (2011): 39-56.
[64] Charles Taylor, Modern Social Imaginaries (Durham, NC: Duke University Press, 2004), 23. Also, Arjun Appadurai, Modernity at Large: Cultural Dimensions of Globalization (Minneapolis, MN: University of Minnesota Press, 1996), 31.
[65] Pretorius, 'Security Imaginary', 112.
[66] Myriam Dunn and Victor Mauer, 'Towards a Global Culture of Cyber-Security', in The International CIIP Handbook 2006, vol. 2: Analyzing Issues, Challenges, and Prospects, eds. Myriam Dunn and Victor Mauer (Zurich: Swiss Federal Institute of Technology, 2006), 189-206; Michael Portnoy and Seymour Goodman, 'A Brief History of Global Responses to Cyber Threats', in Global Initiatives to Secure Cyberspace: An Emerging Landscape, eds. Michael Portnoy and Seymour Goodman (New York: Springer, 2009), 5-10.

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', which includes spatial and temporal cognitive biases.[67] These temporal biases are the empirical focus of this thesis.

## 1.3 Time in International Relations

Explicit attention to time and temporality is rare in International Relations and security studies. It is often remarked, for instance, that dominant IR theories are ahistorical, that they fail to account for change in time and ignore the temporal contingency of political phenomena, both in their historical development and in their constant dynamism and renegotiation.[68] These theories have prioritised the spatial over the temporal and reified 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'.[69] This apparent blindness to history and its philosophy inevitably shapes how we understand contemporary politics, particularly in assumptions about progress, destiny and the teleology of nationhood.[70] Even 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 rather than seeing the world as an historical phenomenon in itself.[71] A putative 'historical turn' in IR has prompted more historical reflection but rather than embracing the 'radical uncertainty of historical meaning' or the problematic meaning of

[67] Deibert, Parchment, 33.
[68] Justin Rosenberg, 'The International Imagination: IR Theory and "Classic Social Analysis"', Millennium: Journal of International Studies 23, no. 1 (1994): 85-108.
[69] John Agnew, 'The Territorial Trap: The Geographical Assumptions of International Relations Theory', Review of International Political Economy 1, no. 1 (1994): 53-80.
[70] R.B.J. Walker, 'History and Structure in the Theory of International Relations', Millennium: Journal of International Studies 18, no. 2 (1989): 163-183; R.B.J. Walker, Inside/Outside: International Relations as Political Theory (Cambridge: Cambridge University Press, 1993).
[71] Geoffrey Roberts, 'History, Theory and the Narrative Turn in IR', Review of International Studies 32, no. 4 (2006): 704. Also, John Hobson and George Lawson, 'What is History in International Relations?', Millennium: Journal of International Studies 37, no. 2 (2008): 415-435; George Lawson, 'The Eternal Divide? History and International Relations', European Journal of International Relations 18, no. 2 (2012): 203-226.

history itself has preferred instead to impose its own 'interpretive closure' on the historical record in order to suppress ambiguity and prevent interpretive superabundance.[72]

Important though the renewed emphasis on history is in IR, it is a limited perspective on time, concerned principally with remaking the past in the present, and other aspects of time should also be of interest in international studies. The elision of time by space in IR may be symptomatic of a related tendency elsewhere in the social sciences and humanities to prioritise the study of space.[73] This perhaps reflects Foucault's 1967 assertion that the 'anxiety of our era has to do fundamentally with space, no doubt a great deal more than with time'.[74] One leading sociologist of time has argued that this 'era' was a period during which time was 'consistently theorised out of existence'.[75] Although the subsequent emergence of a 'temporal turn' is questioned,[76] there have been conscious efforts to make time visible in analyses of the contemporary world because time has a 'pervasive role' in modernity that is often left unquestioned, or is predicated upon simplistic and totalising conceptions of time.[77]

This attention to time and temporality has begun to present itself in IR, exemplified by Kimberly Hutchings' analyses of dominant theories of contemporary world politics, which finds them in thrall to temporal assumptions grounded in Western political thought and philosophies of history.[78] Hutchings provides a counter-balance through her advocacy of postcolonial and feminist theories that better reflect the 'heterotemporality' of international

[72] Nick Vaughan-Williams, 'International Relations and the "Problem of History"', Millennium: Journal of International Studies 34, no. 1 (2005): 117.
[73] Robert Hassan, 'Globalization and the "Temporal Turn": Recent Trends and Issues in Time Studies', The Korean Journal of Policy Studies 25, no. 2 (2010): 83-102.
[74] Michel Foucault, 'Of Other Spaces', diacritics 16, no. 1 (1986): 23.
[75] Barbara Adam, '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 (1989): 464.
[76] Helga Nowotny, 'Time and Social Theory: Towards a Social Theory of Time', Time & Society 1, no. 3 (1992): 421-454.
[77] Barbara Adam, Timewatch: The Social Analysis of Time (Cambridge: Polity Press, 1995), 175.
[78] Kimberly Hutchings, 'Happy Anniversary! Time and Critique in International Relations Theory', Review of International Studies 33, supplement S1 (2007): 71-89; Kimberly Hutchings, Time and World Politics: Thinking the Present (Manchester: Manchester University Press, 2008).

life. Andrew Hom also examines the issue of Western temporal 'hegemony' and its constitutive role in international relations and IR theory.[79] Notable too is Ian Klinke's work on the politics of time as a key constituent of critical geopolitics.[80] Klinke's project is a conscious extension and critique of well-known studies in IR and critical geopolitics, including James Der Derian's work on war, information technology, surveillance and the politics of speed.[81] In turn, Der Derian owes much to the voluminous and provocative oeuvre of the French 'philosopher of speed' Paul Virilio.[82] As Klinke notes, analyses of speed do not exhaust the concepts of time and temporality and may fall prey to totalising conceptions of time that should be challenged through more nuanced political and temporal frameworks, the further development of which is a key ambition of this thesis.

In security studies and allied fields, particularly human geography, a vibrant body of critical and interdisciplinary work has emerged that is concerned with the technologies of risk governance, most noticeably in post-9/11 counterterrorism and resilience policies and practices. The concepts of 'pre-emption', 'precaution' and 'prevention' figure large in political discourses on counterterrorism and resilience and this emphasis on futurity has formed a mostly implicit backdrop of temporality to the large number of analyses of these contemporary security issues. Temporality, however, is foregrounded in examinations of how

[79] Andrew R. Hom, 'Hegemonic Metronome: The Ascendancy of Western Standard Time', Review of International Studies 36, no. 4 (2010): 1145-1170. Also, Andrew R. Hom and Brent J. Steele, 'Open Horizons: The Temporal Visions of Reflexive Realism', International Studies Review 12, no. 2 (2010): 271-300; also, Ronald R. Krebs and Aaron Rapport, 'International Relations and the Psychology of Time Horizons', International Studies Quarterly 56, no. 3 (2012): 530-543.

[80] Ian Klinke, 'Chronopolitics: A Conceptual Matrix', Progress in Human Geography 37, no. 5 (2013): 673-690.

[81] James Der Derian, 'The (S)pace of International Relations; Simulation, Surveillance, and Speed', International Studies Quarterly 34, no. 3 (1990): 295-310; James Der Derian, Antidiplomacy: Spies, Terror, Speed and War (Oxford: Blackwell, 1992); James Der Derian, 'Virtuous War/Virtual Theory', International Affairs 76, no. 4 (2002): 771-788; James Der Derian, 'The Question of Information Technology in International Relations', Millennium: Journal of International Studies 32, no. 3 (2003): 441-456; James Der Derian, Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network, 2nd. edn. (New York: Routledge, 2009/2001).

[82] Jef Huysmans, 'James Der Derian: The Unbearable Lightness of Theory', in The Future of International Relations: Masters in the Making?, eds. Iver B. Neumann and Ole Wæver (London: Routledge, 1997), 361-383; James Der Derian, 'The Conceptual Cosmology of Paul Virilio', Theory, Culture & Society 16, nos. 5-6 (1999): 215-227; James Der Derian, 'Paul Virilio', in Critical Theorists and International Relations, eds. Jenny Edkins and Nick Vaughan-Williams (Abingdon: Routledge, 2009), 330-340.

violent acts like 9/11 ruptured historical consciousness[83] and in analyses of how conceptions of time and temporality have informed the prosecution of the subsequent 'war on terror'.[84] Temporality is central to studies of anticipatory governance of the future[85] and in understanding how a paradoxical 'knowledge of the future' is developed in and through security discourses.[86] 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.[87] This sub-field of security studies has not yet turned to cyber security as a topic of interest. Accordingly, the present enquiry is also an attempt to intervene in these discussions of security and temporality.

## 1.4 Approach and Methods

The conceptual framework developed in this enquiry is constructivist in orientation, dealing principally as it does with the relations between cyber security and the politics of time (chronopolitics) as socially constructed fields of knowledge. Specifically, it asks what social conceptions of time inform the security imaginaries that shape cyber security as a political

---

[83] David Campbell, 'Time is Broken: The Return of the Past in the Response to September 11', Time & Event 5, no. 4 (2002), n.p.; Antoine Bousquet, 'Time Zero: Hiroshima, September 11 and Apocalyptic Revelations in Historical Consciousness', Millennium: Journal of International Studies 41, no. 2 (2006): 739-764.

[84] Paul Fletcher, 'The Political Theology of the Empire to Come', Cambridge Review of International Affairs 17, no. 1 (2004): 49-61; Lee Jarvis, 'Times of Terror: Writing Temporality into the War on Terror', Critical Studies on Terrorism 1, no. 2 (2008): 245-262; Kathryn Marie Fisher, 'Exploring the Temporality In/Of British Counterterrorism Law and Lawmaking', Critical Studies on Terrorism 6, no. 1 (2013): 50-72.

[85] Gabe Mythen and Sandra Walklate, 'Terrorism, Risk and International Security: The Perils of Asking "What If?"', Security Dialogue 39, nos. 2-3 (2008): 221-242; Ben Anderson, 'Security and the Future: Anticipating the Event of Terror', Geoforum 41, no. 2 (2010): 227-235; Ben Anderson, 'Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies', Progress in Human Geography 34, no. 6 (2010): 1-22; Liam P.D. Stockdale, 'Imagined Futures and Exceptional Presents: A Conceptual Critique of "Pre-Emptive Security"', Global Change, Peace & Security 25, no. 2 (2013): 141-157.

[86] Claudia Aradau and Rens van Munster, 'Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future', European Journal of International Relations 13, no. 1 (2007): 89-116; Claudia Aradau and Rens van Munster, 'Taming the Future: The Dispositif of Risk in the "War on Terror"', in Risk and the War on Terror, eds. Louise Amoore and Marieke de Goede (London: Routledge, 2008), 23-40.

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

phenomenon. It proposes that social attitudes to time inform political behaviours and examines cyber security as a lens through which to explore this proposition. Unlike the study of space, for which academic geography may make a claim to seniority, the study of time has no central disciplinary core but is the object of interdisciplinary studies across the natural and social sciences, humanities and the arts. The analytical framework reflects this interdisciplinarity, drawing upon a range of theoretical and conceptual resources to develop an understanding of chronopolitics.

This orientation is further justified by the increasing interdisciplinarity of security studies, which, whilst readily identifiable as a sub-discipline of IR or as a parallel field of enquiry, is also a sub-field of social science more generally.[88] Given its complexity, it is perhaps no longer possible to analyse contemporary security fully from within inherited disciplinary bounds, a situation that suggests a presumption to interdisciplinarity.[89] In historical terms, security studies has always been 'a kind of hybrid, interstitial intellectual space' located 'on the borderlands' between diverse disciplines.[90] What has changed is the diversity of disciplines that now take security as a valid object of enquiry, a shift away from fields characterised by positivist epistemologies to those with more interpretivist and post-positivist perspectives on international politics. Attention to the cultural aspects of international relations is an especially fecund development in this intellectual space and the current enquiry finds affinity with this body of work in IR and security studies.

[88] For conflicting views of the relative disciplinary boundaries of IR and (international) security studies, see Stuart Croft, 'What Future for Security Studies', in Security Studies: An Introduction, ed. Paul D. Williams (London: Routledge, 2008), 499-511; Buzan and Hansen, Evolution, 16-19.
[89] Michael C. Williams, 'The New Economy of Security', Global Crime 13, no. 4 (2012): 312-319.
[90] Hugh Gusterson, 'Missing the End of the Cold War in International Security', in Cultures of Insecurity: States, Communities, and the Production of Danger, eds. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall (Minneapolis, MN: University of Minnesota Press, 1999), 320.

The approach taken in this study is neither amenable to a quantitative treatment nor to the application of a positivist methodology.[91] A qualitative perspective on cyber security is adopted that can best be summarised as a constructivist approach with an historical sensibility. Given its prioritisation of historical contingency and the uniqueness of historical context over grand and timeless theory, constructivism is already inherently 'about how the past shapes the ways actors understand their present situation'.[92] These actors include academics as well as the people and collectivities they study and the historical approach employed here is not an attempt to stabilise truth or meaning, except in the sense of making accessible a particular view of the issues under discussion at this particular time. 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 fits within this characterisation of security analysis as 'the critical analysis of the discursive conditions of emergence of contemporary security regimes'.[93]

Even if an authoritative historical account of these issues were desirable, it would not be possible under current conditions. As Stephen Budiansky has remarked of the closely related topic of signals intelligence, the 'practice and craft of history is a document-driven business, and the documents are not available'.[94] The practices of bureaucratic secrecy, document suppression and textual redaction severely impede the ability of historians to reconstruct key periods and processes in the historical development of national security. In the UK, the 'thirty-year rule' effectively embargoes release of many government documents into the public

[91] Although see, Tim Büthe, 'Taking Temporality Seriously: Modeling History and the Use of Narratives as Evidence', American Political Science Review 96, no. 3 (2002): 481-493. For a review of IR methods, see Jef Huysmans and Claudia Aradau, 'Critical Methods in International Relations: The Politics of Techniques, Devices and Acts', European Journal of International Relations, forthcoming.
[92] Dale C. Copeland, 'The Constructivist Challenge to Structural Realism: A Review Essay', International Security 25, no. 2 (2000): 210.
[93] Michael Dillon and Julian Reid, 'Global Liberal Governance: Biopolitics, Security and War', Millennium: Journal of International Studies 30, no. 1 (2001): 51.
[94] Stephen Budiansky, 'What's the Use of Cryptologic History?', Intelligence & National Security 25, no. 6 (2010): 770.

domain until three decades after their creation.[95] Although accessibility to released records has substantially improved under the provisions of the Freedom of Information Act (2000), 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 information about state security from the crucial period of the 1980s onwards is limited for the purposes of public scrutiny and academic study.[96] Often, even documents statutorily made available to the public are selectively redacted, like the annual reports of the Intelligence and Security Committee (ISC).[97]

Historians are often left to concentrate on narrowly defined case studies or classes of non-governmental documents.[98] Alternatively, they may seek official sponsorship to access restricted archives and publish authorised histories.[99] Retired officials draw upon their personal experiences to illustrate key dynamics in recent military and intelligence history, although they are also bound by legal restraint.[100] Those without such an imprimatur 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.[101] Given the classified nature of many cyber security documents that might be of interest to the historically minded researcher, the

[95] This position is articulated in the provisions of the Public Records Act (1958), as amended in 1967. A phased programme beginning in early 2013 will eventually reduce this period to 20 years.
[96] Freedom of Information Act (2000).
[97] On the ISC, see Peter Gill, 'Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the "War on Terror"', Intelligence & National Security 22, no. 1 (2007): 14-37; Andrew Defty, 'Educating Parliamentarians about Intelligence: The Role of the British Intelligence and Security Committee', Parliamentary Affairs 61, no. 4 (2008): 621-641.
[98] For example, Robert Dover and Michael S. Goodman, eds., Learning from the Secret Past: Cases in British Intelligence History (Washington, DC: Georgetown University Press, 2011).
[99] Christopher Andrew, The Defence of the Realm: The Authorized History of MI5 (London: Allen Lane, 2009); Keith Jeffery, MI6: The History of the Secret Intelligence Service (London: Bloomsbury Publishing, 2010); Michael S. Goodman, The Anvil of Discussion: The Official History of the Joint Intelligence Committee (Routledge, forthcoming).
[100] David Pepper, 'The Business of SIGINT: The Role of Modern Management in the Transformation of GCHQ', Public Policy & Administration 25, no. 1 (2010): 85-97; David Omand, Securing the State (London: Hurst & Company, 2010).
[101] An engrossing example of which is Richard J. Aldrich, GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency (London: HarperCollins, 2010).

best available course of action is to attempt to construct historical narratives, rather than authoritative histories, of the topics we find of interest.

The current enquiry follows 'the practice of telling stories about connected sequences of human action', in order that we might help explain the actions in question and 'enhance and extend understanding, comprehension and experience'.[102] In this sense, narration is the 'syntax of commonsense explanation',[103] although theoretical insights from a variety of disciplines will expand and clarify the comprehension of particular issues. This is a pragmatic approach to theory, as outlined in Ken Booth's discussion of Hannah Arendt's Perlenfischerei (pearl-fishing), in which she delved 'beneath the historical surface' for ideas that were 'sea-changed, rich, and strange'.[104] This need not be an excuse for theoretical incoherence, nor for 'epistemological anarchy'.[105] It is instead a method of generating interesting and productive ideas from one's own empirical investigations.[106] The purpose of this theoretically inflected historical approach is to develop a 'synoptic judgment' of the phenomena under examination, 'how it came to be, what it means, and what understanding of it best integrates the available evidence'.[107]

We are fortunate that cyber security is not restricted to secret military and intelligence operations and the proliferation of cyber security texts is remarkable and reflects its multi-faceted character. A substantial corpus is developing of government cyber security policies, national strategies, diplomatic memoranda, military doctrine, commercial reports, trade

[102] Roberts, 'History', 703-704.
[103] Andrew Abbott, Methods of Discovery: Heuristics for the Social Sciences (New York: W.W. Norton & Company, 2004), 33.
[104] Elisabeth Young-Bruehl, Hannah Arendt: For Love of the World (London: Yale University Press, 1984), 95, in Booth, Theory of World Security, 40.
[105] The phrase is usually associated with Paul Feyerabend, Against Method: Outline of an Anarchistic Theory of Knowledge, 3rd. edn. (London: Verso, 1993/1975).
[106] Richard Swedberg, 'Theorizing in Sociology and Social Science: Turning to the Context of Discovery', Theory & Society 41, no. 1 (2011): 1-40. Also, David A. Lake, 'Why "Isms" are Evil: Theory, Epistemology, and Academic Sects as Impediments to Understanding and Progress', International Studies Quarterly 55, no. 2 (2011): 465-480.
[107] Paul W. Schroeder, 'History and International Relations Theory', International Security 22, no. 1 (1997): 68.

journals, media articles, op-eds, multimedia resources, think-tank reports, technical documents, conference proceedings and academic articles and books. Cyber security has rich and complex historical and conceptual relations with a wide range of practices, disciplines and communities, all of which have generated valuable archival resources. Given the diverse range and volume of available sources, both primary and secondary, an historical approach must inevitably concentrate on those texts in which 'something happens'.[108] 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'.[109] 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: only English sources were consulted and the analysis is inevitably oriented to Anglophone cyber security communities, principally in the United Kingdom and United States.

## 1.5 Thesis Structure

The next chapter, Chapter Two, 'Towards a Politics of Time', sets out the conceptual and theoretical foundations of the thesis. It shows how conceptions of time emerge from the physical universe and stresses the importance of sociotemporality as a form of social knowledge about time. This knowledge is not constrained merely to the subjective experience of human time but extends through reason and technology to incorporate the temporalities of nonhuman others like machines and electromagnetism. All social imaginaries are intersubjectively negotiated fields of knowledge that incorporate conceptions of time and space (chronotopes) in their narrative interpretations of reality. With respect to security imaginaries, many different temporal cognitive biases (chronotypes) co-exist within and across

[108] Latour, Reassembling the Social, 133.
[109] Sean Lawson, '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, eds. Christopher Laing, Atta Badii and Paul Vickers (Hershey, PA: IGI Global, 2013), 169.

different communities and inform the narratives through which these 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 concept that underpins the idea of the politics of time (chronopolitics). It is the task of the remainder of the thesis to show how chronopolitics manifests with respect to the practices of cyber security.

Chapter Three, 'Diagnosing the Present', examines how cyber security discourses identify cyber security with a particular reading of the contemporary 'information age'. Cyber security interlocutors frequently cite the characteristics of this periodization of (post)modernity—speed, acceleration, instantaneity—which are dominant modes of framing the threats and opportunities catalysed by global information technologies like the Internet. Whilst 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 alike—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 such 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.

Chapter Four, ‘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 merely as so many make direct reference to end-times scenarios, but 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, such 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 Five, ‘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 like Pearl Harbor and 9/11 are used to provoke political action in the present by analogizing 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, consistent 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 an Hiroshima, cyber security looks to signature events like Pearl Harbor and 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 Six, 'Inhabiting the Future', draws attention to the ways in which cyber security communities attempt to 'inhabit' the future through exercises, simulations, recruitment and education. Inhabitation is meant both in the sense of occupying future scenarios as active participants and as a way to 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 preparation 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 often abstract notions 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 attempt to bring the future into the present by making it comprehensible and 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 their 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.

Chapter Seven, ‘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 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 Eight summarises the contributions of the thesis to the academy and outlines possible avenues for further development and enquiry.

# 2 TOWARDS A POLITICS OF TIME

Time and power are close, and must be,

for what is power but the attempt to control time, buy time, bide time.[1]

## 2.1 Introduction: 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, but 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, most of us give time little serious thought. 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 may be.

This uncertainty as to the nature of time has long been recognised. In third-century Rome, 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'.[2] A century later, Saint Augustine of Hippo would declare, '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'.[3] In our own time, the philosopher Alfred North Whitehead would remark: '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'.[4] These limits are keenly felt by all who would engage with the problem

[1] Jan Nederveen Pieterse, 'Aesthetics of Power: Time and Body Politics', Third Text 7, no. 22 (1999): 33.
[2] Plotinus, The Enneads (Burdett, NY: Larson Publications, 1992), III.vii.1.
[3] Augustine, Confessions (Oxford: Oxford University Press, 1992), XI.xiv (17).
[4] Alfred North Whitehead, The Concept of Nature (Cambridge: Cambridge University Press, 1920), 73.

of time in physics, 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 21st 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.[5] 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.[6] Despite the intellectual, financial, political and material resources harnessed in the search for the Higgs, no scientist working on this quintessentially 'big science' project would be able to tell you definitively if time—as an ontological constituent of reality—exists or not.[7] 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.[8] In English, 'time' is the most common noun, even above 'person', 'thing', 'world' and 'life'.[9] What we perceive 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 civilizational trappings with which we presently identify the human, Palaeolithic man 'awoke to

[5] Paul S. Wesson, 'Time as an Illusion', in Minkowski Spacetime: A Hundred Years Later, ed. Vesselin Petkov (New York: Springer, 2010), 307-318.
[6] CERN, 'New Results Indicate That New Particle is a Higgs Boson', press release, 14 March 2013.
[7] On post-World War II 'big science', see Peter Galison and Bruce Hevly, eds., Big Science: The Growth of Large-Scale Research (Stanford, CA: Stanford University Press, 1992).
[8] Dennett argues that language is a prosthesis 'that permits us to play such glorious tricks with time'; Daniel Dennett, 'Making Tools for Thinking', in Metarepresentations: A Multidisciplinary Perspective, ed. Dan Sperber (New York: Oxford University Press, 2000), 24.
[9] '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.

the predicament of ourselves in time'.[10] Regardless of what we do in life, death marks the finitude of earthly existence and our inherent 'being-towards-death'—in Heidegger's terminology—is the context of all human action.[11] In the words of the religious historian John McManners,

> The knowledge that we must die gives us our perspective for living, our sense of finitude, our conviction of the value of every moment, our determination to live in such a fashion that we transcend our tragic limitation.[12]

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!'[13] 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 desires and interventions. We induce from commonplace observation and the application of no greatly sophisticated reason the greater and uncontroversial truth that time is a fundamental constituent of reality: ontologically, it just is.

[10] Adam Frank, About Time (Oxford: Oneworld, 2011), xviii.
[11] Mike Parker Pearson, The Archaeology of Death and Burial (Stroud: Sutton Publishing, 1999), 142.
[12] John McManners, Death and the Enlightenment: Changing Attitudes to Death Among Christians and Unbelievers in Eighteenth-Century France (Oxford: Oxford University Press, 1981), 2, quoted in ibid., xviii.
[13] Ovid, Metamorphoses, vol. 2 (London: William Heinemann, 1916), 234-236.

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:

> Time felt is the temporal reality of the world interpreted by the older regions of the mind; time understood is articulated by the newer levels of the brain.[14]

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 contemporary societies, and the subjective ('felt') time of human experience ancient and modern, in which tempus fugit 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.[15]

Small wonder 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 thesis. 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. This 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. 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 fight one another about the issue of time as much as postmodernist relativists might 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

[14] J.T. Fraser, Time, Conflict, and Human Values (Urbana, IL: University of Illinois Press, 1999), 40.
[15] J.T. Fraser, 'Time Felt, Time Understood', KronoScope 3, no. 1 (2003): 15.

time.[16] In all cases, how we perceive time is part of the way in which 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 merely 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, befitting a form of security intending to regulate and control the human and nonhuman entities enmeshed in vast sociotechnical assemblages like the Internet.

This chapter develops the argument in six stages. 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. This demonstrates how different forms of temporality correspond to different 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 different temporalities of nonhuman entities and through reason and technology construct a holistic conception of the temporality of the universe. This is an essential step to addressing the temporalities of information technologies, entities with which we cannot directly communicate but the times of which 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', suggesting, in common with

[16] Cornelius Castoriadis, 'Time and Creation', in Chronotypes: The Construction of Time, eds. John Bender and David E. Wellbery (Stanford, CA: Stanford University Press, 1991), 38-64.

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 expression 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.

## 2.2 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'.[17] 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

[17] Fraser, Time, 35.

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.[18] At the same time, 'let us listen to philosophy but not anchor our enquiry there'.[19] 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'.[20]

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. 'The proposition', writes Fraser, '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.[21] Each temporality is emergent from the last and together they comprise a 'nested hierarchy of presents', which are 'the canonical forms of time'. 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.

[18] J.T. Fraser, 'Space-Time in the Study of Time: An Exercise in Critical Interdisciplinarity', KronoScope 5, no. 2 (2005): 151-175.
[19] Fraser, 'Time Felt', 16.
[20] Derek Gjertsen, Science and Philosophy: Past and Present (London: Penguin Books, 1989), 69.
[21] Fraser, Time, 38.

Atemporality, as the name suggests, is the time of no time and consequently of no causation.[22] 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 light speed), no time has passed in the nearly 14 billion years since its apparent creation.[23] 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.[24] As these entities have mass, they cannot travel at the absolute speed of light and must possess temporality, however rudimentary. Prototemporality is the time of events or instants that may be identified statistically but which 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'.[25] Fraser's example of the natural numbers {0, 1, 2, 3, …} illustrates that although eotemporal events (like natural numbers) are successive they do not

[22] Ibid., 38.
[23] Brian Greene, The Elegant Universe: Superstrings, Hidden Dimensions, and the Quest for the Ultimate Theory (London: Jonathan Cape, 1999), 51.
[24] Fraser, Time, 37.
[25] Ibid., 36.

demonstrate a temporal direction.[26] 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.[27] 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 distinction between self and other, and actions are directed to 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'.[28]

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'.[29] Fraser enlists the assistance of Anne Shullenbeger Lévy's luminous description of sociotemporality to illustrate what this consensus might look like:

[26] Natural numbers are the everyday non-negative integers (whole numbers) used for counting and ordering.
[27] Fraser, Time, 36.
[28] Ibid., 35.
[29] Ibid., 37.

> On the one hand [sociotemporality] creates a sense of significant order in the present (which can be either liberating or constraining). On the other hand, it provides protection from oblivion by building historical constructs and chases away the finality of death by conjuring ladders to eternity.[30]

Fraser admits of 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 the individual. In this 'open-ended' schema, there may be a 'higher' level of temporality to 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.[31] We might also question the omission of a chemical or geological temporality, a 'mesotemporality' between eotemporality and biotemporality.[32] 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.[33]

Fraser moves away from Newtonian absolute time as a receptacle of knowable reality into a scientific and philosophical milieu informed by the 20th-century revelations of relativity and quantum mechanics, in which time is relative and mutable and the only constant is the speed of light. This avoids an historical tendency to relegate the times of the non-present to an

[30] Anne Shullenberger Lévy, 'America Discovered a Second Time: French Perceptions of American Notions of Time from Tocqueville to Laboulaye', PhD thesis, Yale University, 1995, quoted in ibid., 38.
[31] See, Jonathan Schaffer, 'Is There a Fundamental Level?', Noûs 37, no. 3 (2003): 498-517. Physical theories of temporal micro-finitism, however, propose various fundamental quanta of time, the existence of which would rather damage this claim.
[32] Bertrand P. Helm, 'Review: J.T. Fraser, Time, Conflict, and Human Values', The Journal of Speculative Philosophy 15, no. 1 (2001): 50-56.
[33] Paul A. Harris, 'Time and Emergence in the Evolutionary Epic, Naturalistic Theology, and J.T. Fraser's Hierarchical Theory of Time', KronoScope 12, no. 2 (2012): 147-158.

unknowable and largely irrelevant prehistory—'a mere run-up to the real thing'.[34] 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'.[35] 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'.[36] Sociotemporality is therefore a constructed temporality—a temporal assemblage—and an assembled form of knowledge.[37] The next section considers in more detail how, if sociotemporality is a form of knowledge, we humans can know these other temporalities, each peculiar to the entities existing at the six organisational levels of nature.

## 2.3 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 political phenomena—the answer lies in understanding the environment in which cyber security operates and which it intends to regulate. Most cyber security discourses are

[34] Robin Fox, 'Time Out of Mind: Anthropological Reflections on Temporality', KronoScope 1, nos. 1-2 (2001): 129.
[35] Adrian Mackenzie, Transductions: Bodies and Machines at Speed (London: Continuum, 2002), 9.
[36] Ian Hacking, The Social Construction of What? (Cambridge, MA: Harvard University Press, 1999), 49.
[37] Given the common identification of 'assemblage' with 'postmodern' theory, the affinity between Fraser's distinctly modern approach and assemblage theory supports the thesis that assemblage theory 'evokes conditions under modernist theoretical influences with structural allusions', not a characterisation it often admits of itself; George E. Marcus and Erkan Saka, 'Assemblage', Theory, Culture & Society 23, nos. 2-3 (2006): 106.

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 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 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. Cyber security is not merely 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 suggests that nonhuman temporalities are inherently subsumed within the temporalities of politics, which provides a fresh opportunity to understand the political linkages between human and machine.

It is inadequate to assert that man 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). Although von Uexküll did not invent the term Umwelt, he redefined its modern connotation of an animal's perceptual life-world.[38] For Uexküll, the umwelt is the subjective spatio-temporal world particular to living creatures as diverse as the burrowing worm, the butterfly and the

[38] Geoffrey Winthrop-Young, '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 (Minneapolis, MN: University of Minnesota Press, 2010), 215. On account of its naturalisation into English, the German capitalisation is dispensed with and lower case is used hereon.

field mouse.[39] All animals inhabit their individual phenomenological sense-worlds in which meaning and significance are derived subjectively by that animal alone. Significantly, the animal umwelt is 'the world as it appears to the animals themselves, not as it appears to us'.[40] Although Uexküll was influenced by a Kantian understanding of reality as a phenomenon revealed through the human mind, he expanded this to include reality revealed through the body and to the nonhuman animal.[41] 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'.[42]

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'.[43] 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. Although we cannot directly experience the umwelts of photons or celestial bodies, we can begin to know the worlds of other species and material bodies such that they become part of our own 'noetic umwelt', in which 'noetic' pertains to the human mind or nous.[44] This is achievable through the double extension of human senses: first, by dint of our cognitive abilities and the application of reason and theory and, second, through indirect interrogation by technological instrumentation and

[39] Jakob von Uexküll, 'A Stroll Through the Worlds of Animals and Men: A Picture Book of Invisible Worlds', in Instinctive Behavior: The Development of a Modern Concept, ed. Claire H. Schiller (New York: International Universities Press, 1957/1934), 5-80.
[40] Ibid., 5.
[41] Aldona Pobojewska, 'New Biology—Jakob von Uexküll's Umweltlehre', Semiotica 134, nos. 1-4 (2001): 323-339.
[42] Giorgio Agamben, The Open: Man and Animal (Stanford, CA: Stanford University Press, 2004/2002), 39.
[43] Jane Bennett, 'A Vitalist Stopover on the Way to a New Materialism', in New Materialisms: Ontology, Agency, and Politics, eds. Diana Coole and Samantha Frost (Durham, NC: Duke University Press, 2010), 48.
[44] Fraser, Time, 25.

other material tools.[45] This second category we may understand as technical orthoses, artefacts that supplement or extend human capabilities.[46] 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.[47]

Of this extensibility of the human experience, Martin Heidegger, also influenced by Uexküll,[48] wrote:

> … the world of man is a rich one, greater in range, far more extensive in its penetrability, constantly extendable not only in its range …. but also in respect to the manner in which we can penetrate ever more deeply in this penetrability.[49]

Heidegger thereby characterised man as 'world-forming' (weltbildend), against the animal that is 'poor in world' (weltarm) and the material object such as the stone, that is 'worldless' (weltlos). Heidegger defines 'world' as having access to beings outside the subject. The stone has no world as it has no way of accessing external beings, unlike 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'.[50] As the novelist J.M. Coetzee writes, for animals, 'their whole being is in the living flesh'.[51] In this Heideggerian formulation, the animal is deprived of aspects of the world and is therefore 'poor in world'. The human

---

[45] Fraser, Time, 24-25; J.T. Fraser, 'The Extended Umwelt Principle: Uexküll and the Nature of Time', Semiotica 134, nos. 1-4 (2001): 263-273.
[46] Roger Clarke, 'Cyborg Rights', IEEE Technology & Society Magazine 30, no. 3 (2011): 49-57.
[47] Donna Haraway, 'A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century', Simians, Cyborgs and Women: The Reinvention of Nature (New York: Routledge, 1991), 150.
[48] Brett Buchanan, Onto-Ethologies: The Animal Environments of Uexküll, Heidegger, Merleau-Ponty, and Deleuze (Albany, NY: State University of New York Press, 2008).
[49] Martin Heidegger, The Fundamental Concepts of Metaphysics: World, Finitude, Solitude (Bloomington, IN: Indiana University Press, 1995/1929-1930), 193.
[50] Ibid., 198.
[51] J.M. Coetzee, The Lives of Animals (Princeton, NJ: Princeton University Press, 1999), 65.

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'.[52]

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,[53] 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 our purpose all that is necessary and sufficient is to have established a working concept of reality—the extended umwelt principle—and to note that as our knowledge of the world expands, so does our reality. This amounts to equating epistemology with ontology; the world is the way we find it to be through the many forms of human knowledge[54]

Although left unstated, this is a constructivist perspective in which intersubjective epistemology assumes ontological importance in social reality. Knowledge is not communicated to the senses in unmediated fashion but must be actively constructed by the cognising subject. Fraser maintains the Kantian precept that the subject has no direct access to

[52] Ibid.
[53] Fraser, Time, 23.
[54] Fraser, Time, 25.

external reality, whilst not denying the probable existence of that reality or the material origins of the human mind.[55] Although we cannot know directly the temporalities of neutrons or narwhals, 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.[56] 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.

## 2.4 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. We encounter 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:

[55] The extent to which Kant is constructivist or not is moot. See, Paul Formosa, 'Is Kant a Moral Constructivist or a Moral Realist?', European Journal of Philosophy 21, no. 2 (2013): 170-196.
[56] Fraser, Time, 34. Fraser acknowledges that in practice there may be little difference between noetic time and sociotemporality; ibid, 68. For the purposes of clarity, sociotemporality is preferred here.

> 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'.[57]

Heraclitus' emphasis on the perpetual Becoming of the cosmos has been glossed through the centuries as 'everything flows' (Gr. panta rhei)[58] and has greatly influenced subsequent thinkers.[59] Marcus Aurelius would write in the second century AD:

> 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.[60]

Philosophers have long recognised the problems of using metaphors of spatial mobility to describe time.[61] As Arthur Prior notes: 'Time may be […] like an ever-rolling stream, but it isn't really and literally an ever-rolling stream'.[62] 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'.[63] Time, like the language that expresses it, is 'tensed' and events and processes have locations—past, present, future—in time.[64] Moreover, these tenses portend the deeper apparent truth that time passes in one direction

---

[57] Francesco Ademollo, The Cratylus of Plato: A Commentary (Cambridge: Cambridge University Press, 2011), 203.
[58] F.E. Peters, Greek Philosophical Terms: A Historical Lexicon (New York: New York University Press, 1967), 178.
[59] Nietzsche remarked that in Heraclitus, 'I must recognise him who has come nearest to me in thought hitherto'; Friedrich Nietzsche, Ecce Homo (New York: Macmillan, 1911/1888), 73. On Heraclitus' influence on Nietzsche, Heidegger and others, see Joanne B. Waugh, 'Heraclitus: The Postmodern Presocratic?', The Monist 74, no. 4 (1991): 605-623.
[60] Marcus Aurelius, Meditations (London: Penguin Books, 2006), IV.43.
[61] Donald C. Williams, 'The Myth of Passage', The Journal of Philosophy 48, no. 15 (1951): 457-472. Also, Daniel Casasanto and Lera Boroditsky, 'Time in Mind: Using Space to Think about Time', Cognition 106, no. 2 (2008): 579-593.
[62] Arthur N. Prior, 'Changes in Events and Changes in Things', in The Philosophy of Time, eds. Robin Le Poidevin and Murray MacBeath (Oxford: Oxford University Press, 1993), 35. Prior alludes to Isaac Watts' paraphrasis of Psalm 90 in his hymn, 'Our God, Our Help in Ages Past': 'Time, like an ever-rolling stream/Bears all its sons away/They fly, forgotten as a dream/Dies at the opening day'.
[63] Prior, 'Changes', 35.
[64] Etymologically, 'time' and 'tense' both derive from the Latin tempus (time). The three tenses—past, present and future—have much older histories; Robert I. Binnick, Time and the Verb: A Guide to Tense and Aspect (New York: Oxford University Press, 1991).

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.[65] 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 such 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 writing,

> 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.[66]

All moments are therefore supposed to possess all temporal properties (pastness, presentness, futurity) but no moment can actually co-instantiate all these mutually exclusive properties, leading to the philosophical conclusion that this is an absurd proposition and

[65] Arthur S. Eddington, The Nature of the Physical World (New York: Macmillan, 1928), 69. Strictly speaking, the 'arrow' points towards increased entropy which, if it could be reversed in time, would mean the arrow would point to the past from our current perspective. However, as time itself would be reversed in so doing, and us with it, the arrow would still point to the future.
[66] T.S. Eliot, 'Burnt Norton', Four Quartets (San Diego, CA: Harvest, 1971/1943), I.1-5.

tenses are unreal.[67] The problem of tense is the foundation for J.M.E. McTaggart's famous deduction from logical principles that time too must be unreal.[68]

Metaphysical discussions over the unreality of tense and time aside, the nature of the present and what constitutes the 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 generalizable. 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.[69] This perturbed Einstein greatly, Rudolf Carnap reporting that,

> [Einstein] explained that the experience of the Now means something special for man, something essentially different from the past and the future, but that this important difference does not and cannot occur within physics. That this experience cannot be grasped by science seemed to him a matter of painful but inevitable resignation … there is something essential about the Now which is just outside the realm of science.[70]

It is unlikely that any scientific resolution to the issue of the nature of nowness is forthcoming. As the philosopher of physics Simon Saunders observes, 'the meaning of time has become

---

[67] D.H. Mellor, 'The Unreality of Tense', in Poidevin and MacBeath, Philosophy of Time, 51.
[68] J.M.E. McTaggart, 'The Unreality of Time', Mind: A Quarterly Review of Psychology & Philosophy 17, no. 4 (1908): 457-474. McTaggart's argument is more complex and extensive than this and the single issue of tense is presented here for illustrative purposes only. I mean no insult to his original thesis, unlike C.D. Broad, who described it as a philosophical 'howler'; C.D. Broad, An Examination of McTaggart's Philosophy, vol. 2, part 1 (Cambridge: Cambridge University Press, 1938), 316.
[69] Barry Dainton, Time and Space, 2nd. edn. (Durham: Acumen, 2010/2001), 324-327.
[70] Rudolf Carnap, 'Intellectual Autobiography', in The Philosophy of Rudolf Carnap, ed. Paul Arthur Schilpp (LaSalle, IL: Open Court, 1963), 37-38, originally quoted in Julian Barbour, The End of Time: The Next Revolution in Our Understanding of the Universe (London: Phoenix, 2000), 143.

terribly problematic … The situation has become so uncomfortable that by far the best thing is to declare oneself an agnostic'.[71]

Modern philosophers have been less reticent in asserting the nature of nowness and in exploring it from multiple perspectives, a review of which is beyond the scope of the present enquiry. However, 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 hold that passage involves a special property of 'presentness' moving along the timeline. Others explain passage in terms of the non-existence of the future: only the past and present are real …. Others deny reality to both the past and the future: time consists of a succession of ephemeral presents.[72]

The Heraclitean, presentist view of temporal passage and Becoming is rejected by eternalists, who subscribe to a static universe in which 'all moments of time (and all events) are equally real, and there is no moving or changing present; nothing becomes present and then ceases to be present'.[73] 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'.[74] Although the details of Parmenides' argument—in which he denied the logical possibility of change and therefore of an ultimate cause of Creation—are often considered absurd, his proposition has become 'the historical symbol of a negative emotional

[71] Tim Folger, 'Newsflash: Time May Not Exist', Discover Magazine, June 2007.
[72] Dainton, Time and Space, 7.
[73] Ibid.
[74] John Burnet, Early Greek Philosophy, 4th. edn. (London: Adam and Charles Black, 1930/1892), 174-175.

attitude toward the flow of time'.[75] This image of a 'block universe' holds that 'the future is just as real, solid and immutable as the past', and in its temporal determinism has serious consequences for the possibilities of free will.[76]

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'.[77] 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'.[78] Henri Bergson, too, 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.[79] Husserl would pursue 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.[80]

Like Bergson, Husserl dispensed with notions of a 'specious present' 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.[81] Deeply influenced by Husserl, Heidegger would reject the priority granted the present in 'vulgar' conceptions of time,

---

[75] Hans Reichenbach and Maria Reichenbach, The Direction of Time (Berkeley, CA: University of California Press, 1956), 6.
[76] Dainton, Time and Space, 9.
[77] Whitehead, Concept of Nature, 72-73.
[78] Ibid., 72.
[79] Henri Bergson, Time and Free Will: An Essay on the Immediate Data of Consciousness, 3rd. edn. (Mineola, NY: Dover Publications, 2001/1913).
[80] Edmund Husserl, The Phenomenology of Internal Time-Consciousness, ed. Martin Heidegger (The Hague: Martinus Nijhoff, 1964/1928).
[81] Alfred Gell, The Anthropology of Time: Cultural Constructions of Temporal Maps and Images (Oxford: Berg, 1992), 223. On the conceptual origins of the 'specious present', see Holly K. Andersen and Rick Grush, 'A Brief History of Time-Consciousness: Historical Precursors to James and Husserl', Journal of the History of Philosophy 47, no. 2 (2009): 277-307.

preferring instead a conception of phenomenological (and finite) time as a unity of past, present and future.[82] 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'.[83] This unitary experience manifests in a 'moment of vision' (Augenblick), a singular and ecstatic temporality that constitutes and gives meaning to Being itself.[84] 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'.[85] The concept of duration is maintained into the social present and connotes the 'amount of time needed for coordinating collective action'.[86] 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 consensuses to emerge that enable 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

[82] Martin Heidegger, Being and Time, rev. edn. (Albany, NY: State University of New York Press, 2010/1927).
[83] Koral Ward, Augenblick: The Concept of the 'Decisive Moment' in 19th- and 20th-Century Philosophy (Aldershot: Ashgate Publishing, 2008), 100.
[84] Ibid., 101.
[85] Fraser, Time, 35; also, J.T. Fraser, 'Human Temporality in a Nowless Universe', Time & Society 1, no. 2 (1992): 159-173.
[86] Fraser, Time, 35.

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. As we have previously observed, 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. Embedded within it is its own genealogy—the stories of science and philosophy, of myth 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.

## 2.5 Temporality and Narrative

In the 1930s, Mikhail Bakhtin introduced the concept of the 'chronotope' into literary criticism and the philosophy of language.[87] 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 to stand for 'the intrinsic connectedness of temporal and spatial relationships that are artistically expressed in literature'.[88] 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

[87] Mikhail Bakhtin, 'Forms of Time and of the Chronotope in the Novel: Notes Towards an Historical Poetics', in The Dialogic Imagination: Four Essays by M.M. Bakhtin, ed. Michael Holquist (Austin, TX: University of Texas Press, 1981/1937-1938), 84-258.
[88] Ibid., 84.

movements of time, plot and history'.[89] Bakhtin's subsequent analysis shows how chronotopes infuse and structure diverse genres of the novel; indeed, Bakhtin proposes that chronotopes determine genre. Although many chronotopes may co-exist in any text, narratives tend to be dominated by single chronotopes, which act as 'organizing centers' around which 'the knots of narrative are tied and untied'.[90] Dominant chronotopes are stabilised and stabilising cognitive representations of spatiotemporal reality that construct meaning and shape narrative.

Illustrating that it is not just the writer of fiction that may draw inspiration in such fashion, Bakhtin's analysis is influenced by the notion of 'spacetime' developed in early 20th-century physics. In 1908, 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'.[91] 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.[92]

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'.[93] Taking a direct cue from Kant's notions of space and time as transcendental of human

[89] Ibid.
[90] Ibid., 250.
[91] Hermann Minkowski, 'Space and Time', in Minkowski Spacetime: A Hundred Years Later, ed. Vesselin Petkov (New York: Springer, 2010), xv.
[92] Bakhtin attributes 'spacetime' to Einstein but it was Minkowksi that radicalised Einstein's 1905 formulation of special relativity and formalised 'spacetime'; only later did spacetime re-emerge in Einstein's work on general relativity.
[93] Bakhtin, 'Forms of Time', 84; Luis Alberto Brandão, 'Chronotope', Theory, Culture & Society 23, nos. 2-3 (2006): 133-134.

experience,[94] 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.[95] Bakhtin 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.[96] As Einstein himself would remark a few years later, 'time and space are modes by which we think and not conditions in which we live'.[97]

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'.[98] 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.[99] 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.[100]

---

[94] Immanuel Kant, Critique of Pure Reason (Cambridge: Cambridge University Press, 1998/1781/1787): 153-192.
[95] Michael Holquist, 'The Fugue of Chronotope', in Bakhtin's Theory of the Literary Chronotope: Reflections, Applications, Perspectives, eds. Nele Bemong, Pieter Borghart, Michel de Dobbeleer, Kristoffel Demoen, Koen de Temmerman and Bart Keunen (Ghent: Ginkgo Academia Press, 2010), 19-33.
[96] Gary Saul Morson and Caryl Emerson, Mikhail Bakhtin: Creation of a Prosaics (Stanford, CA: Stanford University Press, 1990), 254.
[97] Aylesa Forsee, Albert Einstein: Theoretical Physicist (New York: Macmillan, 1963), 81, quoted in John Archibald Wheeler, 'The Computer and the Universe', International Journal of Theoretical Physics 21, nos. 6-7 (1982): 559.
[98] Frank, About Time, 9.
[99] Karen Barad, Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning (Durham, NC: Duke University Press, 2007).
[100] Helge S. Kragh, Conceptions of the Cosmos—From Myths to the Accelerating Universe: A History of Cosmology (Oxford: Oxford University Press, 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.[101] 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.[102] 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'.[103] 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, including the source materials interrogated in the current investigation.[104] 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'.[105] 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

[101] Ibid.
[102] Katerina Clark and Michael Holquist, Mikhail Bakhtin (Cambridge, MA: Harvard University Press, 1984), 279.
[103] Frank, About Time, 10.
[104] Stuart Allan, '"When Discourse is Torn From Reality"': Bakhtin and the Principle of Chronotopicity', Time & Society 3, no. 2 (1994): 211.
[105] Ian Klinke, 'Chronopolitics: A Conceptual Matrix', Progress in Human Geography 37, no. 5 (2013): 680.

always already a political move'.[106] It is also deeply interlaced with the politics of space, as Bakhtin's original merging of chronos and topos suggests. Haraway summarises this complex relationship and the importance of Bakhtin's insights to contemporary politics:

> Like both place and space, time is never 'literal', just there; chronos always intertwines with topos …. Time and space organize each other in variable relationships that show any claim to totality, be it the New World Order, Inc., the Second Millennium, or the modern world, to be an ideological gambit linked to struggles to impose bodily/spatial/temporal organization. Bakhtin's concept requires us to enter the contingency, thickness, inequality, incommensurability, and dynamism of cultural systems of reference through which people enrol each other in their realities.[107]

This reminds us that although we may concentrate on time in our enquiries, 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.[108] 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.[109] Our discussion turns to the relations between politics and this sociotemporal present and characterises the temporality in which politics is situated.

---

[106] Ibid., 686.
[107] Donna J. Haraway, Modest Witness@Second_Millennium. FemaleMan©_Meets_OncoMouse™: Feminism and Technoscience (New York: Routledge, 1997), 41-42.
[108] Barbara Adam, 'Of Timescapes, Futurescapes and Timeprints', paper presented at Lüneberg University, 17 June 2008.
[109] On the need to 'overcome' the time/space dichotomy, see Doreen Massey, 'Politics and Space/Time', New Left Review 196 (1992): 65-84; Jon May and Nigel Thrift, 'Introduction', in Timespace: Geographies of Temporality, eds. Jon May and Nigel Thrift (London: Routledge, 2001), 1-46.

## 2.6 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:

> we now have to divide up our time […] between politics and our equations. But to me our equations are far more important, for politics are only a matter of present concern. A mathematical equation stands forever.[110]

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 have always been equated with the temporal, not just in the sense of being somehow 'of time' but as temporary and transient. Politics are differentiated from the more profound realms of science and spirit and the enduring truths encountered therein. The members of the upper house of the British parliament are formally divided between two estates of the Realm: 'Lords Spiritual'—the 26 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.[111] 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.[112] 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'.[113] In this tradition, the political

[110] Robert Jungk, Brighter Than a Thousand Suns: The Moral and Political History of the Atomic Scientists (London: Victor Gollancz, 1958/1956), 243.
[111] House of Lords, Companion to the Standing Orders of and Guide to the Proceedings of the House of Lords, 22nd. edn. (Norwich: The Stationery Office, 2010/1862), 13. Also, Luke Owen Pike, A Constitutional History of the House of Lords (London: Macmillan and Co., 1894), esp. pp. 151-168.
[112] See, Roland J. Teske, 'William of Auvergne on Time and Eternity', Traditio 55 (2000): 125-141.
[113] Paul Weithman, 'Augustine's Political Philosophy', in The Cambridge Companion to Augustine, eds. Eleonore Stump and Norman Kretzmann (Cambridge: Cambridge University Press, 2001), 237.

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; 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'.[114] Politics 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 Western philosophers distinguished between chronos, the quantifiable and measurable time of the cosmos, and kairos, the qualitative time of lived human experience.[115] Although Cornelius Castoriadis warns against adopting wholesale such 'old-fashioned and platitudinous' dichotomies,[116] the distinction between chronos and kairos does retain heuristic value and analytical utility due to its persistence in discussions of time and politics, justification enough for its inclusion here. The classical expression of chronos is found in Aristotle's Physics, in which chronotic time is defined—perhaps rather circuitously—as 'a number of change in respect of before and after; and because it is a number of something continuous, it is continuous itself'.[117] Before Aristotle, Plato conceived of chronos as the

[114] Andrew Heywood, Key Concepts in Politics (Basingstoke: Palgrave Macmillan, 2000), 33.
[115] John E. Smith, 'Time, Times, and the "Right Time"; Chronos and Kairos', The Monist 53, no. 1 (1969): 1-13; John E. Smith, 'Time and Qualitative Time', The Review of Metaphysics 40, no. 1 (1986): 3-16.
[116] Castoriadis, 'Time and Creation', 38-39.
[117] Aristotle, Physics (Oxford: Oxford University Press, 1996), IV.11.219b.

universal clock, 'not mere succession or duration but a standard by which duration can be measured'.[118]

Since Newton in the late 17th 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 man and measurement. Newton proposed an 'absolute space' independent of matter, which existed in 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 time: 'Absolute, True, and Mathematical Time, of itself, and from its own nature flows equably without regard to any thing external'.[119] In the Newtonian universe, nothing in the material universe could alter or otherwise perturb the 'flow of time'.

In contrast, Aristotelian kairos is 'the time that gives value', and other ancient Greek philosophers conferred upon kairos the qualities of 'exact time, critical time, season, or opportunity'.[120] Smith summarises the essential features of kairos as timing, tension and opportunity.[121] 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,

[118] W.K.C. Guthrie, A History of Greek Philosophy, vol. 5: The Later Plato and the Academy (Cambridge: Cambridge University Press, 1978), 300.
[119] Isaac Newton, The Mathematical Principles of Natural Philosophy, vol. 1 (London: Benjamin Motte, 1729), 9. This is often held as proof of Newton's conception of time as antithetical to 20th-century relativity but he preceded it by noting the 'Relative, Apparent, and Common Time' of the everyday observer, which has many similarities to time in a relativistic universe.
[120] Hans Rämö, 'An Aristotelian Human Time-Space Manifold: From Chronochora to Kairotopos', Time & Society 8, no. 2 (1999): 312.
[121] Smith, 'Time and Qualitative Time', 10-11.

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'.[122] Kimberly Hutchings summarises well the fundamental difference between these concepts of time:

> The qualitative distinction is, essentially, one between time being understood as the medium (a common, reliable and regular, context in which and through which objects exist and events take place, but which is distinct from those objects and events) and time being understood as the message (a creative force in its own right, intervening in relation to objects and events, rather than operating as a neutral medium).[123]

Chronos and kairos are not, however, ontologically exclusive temporalities, and the two are not easily divorced. Smith contends that 'kairos presupposes chronos which is thus a necessary condition underlying qualitative times'.[124] 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'.[125] Like Newtonian time—the temporal dimension of the divine sensorium—chronos is the basis for the existence of kairos, indeed 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 offers kairos as, in part, the time of human political action. The temporality of kairotic politics can be further disassembled through

[122] Ward, Augenblick, xii.
[123] Kimberly Hutchings, Time in World Politics: Thinking the Present (Manchester: Manchester University Press, 2008), 25.
[124] Smith, 'Time and Qualitative Time', 6.
[125] Giorgio Agamben, The Time That Remains: A Commentary on the Letter to the Romans (Stanford, CA: Stanford University Press, 2005/2000), 69.

considerations of duration, tempo, acceleration and timing, which allow for finer-grained analyses of how politics operates in this temporal register.[126]

Time is not merely the cosmic vessel within which we recognise tense and measure the passing of human lives and societies. The 20th-century revelations 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.[127] As the narrator of a Marcel Aymé 1943 short story suggests, it 'became obvious that the notion of time, as our ancestors had transmitted it down the millennia, was in fact absurd claptrap'.[128] 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.[129] 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.[130] Modern science has irrevocably

[126] Anna Grzymala-Busse, 'Time Will Tell? Temporality and the Analysis of Causal Mechanisms and Processes', Comparative Political Studies 44, no. 9 (2011): 1267-1297. Also, Donald F. Miller, 'Political Time: The Problem of Timing and Chance', Time & Society 2, no. 2 (1993): 179-187.

[127] Peter Galison, Einstein's Clocks, Poincaré's Maps: Empires of Time (New York: W.W. Norton & Company, 2003), 236-237.

[128] Marcel Aymé, 'The Problem of Summertime', in The Man Who Walked Through Walls (London: Pushkin Press, 2012/1943), 109.

[129] Although not quite arguing that what we call 'time' does not exist, as is often reported, Julian Barbour presents a strong challenge to the received interpretation of time as a fundamental dimension of the universe; Barbour, The End of Time.

[130] Galison, Einstein's Clocks, 42, 47. This convergence has led to a tension between physics, philosophy and the experience of time that has barely been addressed; Levi Bryant, Nick Srnicek and Graham Harman, 'Towards a Speculative Philosophy', in The Speculative Turn: Continental Materialism and Realism, eds. Levi Bryant, Nick Srnicek and Graham Harman (Melbourne: re.press, 2011), 17.

altered how we must view time, even as we should be cautious of attempting to impose scientific ontologies on the social world.[131]

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'.[132] The incarcerated Martin Luther King wrote similarly in 1963, 'time itself is neutral; it can be used either destructively or constructively'.[133] Time is not the silent background before 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 rubric of sociotemporality.

Sociotemporality is the temporal umwelt that corresponds to the level of collective social entities and 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'.[134] 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.[135]

---

[131] Patrick Thaddeus Jackson, The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics (London: Routledge, 2011), 26-32. In time studies, see Eric Kincanon, 'Misuses of Physical Models in Understanding Time', KronoScope 4, no. 1 (2004): 70-73.
[132] Peter G. Tsouras, ed., The Greenhill Dictionary of Military Quotations (London: Greenhill Books, 2000), 479.
[133] Martin Luther King, Jr., 'Letter from Birmingham Jail', University of California Davis Law Review 26, no. 4 (1993): 843.
[134] Frederick F. Schmitt, '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., 1994), 1.
[135] Alvin I. Goldman, Knowledge in a Social World (Oxford: Oxford University Press, 1999); Steve Fuller, Social Epistemology, 2nd. edn. (Bloomington, IN: Indiana University Press, 2002/1988).

> [Social epistemology] encompasses an interwoven set of historically contingent intersubjective mental characteristics, ranging from spatial or temporal cognitive biases, to shared symbolic forms, to various group identities, or to 'imagined communities' […] which are unique to a specific historical context, and differentiate one epoch from another.[136]

With respect to the 'temporal cognitive biases' 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.[137] Whilst stressing sociotemporal heterogeneity within the human species, this extensive body of work posits a general understanding that conceptions of time are fundamental to collective self-understanding and social organisation. This baseline assumption has been challenged recently by studies of Amazonian social groups whose languages lack tenses and other linguistic constructions indicative of such a universal grammar of time.[138] That these conceptions of temporality are often culture- or language-specific is illustrated by the difficulties experienced by those learning second languages in accessing the subtleties and idioms of temporality embedded in those other languages.[139] Not being able 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

---

[136] Ronald J. Deibert, Parchment, Printing, and Hypermedia: Communication in World Order Transformation (New York: Columbia University Press, 1997), 33. Also, Ronald J. Deibert, 'Harold Innis and the Empire of Speed', Review of International Studies 25, no. 2 (1999): 273-289.

[137] Gell, Anthropology of Time; Nancy D. Munn, 'The Cultural Anthropology of Time: A Critical Essay', Annual Review of Anthropology 21 (1992): 93-123.

[138] Daniel L. Everett, 'Cultural Constraints on Grammar and Cognition in Pirahã', Current Anthropology 46, no. 4 (2005): 621-646; Chris Sinha, Vera da Silva Sinha, Jörg Zinken and Wany Sampaio, 'When Time is Not Space: The Social and Linguistic Construction of Time Intervals and Temporal Event Relations in an Amazonian Culture', Language & Cognition 3, no. 1 (2011): 137-169.

[139] Rainer Dietrich, Wolfgang Klein and Colette Noyau, The Acquisition of Temporality in a Second Language (Amsterdam: John Benjamins Publishing Company, 1995).

of temporality to convey 'important social messages' of similarity and difference within both interpersonal relations and societal politics.[140]

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'.[141] This prefigures Helga Nowotny's later idea that everyone is 'a practician and theoretician of time'.[142] Stressing the socially constructed aspect of temporality, time is not given but 'fabricated in an ongoing process'.[143] Moreover, as Bakhtin might have said:

> Chronotypes are themselves temporal and plural, constantly being made and remade at multiple individual, social, and cultural levels. They interact with one another, sometimes cooperatively, sometimes conflictually. They change over time and therefore have a history or histories, the construal of which itself is an act of temporal construction.[144]

Chronotypes are not 'produced ex nihilo; they are improvised from an already existing repertoire of cultural forms and natural phenomena'; the 'social and cultural processes of temporal construction rely on and also reelaborate antecedent rhythms and articulations'.[145] 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'.[146] Socially constructed and historicised notions of time are open to refutation, contestation and

---

[140] Eviatar Zerubavel, 'The Language of Time: Toward a Semiotics of Temporality', The Sociological Quarterly 28, no. 3 (1987): 343-356.
[141] John Bender and David E. Wellbery, 'Introduction', in Bender and Wellbery, Chronotypes, 4.
[142] Helga Nowotny, Time: The Modern and Postmodern Experience (Cambridge: Polity Press, 1994), 6.
[143] Bender and Wellbery, 'Introduction', 4.
[144] Ibid. Bakhtin wrote: 'Chronotopes are mutually inclusive, they co-exist, they may be interwoven with, replace or oppose one another, contradict one another or find themselves in ever more complex relationships', Bakhtin, 'Forms of Time', 252.
[145] Bender and Wellbery, 'Introduction', 4, 15.
[146] Ibid., 15.

resistance, and recognition of the potential for conflict between sociotemporal chronotypes is at the heart of chronopolitics.

## 2.7 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, 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.[147]

[147] Charles S. Maier, '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. Maier (Cambridge: Cambridge University Press, 1987), 151-152.

There always exists a politics of time because those or govern or desire to do so will always advance their own visions of how society should 'reproduce itself through time'.[148] 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.[149]

Johannes Fabian demonstrates how temporal narratives construct the Other through the anthropological 'denial of coevalness' between cultures—'I am modern, you are not'—instantiating webs of powerfully asymmetric social relations.[150] To travel to a society under such 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.[151] Least this be thought purely a relic of Western colonialism and Kantian cosmopolitanism, these discourses operate even in 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 pre-modern rules of social and political organisation that are 'out of time' with respect to its geopolitical neighbours.[152]

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

---

[148] Ibid., 152.
[149] Ibid. Also, Hutchings, Time; Peter Osborne, The Politics of Time: Modernity and Avant-Garde (London: Verso, 1995).
[150] Johannes Fabian, Time and the Other: How Anthropology Makes Its Object (New York: Columbia University Press, 2002/1983); also, Barry Hindess, 'The Past is Another Culture', International Political Sociology 1, no. 4 (2007): 325-338.
[151] James Duncan, 'Sites of Representation: Place, Time and the Discourse of the Other', in Place/Culture/Representation, eds. James Duncan and David Ley (London: Routledge, 1993), 39-56.
[152] John Agnew, 'Time Into Space: The Myth of "Backward" Italy in Modern Europe', Time & Society 5, no. 1 (1996): 27-45. Also, Maria Todorova, 'The Trap of Backwardness: Modernity, Temporality, and the Study of Eastern European Nationalism', Slavic Review 64, no. 1 (2005): 140-164.

individual resource'.[153] We might distinguish, as does Maier, between the sociotemporalities that inform the politics of 19th-century liberal modernity and of 20th-century totalitarianism. 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 20th 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'.[154] Soviet time subordinated 'the private present to the collective [socialist] future' and claimed 'social immortality'. Nazi time was more romantic and primitive and even whilst 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.[155] 'The only thing that matters', said Hitler in 1933, 'is that it is we who are the last to make history in Germany'.[156] 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 may belong to 'the political economy of relations between individuals, classes, and nations'.[157] In many influential accounts, the increased commodification of time is presented as a key driver of the successful

[153] Maier, 'Politics of Time', 153.
[154] Ibid., 161.
[155] Ibid.
[156] Adolf Hitler, Reden und Proklamationen 1932-1945 (Munich: Süddeutscher Verlag, 1965), I.i, 176, quoted in Reinhart Koselleck, Futures Past: On the Semantics of Historical Time (New York: Columbia University Press, 2004/1979), 203.
[157] Fabian, Time, xli.

spread of global capitalism.[158] Nowhere is this thesis presented so strongly than in Lewis Mumford's Technics and Civilization (1934), in which he writes: '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'.[159] 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'.[160] Economic and other practices not only unfold in time but instantiate dominant political and cultural conceptions of time: time is always embedded in practices.[161] 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 on speed and acceleration—we submit to a form of technological determinism 'which unproblematically maps the apparent power of things on to subjects'.[162] Furthermore, we might argue that speed itself is a culturally relativist creation, a modernist trope that itself depends upon the construction of a 'non-speedy' Other.[163] This is but an alternative manifestation of the forms of chronopolitical othering theorised by Fabian and others.

Yet these narratives persist, and Chapter Three is concerned with their relevance to the chronopolitics of cyber security. In one dystopian account of contemporary 'time wars', Jeremy Rifkin pits the political strategists of speed and technologized efficiency against those who

[158] On the temporalities of globalisation, see Bob Jessop, 'The Spatiotemporal Dynamics of Globalizing Capital and Their Impact on State Power and Democracy', in High-Speed Society: Social Acceleration, Power, and Modernity, eds. Hartmut Rosa and William E. Scheuerman (University Park, PA: Pennsylvania State University Press, 2009), 135-158.
[159] Lewis Mumford, Technics and Civilization (New York: Harcourt, Brace and Company, 1934), 14-15.
[160] Maier, 'Politics of Time', 152.
[161] Paul Glennie and Nigel Thrift, Shaping the Day: A History of Timekeeping in England and Wales 1300-1800 (Oxford: Oxford University Press, 2009), 68-71.
[162] Nigel Thrift, Non-Representational Theory: Space, Politics, Affect (London: Routledge, 2008), 63.
[163] Ibid.

would pursue life more in tune with the ancient rhythms of body and nature.[164] The roots of this conflict lie deep in Western culture, and are intelligible through the lens of chronopolitics:

> Since the dawn of Western consciousness, we have lived out our lives in a schizophrenic middle kingdom where biological and physical time clash head-on with our cultural and social time. And with every change in rhythm, tempo, and timing of either temporal order, we are forced to mediate a compromise that will allow us to continue to walk the tightrope that separates these two distinct and irreconcilable temporal worlds.[165]

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'.[166] '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'.[167] This account insists on the separation of nature and culture as a key facet of modernity, which differentiates it from the present enquiry. As Fraser shows, 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.[168] In related fashion, Bruno Latour argues that 'we have never been modern': the artificial distinction between culture and nature serves to obscure the

[164] Jeremy Rifkin, Time Wars: The Primary Conflict in Human History (New York: Henry Holt and Company, 1987).
[165] Ibid., 43.
[166] Ibid., 43.
[167] Ibid., 13.
[168] Fraser, Time.

innumerable intense and constitutive relations between 'cultural' humans and the 'natural' objects and phenomena populating the world in which we live.[169]

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 discourses 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.

[169] Latour, We Have Never Been Modern.

# 3 DIAGNOSING THE PRESENT

For we which now behold these present days

Have eyes to wonder, but lack tongues to praise.[1]

To define the present in isolation is to kill it.[2]

## 3.1 Introduction: The Revolutionary Present

Elite cyber security discourses are keen to emphasise the historical importance of the times in which we live. The UK Cyber Security Strategy (2011) 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'.[3] 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'.[4] 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 and the language of revolution is never far away. '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'.[5] Cyber security, argues the White House, is essential to realising the 'full potential' of this

[1] William Shakespeare, 'Sonnet 106', in The Complete Works, eds. Stanley Wells and Gary Taylor (Oxford: Clarendon Press, 1988), 764.
[2] Paul Klee, quoted in Paul Virilio, Open Sky (London: Verso, 1997/1995), 10.
[3] Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (London: Cabinet Office, November 2011), 11.
[4] Michael V. Hayden, Aspen Security Forum, Aspen, CO, 29 July 2011.
[5] White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: White House, May 2011), 25.

revolution.[6] The UK government grants 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'.[7] 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,[8] and responsible for making the US a nation 'now fully dependent on cyberspace'.[9] 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.[10]

Cyber security is located relative to the wider transformations of an 'information age', ushered in by an ongoing 'information revolution'.[11] 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.[12] It serves as the convenient demarcation of one period of human history from another, even if such crude periodization is well recognised as a problematic abstraction from historical reality.[13] 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 in the 19th century to provide a

[6] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, DC: White House, May 2009), i.
[7] HM Government, Digital Britain: Final Report, Cm. 7650 (Norwich: The Stationery Office, June 2009), 7.
[8] Ibid., 8.
[9] White House, The National Strategy to Secure Cyberspace (Washington, DC: White House, February 2003), 5.
[10] Jörg Krüger, Bertram Nickolay and Sandro Gaycken, 'Preface', in The Secure Information Society: Ethical, Legal and Political Challenges, eds. Jörg Krüger, Bertram Nickolay and Sandro Gaycken (London: Springer-Verlag, 2013), v.
[11] The UK government has registered the possibilities of an information-technological 'revolution' since at least the mid-1950s; e.g. Annual Report of the Chief of Inspector of Factories for the Year 1954, Cmd. 9605 (London: HMSO, November 1955), 12. The language of IT revolution was established early in the Blair administration that eventually produced 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, Our Information Age: The Government's Vision, INDY J98-2429, URN 98/677 4/98 (London: Central Office of Information, 1998), 3.
[12] For example, Walter B. Wriston, 'Bits, Bytes, and Diplomacy', Foreign Affairs 76, no. 5 (1997): 172-182.
[13] A problem recognised since the end of the 18th century; Reinhart Koselleck, Futures Past: On the Semantics of Historical Time (New York: Columbia University Press, 2004/1979), 244-245.

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.[14] 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'.[15] In this case, periodization 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 periodization of the information age is a social construction. As Foucault notes, it is perhaps more accurate to speak of periodization 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.[16] Even recognising this, we still run the risk, as Daniel Pick notes, of 'singularising what was always plural'.[17] This is not to suggest 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'.[18] More radically still, 'the hegemonic conception of the information revolution is an awesome phenomenon with real meaning and consequence in

[14] Gavin Lucas, The Archaeology of Time (London: Routledge, 2005), 50-51.
[15] Graham Connah, Writing About Archaeology (Cambridge: Cambridge University Press, 2010), 63.
[16] Michel Foucault, 'What is Enlightenment?', in The Foucault Reader, ed. Paul Rabinow (New York: Pantheon Books, 1984), 39.
[17] Daniel Pick, War Machine: The Rationalisation of Slaughter in the Modern Age (New Haven, CT: Yale University Press, 1993), 203.
[18] Kees Brants, 'The Social Construction of the Information Revolution', European Journal of Communication 4, no. 1 (1989): 90-91.

and for our lives'. [19] The information revolution is a discursive construction, a system of knowledge, ideas and practices that shapes and constrains what is possible:

> The information revolution produces the information age …. An age connotes an all-pervasive logic, a logic that requires that everything be explained in its own terms. The articulation of an age is thus an essentialized articulation in which everyone and everything is subsumed to a new, expressive, reductive logic. The articulation suppresses any possible contradiction or non-correspondence. Everything is made to fit, to conform.[20]

Myriam Dunn Cavelty notes one of the principal outcomes of this problematic periodization in cyber security:

> [It gives] expression to the common cyber-enthusiasm to which it is so easy to succumb, and a manifestation of the tendency to call everything that is related to the 'information revolution' 'new' and to see it as radically different from what came before.[21]

This is a key consideration in any discussion of cyber security and the social present. Frank Webster notes the 'divide between information society theorists who announce the novelty of the present and informatisation thinkers who recognise the force of the past on today's developments'.[22] There is a distinction between those who proclaim the 'newness' of contemporary society, in which the Internet and other information technologies have

---

[19] Jennifer Daryl Slack, 'The Information Revolution as Ideology', Media, Culture & Society 6, no. 3 (1984): 250.
[20] Ibid., 253. Also, Jos de Mul, 'The Informatization of the Worldview', Information, Communication & Society 2, no. 1 (1999): 69-94.
[21] Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008), 16. Also, Myriam Dunn, 'Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory', in International Relations and Security in the Digital Age, eds. Johan Eriksson and Giampiero Giacomello (London: Routledge, 2007), 87-88.
[22] Frank Webster, Theories of the Information Society, 3rd. edn. (London: Routledge, 2006/1995), 8.

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'.[23] In historical perspective, it would seem that 'continuity exceeds discontinuity',[24] and it is more accurate to describe contemporary transitions as evidence of evolution rather than revolution.[25]

The language of revolution is overused but it is reasonable 'to explore the premise that the digital networked computer environment is unleashing significant discontinuities from previous eras'.[26] Such qualified opinion is not found in most government cyber security discourses, which unequivocally align with a perspective that stresses the novelty of the revolutionary present.[27] '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

[23] Ibid., 7.
[24] Peter Golding, 'Forthcoming Features: Information and Communications Technologies and the Sociology of the Future', Sociology 34, no. 1 (2000): 166.
[25] Dunn Cavelty, Cyber-Security, 15.
[26] Richard J. Harknett, '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 2011.
[27] This contrasts with government documents of even a decade ago. Arguably the UK government's first attempt to develop an holistic perspective on the 'new landscape' of information technologies and society noted: 'What is so potent about the communications revolution is the way it combines the old and the new'; Department of Trade and Industry and Department for Culture, Media and Sport, A New Future for Communications, Cm. 5010 (London: HMSO, December 2000), 7.

and depth, its thought has become, in the main, unhistorical or antihistorical'.[28] This tendency surfaces in the thin appeals of cyber security to historical periodization, 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.[29] The social present is a richly textured aggregate of competing and complementary temporalities but it is also a stratified temporal assemblage, in which 'one time structure never eliminated another [but] each new structure was overlaid on the top of the previously dominant structure'.[30] 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.[31] We can read this additionally against the 'emergent temporality' framework described in Chapter Two, which proposes that sociotemporality incorporates knowledge about lower-order temporalities identifiable with nonhuman assemblages of matter and energy.

The historicization 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

---

[28] Ernest Gellner, Plough, Sword and Book: The Structure of Human History (London: Collins Harvill, 1988), 12, quoted in Justin Rosenberg, 'The International Imagination: IR Theory and "Classic Social Analysis"', Millennium: Journal of International Studies 23, no. 1 (1994): 88.

[29] A similar observation may be made of technology, which can endure in the face of change and exert 'ongoing and technical influence simply because it is "there" and because people have come to depend on its being there'; John M. Staudenmeier, Technology's Storytellers: Reweaving the Human Fabric (Cambridge, MA: MIT Press, 1985), 156,.

[30] Jacques Attali, Histoires du Temps (Paris: Fayard, 1982), 247-248, quoted in Olivier Klein, 'Social Perception of Time, Distance and High-Speed Transportation', Time & Society 13, nos. 2-3 (2004): 252.

[31] Attali: 'the theory for each new time structure would seem never to be totally formulated until the end of the given structure's domination'; ibid.

a technical or policy persuasion necessarily to indulge in historical exegeses ahead of their often fine-grained analyses of contemporary issues and problems.[32] 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 19th century, a contribution that states, 'History Informs our Future'.[33] This bucks the 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'.[34]

The delineation of an information age is an exercise in periodization 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 dehistoricized 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 sociotemporality 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

[32] In the author's experience, technical professionals—more than policymakers—are often keenly aware of the heritage of their fields but allow this to inform their work rather than become its central feature. This accounts for the frequency of historical case studies in works on information security but the dearth of histories of information security itself. For an attempt at the latter, see Karl de Leeuw and Jan Bergstra, eds., The History of Information Security: A Comprehensive Handbook (Amsterdam: Elsevier, 2007).

[33] White House, 'Appendix C: Growth of Modern Communications Technology in the United States and Development of Supporting Legal and Regulatory Frameworks', Cyberspace Policy Review, C1-C12.

[34] Gellner, Plough, Sword and Book, 12. Also, the History and Policy initiative, 'connecting historians, policymakers and the media', http://www.historyandpolicy.org/.

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'.[35] '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'.[36] 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 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 a temporal present that combines and conflicts with others in the sociotemporality through which the cyber security present is imagined and constructed. In the first section, the concepts of speed and acceleration are situated historically as the intersubjective experience of all cultures and as a key aspect of the politics of modernity and postmodernity. Two subsequent sections examine multiple aspects of sociotechnical speed, which we here 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 emerge from this sociotemporal imaginary.

[35] James Der Derian, Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network, 2nd. edn. (New York: Routledge, 2009/2001), 250.
[36] Ibid., 251.

## 3.2 Speed and Acceleration

Marshall McLuhan observed that the 'message' of any medium of technology is 'the scale or pace or patterns that it introduces into human affairs'.[37] Illustrating this thesis with reference to the railway, McLuhan wrote that

> it did not introduce movement or transportation or wheel or road into human society, but it accelerated and enlarged the scale of previous human functions, creating totally new kinds of cities and new kinds of work and leisure.[38]

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.[39] 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'.[40] 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 solely 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 the acceleration of history and the contraction of the planet'.[41] 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

---

[37] Marshall McLuhan, 'The Medium is the Message', in Media and Cultural Studies: KeyWorks, rev. edn., eds. Meenakshi Gigi Durham and Douglas M. Kellner (Malden, MA: Blackwell Publishing, 2006/2001), 108.
[38] Ibid.
[39] Wolfgang Schivelbusch, The Railway Journey: The Industrialization of Time and Space in the 19th Century (Berkeley, CA: University of California Press, 1986/1977). See also the case study in Carlene Stephens, '"The Most Reliable Time": William Bond, the New England Railroads, and Time Awareness in 19th-Century America', Technology & Culture 30, no. 1 (1989): 1-24.
[40] McLuhan, 'The Medium', 108.
[41] Marc Augé, Non-Places: Introduction to the Anthropology of Supermodernity (London: Verso, 1995/1992), 119.

light and collapse 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.[42]

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'.[43] 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.[44] The term has limited social-scientific analytical utility but it refuses to go away. As Julie Cohen argues, the 'cyberspace metaphor is neither an arbitrary fiction that can be jettisoned nor a description of some fixed, eternal reality, but rather an inevitable perceptual byproduct [sic] of the human cognitive apparatus …. The commitment to spatiality runs far deeper than mere politics or intellectual fashion'.[45] 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 as the ethereal 'noosphere' of Teilhard de Chardin, or any other of the more venerable but less easily grasped concepts through which cyberspace has been approached and theorised.[46] At the same time, cyberspace is constructed as a space apart

[42] David Harvey, The Condition of Postmodernity: An Enquiry Into the Origins of Cultural Change (Cambridge, MA: Blackwell, 1990). William Gibson's original description of cyberspace uses the word 'nonspace', but with respect to the 'the nonspace of the mind'; William Gibson, Neuromancer (London: HarperCollins, 1984), 67. The dimensionality of space and the locationality of place are not equivalent; see, John Agnew, 'Space and Place', in Handbook of Geographical Knowledge, eds. John Agnew and David N. Livingstone (London: Sage, 2011), 316-330.

[43] William J. Mitchell, City of Bits: Space, Place, and the Infobahn (Cambridge, MA: MIT Press, 1995), 3.

[44] Richard Rogers, '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 & Politics 7, nos. 2-3 (2010): 241-260.

[45] Julie E. Cohen, 'Cyberspace As/And Space', Columbia Law Review 107, no. 1 (2007) 234.

[46] For example, David Ronfeldt and John Arquilla, 'From Cyberspace to the Noosphere: Emergence of the Global Mind', New Perspectives Quarterly 17, no. 1 (2000): 18-25.

from 'real life', an instantiation of 'digital dualism' that preserves a false dichotomy between 'the virtual' and 'the actual'.[47]

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 UK, 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'.[48] 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'.[49] 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.[50] Specifically, it suggests the following, citing a 2011 McKinsey report:

> Real GDP [gross domestic product] per capita has risen by $500 over the last 15 years in mature countries enabled by the internet. By comparison, it took 50 years for the industrial revolution to have the same effect.[51]

The original McKinsey report notes 'both the magnitude of the positive impact of the Web at all levels of society and the speed at which it delivers benefits'.[52] The comparative GDP data suggests that the rate of change in GDP has accelerated since the Industrial Revolution, so that the increase in GDP has occurred three times more quickly than it did during the earlier 'revolutionary' period. Crude though this measure is, it is one example of how speed and

---

[47] Tom Boellstorff, Coming of Age in Second Life: An Anthropologist Explores the Virtually Human (Princeton, NJ: Princeton University Press, 2008), 18-21.
[48] Webster, Theories, 142, original emphasis.
[49] Cabinet Office, Cyber Security Strategy, 21.
[50] Brants, 'Social Construction', 91.
[51] Cabinet Office, Cyber Security Strategy, 21.
[52] Matthieu Pélissié du Rausas, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui and Rémi Said, Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity (New York: McKinsey Global Institute, May 2011), 19.

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.[53]

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'.[54] Speed can only be experienced subjectively if there are discrete events whose frequency we can sense, if not always 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 similarly 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.

[53] The literature on speed and acceleration as distinct facets of technological (post)modernity is formidable and diverse. Recent important contributions include: Robert Hassan and Ronald E. Purser, eds., 24/7: Time and Temporality in the Network Society (Stanford, CA: Stanford Business Books, 2007); Robert Hassan, Empires of Speed: Time and the Acceleration of Politics and Society (Leiden: Brill, 2009); Hartmut Rosa and William E. Scheuerman, eds., High-Speed Society: Social Acceleration, Power, and Modernity (University Park, PA: Pennsylvania State University Press, 2009); Simon Glezos, The Politics of Speed: Capitalism, the State and War in an Accelerating World (London: Routledge, 2012).

[54] Anna Grzymala-Busse, 'Time Will Tell? Temporality and the Analysis of Causal Mechanisms and Processes', Comparative Political Studies 44, no. 9 (2011): 1282.

Speed and acceleration have always been problematic aspects of sociotemporality and its relations with technology. Jose Harris records that towards the end of the 19th 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'.[55] The proximate reasons for this are not hard to identify:

> in a myriad mundane but basic ways the regime of nature slackened its hold on human life, as medicine began to cure as well as kill, as water flowed out of taps and excrement flowed into sewers, as the glare of gas and electricity replaced the age-old illumination of oil-lamp and candle, and as the man-made tempo of great cities increasingly superseded the diurnal, seasonal, and annual rhythms of the natural world.[56]

In historical perspective, we might see these phenomena 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'.[57] 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.[58] Later authors have lamented this driving of 'a permanent wedge between the rhythms of culture and the rhythms of nature',[59] but this rupture was glorified by some at the time, including the founders of Italian Futurism, probably the first authentic European avant-garde:

---

[55] Jose Harris, Private Lives, Public Spirit: Britain 1870-1914 (London: Penguin Books, 1993), 32, emphasis added.
[56] Ibid., 33.
[57] Ibid.
[58] Ruth E. Iskin, 'Father Time, Speed, and the Temporality of Posters Around 1900', KronoScope 3, no. 1 (2003): 47. Also, Stephen Kern, The Culture of Time and Space 1880-1918 (Cambridge, MA: Harvard University Press, 1983), 117-124.
[59] Jeremy Rifkin, Time Wars: The Primary Conflict in Human History (New York: Henry Holt and Company, 1987), 47.

> 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.[60]

In its fascistic muscularity, misogyny and paeans to the glories of 'hygienic' war, Futurism may still shock the contemporary mind.[61] 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 19th-century industrialisation and mass commercialisation, not least in its pessimistic register.[62] 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'.[63] 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.[64] Speed has 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'.[65] As Jacques Derrida suggests,

---

[60] Filippo Tommaso Marinetti, 'The Founding and Manifesto of Futurism', in Futurist Manifestos, ed. Umbro Apollonio (New York: Viking Press, 1973), 21-22, originally published in Gazzetta dell'Emilia, 5 February 1909.

[61] The centenary of the Futurist Manifesto has occasioned many considerations of the legacy of Futurism; see, Geert Buelens, Harald Hendrix and Monica Jansen, eds., The History of Futurism: The Precursors, Protagonists, and Legacies (Plymouth: Lexington Books, 2012).

[62] Ryan Anthony Vieira, 'Connecting the New Political History with Recent Theories of Temporal Acceleration: Speed, Politics, and the Cultural Imagination of Fin de Siècle Britain', History & Theory 50, no. 3 (2011): 386-388.

[63] Harris, Private Lives, 34. As Robert D'Amico asserts, 'human understanding is always a "captive" of its historical situation'; Robert D'Amico, Historicism and Knowledge (New York: Routledge, 1989), x, quoted in Ronald J. Deibert, 'Harold Innis and the Empire of Speed', Review of International Studies 25, no. 2 (1999): 281.

[64] Kern, Culture of Time and Space, 129. It is symptomatic of this dialectic that a Wikipedia search for 'Slow' redirects immediately to 'Speed', http://en.wikipedia.org, accessed 1 October 2013.

[65] Simon Glezos, in Annalee Newitz and Simon Glezos, 'Digital Inflections: Annalee Newitz in Conversation with Simon Glezos', CTheory, 30 November 2010.

'[a]t the beginning there will have been speed'.[66] Speed 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.

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'.[67] 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. In Beissinger's reading of thickened history, events structure history but our historical sensitivity is hampered by the human inability to process information about these events and the social and political effects they catalyse. Our subjective experience is principally one of great speed, with multiple events occurring rapidly in sequence 'within an extremely compressed period of time'.[68] 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, in which the increasing frequency of events can lead to disorientation and an inability to interpret this acceleration in historical perspective.[69] As David Harvey notes, 'time-space compression always exacts its toll on our capacity to grapple with the realities unfolding around us'.[70]

Cyber security actors identify speed and acceleration as fundamental aspects of the present and as key drivers of uncertainty and insecurity. They are important facets of the

[66] Jacques Derrida, 'No Apocalypse, Not Now (Full Speed Ahead, Seven Missiles, Seven Missives)', diacritics 14, no. 2 (1984): 20.
[67] Marc R. Beissinger, Nationalist Mobilization and the Collapse of the Soviet State (Cambridge: Cambridge University Press, 2002), 27.
[68] Ibid.
[69] Also, James R. Beniger, The Control Revolution: Technological and Economic Origins of the Information Society (Cambridge, MA: Harvard University Press, 1986), 1-6.
[70] Harvey, Condition of Postmodernity, 306.

sociotemporality informing the politics and practices of cyber security but they are not the only ones. The following discussion examines two distinct but co-existing dimensions of the cyber security present, with reference to the temporalities of people, social groups, machines and networks, which together are components of what we might call, 'netspeed'. This term is used with obvious reference to the Internet (the 'Net) and to its 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.

## 3.3 Netspeed I: Acceleration

Cyber security actors are explicit about the speed and acceleration of events. 'Events in cyberspace can happen at great speed', observes the UK government.[71] The threats posed by computer networks are framed as threats happening at the speed of those networks. 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'.[72] 'Attacks cross borders at light speed', the White House notes.[73] 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.[74]

Nowhere is the frequency and acceleration of events stressed more than in formulations of 'cascading failure', in which 'events triggering a collapse produce a series of secondary effects

[71] Cabinet Office, Cyber Security Strategy, 7
[72] Jim Garamone, 'Lynn Calls for Collaboration in Establishing Cyber Security', American Forces Press Service, 1 October 2009.
[73] White House, National Strategy, 49.
[74] For example, Leon Panetta, 'Remarks by Secretary Panetta on Cybersecurity', speech to Business Executives for National Security, New York, 11 October 2012.

in interdependent infrastructures'.[75] 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.[76] In information infrastructures, failures thereby catalysed will 'escalate rapidly beyond control before anyone understands what is happening and is able to intervene'.[77]

This accelerated frequency of events is diagnosed for ICTs and the contemporary world in general and expressed in the language of technological change. The UK government observes that the 'technology that underpins [cyberspace] continues to develop at a rapid pace'.[78] Not only is the pace of change rapid but it 'will not let up'; it is 'relentless'.[79] We may assume that various inflections of the adjective are intended, in its evocation of inexorability and of its sternness or lack of mercy. 'We cannot afford to be complacent' about the pace of technological change, says the British government.[80] 'We expect the rapid development and exploitation of computers and electronic communication technologies to continue to accelerate'.[81]

Cyber security texts repeatedly stress the subordinate position of humans in computer networks. One article begins, it is now 'a truism that most humans cannot keep up with the

[75] Tony H. Grubesic and Alan T. Murray, 'Vital Nodes, Interconnected Infrastructures, and the Geographies of Network Survivability', Annals of the Association of American Geographers 96, no. 1 (2006): 64. Also, Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', IEEE Control Systems 21, no. 6 (2001): 11-25; Richard G. Little, 'Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures', Journal of Urban Technology 9, no. 1 (2002): 109-123.
[76] Tomas Hellström, 'Systemic Innovation and Risk: Technology Assessment and the Challenge of Responsible Innovation', Technology in Society 25, no. 3 (2003): 369-384; Tomas Hellström, 'Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework', Safety Science 45, no. 3 (2007): 415-430.
[77] Dunn Cavelty, Cyber-Security, 18.
[78] HM Government, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, Cm. 7642 (Norwich: The Stationery Office, June 2009), 3.
[79] Cabinet Office, Cyber Security Strategy, 13, 29.
[80] HM Government, Digital Britain, 48.
[81] Home Office, Cyber Crime Strategy, Cm. 7842 (Norwich: The Stationery Office, March 2010), 5.

speed of technological development across cyber space'.[82] '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.[83] From the computer science perspective,

> Current cyber-defense systems involve humans at multiple levels, but people are often far down in the control structure, requiring them to make too many time-critical decisions. Information flow between humans is slow and frequently asynchronous. In a crisis, humans may be unable to cooperate because of cultural, language, legal, proprietary, availability, or other obstacles. Such systems cannot adapt to rapid cyber threats.[84]

Over the last two decades, the automation of response systems has resulted in a gradual removal of humans from decision loops.[85] One information security professional remarked:

> Automated software has increased the speed of attacks to the point where little human interaction is needed, and less can be done to prevent it. All we see is the battlefield when it's over.[86]

The deliberate, rather than incidental, excision of human inputs and decision-making is suggested in the array of technologies marketed as 'active defence' solutions to cyber security

---

[82] Misha Glenny and Camino Kavanagh, '800 Titles But No Policy—Thoughts on Cyber Warfare', American Foreign Policy Interests 34, no. 6 (2012): 287.
[83] Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (New York: Ecco, 2010), 215.
[84] Jerome N. Haack, Glenn A. Fink, Wendy M. Maiden, A. David McKinnon, Steven J. Templeton and Errin W. Fulp, 'Ant-Based Cyber Security', Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations (ITNG 2011), Las Vegas, NV, 11-13 April 2011, 918.
[85] Natalia Stakhanova, Samik Basu and Johnny Wong, 'A Taxonomy of Intrusion Response Systems', International Journal of Information & Computer Security 1, nos. 1-2 (2007): 169-184; Alireza Shameli-Sendi, Naser Ezzati-jivan, Masoume Jabbarifar and Michael Dagenais, 'Intrusion Response Systems: Survey and Taxonomy', International Journal of Computer Science & Network Security 12, no. 1 (2012): 1-14.
[86] Donn Parker, quoted in Bruce Haring, 'Hackers Rampant in Cyberspace', USA Today 28 March 1995.

problems.[87] These systems have been suggested since at least the mid-1990s, when they were presented as analogous to the human immune system.[88] Active defence systems—described as '[p]art sensor, part sentry, part sharpshooter'[89]—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.[90] 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'.[91]

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.[92] 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

[87] Contrast with the desire to keep human operators embedded within another critical infrastructure component: Zoe Kleinman, 'Why Air Traffic Control Still Needs the Human Touch', BBC News, 5 February 2013.

[88] Richard O. Hundley and Robert H. Anderson, 'Emerging Challenge: Security and Safety in Cyberspace', IEEE Technology & Society 14, no. 4 (1995): 25. The language of public health remains an important source of cyber security analogies; David J. Betz and Tim Stevens, 'Analogical Reasoning and Cyber Security, Security Dialogue 44, no. 2 (2013): 147-164.

[89] William J. Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy', Foreign Affairs 89, no. 5 (2010): 103.

[90] Jay P. Kesan and Carol M. Hayes, '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, 2010), 327-342; also, Richard Colbaugh and Kristin Glass, eds., Proactive Defense for Evolving Cyber Threats, SAND2012-10177 (Albuquerque, NM: Sandia National Laboratories, 2012).

[91] Ellen Nakashima, 'US Builds a Cyber "Plan X"', The Washington Post, 31 May 2012.

[92] Also, Boellstorff, Coming of Age, 19-20. The control aspect of cybernetics 'haunts' discourse on new media and the same might be said of its rarely unacknowledged presence in cyber security discourse; Mark Andrejevic, iSpy: Surveillance and Power in the Interactive Era (St. Lawrence, KS: University Press of Kansas, 2007), 18. As Dunn Cavelty notes (Cyber-Security, 17-18), the control paradigm can only take us so far in understanding cyber security, and concepts like complexity also need to be taken into account. Also, Paul N. Edwards, The Closed World: Computers and the Politics of Discourse in Cold War America (Cambridge, MA: MIT Press, 1996); Antoine Bousquet, The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity (London: Hurst & Company, 2009).

technoscientific human knowledge could be brought under control: cybernetics could 'deal simultaneously with the dark politics and bright theology of a the new age'.[93]

In these scenarios, we see a fundamental discrepancy between the speeds of computer networks and their effects, and 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.[94] Systems will be implemented that act at the speed of the networks and the machines that comprise them; humans have no operational utility in such an environment. Even serious proposals for slowing network traffic in order to restore tactical advantage to network defenders leave little scope for human decision-making, despite their claims to grant network administrators 'Flash-like superpowers'.[95]

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 light-speed. As this light travels

[93] Geoffrey Bowker, 'How to Be Universal: Some Cybernetic Strategies, 1943-70', Social Studies of Science 23, no. 1 (1993): 113. Complementary views were held on the other side of the Iron Curtain; Slava Gerovitch, 'InterNyet: Why the Soviet Union Did Not Build a Nationwide Computer Network', History & Technology 24, no. 4 (2008): 335-350.

[94] It takes one-tenth of a second for a human to respond to an external stimulus, far slower than any process relevant to technical aspects of computing. On the significance of this duration, see Jimena Canales, A Tenth of a Second: A History (Chicago: University of Chicago Press, 2009). This is not to deny the great rapidity of electrical impulses in mammalian nervous systems, although the fastest are several million times slower than electricity conducted through wire. It is worth noting that the human brain operates in a matrix of electrochemical temporalities due to the differential processing speeds of information obtained from different sensory modalities; Virginie van Wassenhove, 'Minding Time in an Amodal Representational Space', Philosophical Transactions of the Royal Society B 364, no. 1525 (2009): 1815-1830. Also, Peter Hancock, 'On the Nature of Time in Conceptual and Computational Nervous Systems', KronoScope 7, no. 2 (2007): 185-196.

[95] Daniel Guernsey, Mason Rice and Sujeet Shenoi, 'Implementing Novel Reactive Defense Functionality in MPLS Networks Using Hyperspeed Signalling', International Journal of Critical Infrastructure Protection 5, no. 1 (2012): 40-52. The allusion is to various 'super-speed' comic characters known as 'The Flash'.

in glass rather a vacuum 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. Even at this local speed, 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 with 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 merely vibrate, 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, 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'.[96]

When the UK government states enthusiastically that information can be exchanged across global networks 'in timescales that were previously unimaginable',[97] 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 peak operating performance of 54.91 petaflops, or nearly 55 quadrillion ($10^{15}$) 'floating-point operations per second', is natively incomprehensible.[98] The many online applications available for testing domestic broadband speeds return results that mean almost nothing to the technically untutored. The aim of the UK government's Broadband Delivery UK unit is to 'provide universal

[96] Adrian Mackenzie, Transductions: Bodies and Machines at Speed (London: Continuum, 2002), 88.
[97] HM Government, Digital Britain, 190.
[98] BBC News, 'China's Tianhe-2 Retakes Fastest Supercomputer Crown', 17 June 2013.

access to standard broadband with a speed of at least 2Mbps'.[99] What this means is difficult to say, except that government policy aims to deliver 'the best superfast broadband network in Europe'; it is 'fundamental to our future prosperity'.[100] The national ambition 'should be for a broadband system that is the engine of the nation's mind'.[101] 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 commoditized 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.[102] 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.[103] Their names—Jaguar, Tianhe-1, K, Sequoia, Titan and the aforementioned Tianhe-2—have some of the sober resonance of their Cold War origins and also act as technical proxies of national power and prestige, as did the earlier contests between Britain and its maritime rivals to achieve ever-faster crossings of the North Atlantic sea routes in the late-19th and early-20th centuries.[104] HPC speeds are indeed 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.

---

[99] Department for Culture, Media and Sport, 'Stimulating Private Sector Investment to Achieve a Transformation in Broadband in the UK by 2015', 27 February 2013, http://www.culture.gov.uk/what_we_do/telecommunications_and_online/7763.aspx, accessed 19 May 2013.

[100] HM Government, Britain's Superfast Broadband Future (London: Department for Business, Innovation and Skills, December 2010), 7.

[101] HM Government, Digital Britain, 47.

[102] Donald MacKenzie, 'Nuclear Weapons Laboratories and the Development of Supercomputing', Knowing Machines: Essays on Technical Change (Cambridge, MA: MIT Press, 1996), 99-129. Industry requirements have often prioritised qualities other than speed, such as reliability and usability; see, Boelie Elzen and Donald MacKenzie, 'The Social Limits of Speed: The Development and Use of Supercomputers', IEEE Annals of the History of Computing 16, no. 1 (1994): 46-61.

[103] Top500 Supercomputer Sites, http://www.top500.org/.

[104] Kern, Culture of Time and Space, 109-110.

Tellingly, given its historical analogues, this supercomputer rivalry is not infrequently reported as a contemporary 'arms race'.[105] President Obama 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.[106] Although the White House has dismissed talk of an HPC 'arms race' as a distraction,[107] Obama has spoken of these issues in just such language: 'In the race for the future, America is in danger of falling behind'.[108] After 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.[109] Recent presidential addresses have been less polarised, preferring the exhortatory yet qualified optimism of 'we are going to be just fine … as long as …'[110] As in the Cold War, these views are expressed with reference to an abstracted conception of an eastern Other—in this case, China—although the air of existential dread that pertained during the decades of nuclear standoff is so far generally absent.[111]

British Prime Minister David Cameron's similar 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

---

[105] An early example is John Markoff, 'A New Arms Race to Build the World's Mightiest Computer', The New York Times, 19 August 2005. The language of arms racing is also used to describe the development of offensive cyberwarfare capabilities and the militarisation of cyberspace; e.g. Ronald J. Deibert, '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, 2008), 152-153.

[106] Barack Obama, 'Remarks by the President on the Economy', 6 December 2010, Winston-Salem, NC.

[107] President's Council of Advisors on Science and Technology, Report to the President and Congress: Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology (Washington, DC: White House, December 2010), 67.

[108] Obama, 'Remarks by the President'. A proposed American Super Computing Leadership Act would require formal government investment in HPC and is framed by its sponsors as a direct response to Chinese advances in this field; Patrick Thibodeau, 'Fear of Thinking War Machines May Push US to Exascale', ComputerWorld, 20 June 2013.

[109] Jack Lule, 'Roots of the Space Race: Sputnik and the Language of US News in 1957', Journalism & Mass Communication Quarterly 68, nos. 1-2 (1991): 76-86.

[110] Obama, 'Remarks by the President'.

[111] That said, adversarial use of HPC (and new forms of computing) for cryptological purposes is an emerging national security concern; e.g. Ministry of Defence, Global Strategic Trends: Out to 2040, 4th. edn., Development, Concepts and Doctrine Centre Strategic Trends Programme, January 2010, 140.

an hour of reckoning for countries like ours. Sink or swim. Do or decline'.[112] Speaking to business executives, Cameron said, 'You need us to be tough. To be radical. To be fast …. So this government has been tough and we've been 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'.[113] Cameron has made plain the existential implications of not embracing the speed of global commerce, ironically emanating from and exemplified by many of the same post-colonial and post-Soviet countries traditionally referred to in the racialized subtexts of Western political discourse as 'backward'.[114] The philosopher John Gray summarised Cameron's political outlook:

> Along with much of the political class, 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.[115]

Gray locates Cameron's politics firmly within the global vector of speed through his reference to the commercial non-places of air travel and the Prime Minister's apparently shallow appreciation of temporality.

---

[112] David Cameron, speech to Conservative Party Conference, Birmingham, 10 October 2012. 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'; Frank Webster and Kevin Robins, Information Technology: A Luddite Analysis (Norwood, NJ: Ablex Publishing Corporation, 1986), 15.

[113] David Cameron, speech to Confederation of British Industry, London, 19 November 2012.

[114] British trade envoys have been newly appointed to Algeria, Azerbaijan, Cambodia, Indonesia, Jordan, Kazakhstan, Kuwait, Laos, Mexico, Morocco, Palestinian Territories, South Africa, Turkmenistan and Vietnam; BBC News, 'David Cameron: We Must Push in "Global Trade Race"', 12 November 2012; HM Government, The Coalition: Together in the National Interest, January 2013 (London: Cabinet Office), 5.

[115] John Gray, 'Ignore at Our Peril', The Guardian, 2 February 2013.

After the French Revolution, politics became a driver of social acceleration and deceleration, the progressive left favouring the acceleration of history, the conservative right struggling to preserve the virtues of the past or even to slow down change.[116] At the beginning of the present century, this dichotomy has been eroded, perhaps even reversed:

> if the distinction between left and right has retained any discriminatory power at all, 'progressives' tend to sympathize with the advocates of deceleration (stressing locality, political control of the economy, democratic negotiation, environmental protection, etc.), whereas 'conservatives' have become strong defenders of the need for further acceleration (embracing new technologies, rapid 'free' markets, and fast administrative decision-making).[117]

If, in these terms, speed has become the 'center of an ideological battle' between 'left' and 'right',[118] this conflict is rarely seen in elite cyber security discourse: there is no substantive argument between the nominal 'left' and 'right' over the fundamental politics of cyber security. A remarkable bipartisan unanimity states that cyber security is needed and it is needed now. The sociotemporality of cyber security is shared across this traditional political divide; it is in ecstatic thrall to speed and acceleration as much as it is terrified by the changes they bring.[119] That conservative politicians should be so convinced by the need to embrace speed is symptomatic of the seductiveness of speed. One answer to speed—traditionally the enemy of conservatism—is not to resist it but to allow oneself to be enfolded by it, even as we may detest both its capacity for social change and our genuflection before its ecstatic potency. After all, writes Milan Kundera, speed is 'the form of ecstasy the technical revolution has

---

[116] Hartmut Rosa, 'The Speed of Global Flows and the Pace of Democratic Politics', New Political Science 27, no. 4 (2005): 450.
[117] Ibid., 453; also, Hartmut Rosa, 'Social Acceleration: Ethical and Political Consequences of a Desynchronized High-Speed Society', in Rosa and Scheuerman, High-Speed Society, 101-102.
[118] Rosa, 'Speed of Global Flows', 453.
[119] This dual character affects 'speed-elites' and pro-deceleration activists alike; see, Ingrid M. Hoofd, Ambiguities of Activism: Alter-Globalism and the Imperatives of Speed (New York: Routledge, 2012).

bestowed on man'.[120] 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 sedimented as ontology, rather than remaining open for epistemological, let alone 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.

## 3.4 Netspeed II: Deceleration

Politically, deceleration may be something to promote actively, a necessary political resistance and theoretical counterbalance to the speed and acceleration of 21st-century life.[121] Certainly, the imperative to 'slow down' is at the heart of much historical and contemporary social activism.[122] It is both an encouragement to decelerate and 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

[120] Milan Kundera, Slowness: A Novel (New York: HarperCollins, 1997), 2.
[121] Nicholas Gane, 'Speed Up or Slow Down? Social Theory in the Information Age', Information, Communication & Society 9, no. 1 (2006): 20-38; Michael Saward, 'Slow Theory: Taking Time Over Transnational Democratic Representation', Ethics & Global Politics 4, no. 1 (2011): 1-18.
[122] Wendy Parkins, 'Out of Time: Fast Subjects and Slow Living', Time & Society 13, nos. 2-3 (2004): 363-382.

be eternal'.[123] 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.

Yet there is apparently no question that cyber security might in any way embrace deceleration. It is never mentioned and must be reconstructed from texts, even though 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 is less important for present purposes than establishing the subjective impression of deceleration relative to an accelerating other.[124] 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 faster apart from one another that is significant. We need not be discussing single entities either: the 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 suggests 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 macroeconomics, the concept of 'lag' refers to time delays between the identification of economic problems and the effects of economic solutions.[125] The 'inside lag' is the length of

[123] Manuel Castells, 'Urban Sustainability in the Information Age', City: Analysis of Urban Trends, Culture, Theory, Policy, Action 4, no. 1 (2000): 118; also, John Urry, 'Time, Leisure and Social Identity', Time & Society 3, no. 2 (1994): 131-149.
[124] On measuring the various components of 'social acceleration'—technological acceleration, acceleration of social change, acceleration of the pace of life—see, Rosa, 'Social Acceleration', 81-87.
[125] The problem of time lags was first discussed by Milton Friedman, 'The Lag in Effect of Monetary Policy', Journal of Political Economy 69, no. 5 (1961): 447-466.

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', between the recognition of the problem and policy responses, also known as the 'decision lag', 'administration lag' or 'implementation lag'.[126] The 'outside lag' or 'effectiveness lag' is the time taken for authoritative action to have a measurable effect on the economy. By analogy, cyber security has in most countries passed through a long period of recognition lag, as cyber security problems are today generally recognised 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 differs between states 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 specific 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.[127] 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'.[128] 'To put a pessimistic face on it', writes one, 'risks are unmeasurable, we run on hamster wheels of pain, and budgets are

[126] The policy lag 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'; H.G. Wells, The Work, Wealth and Happiness of Mankind, new and rev. edn. (London: William Heinemann, 1934/1931), 584.
[127] Philip Bobbitt, Terror and Consent: The Wars for the Twenty-First Century (London: Penguin, 2008), 234.
[128] O. Sami Saydjari, quoted in Greg Bruno, 'Backgrounder: The Evolution of Cyber Warfare', The New York Times, 27 February 2008.

slashed'.[129]. Just as the biotemporality of man is incapable of operating at the same speed as computer networks, so the sociotemporality of politics would seem to trail behind the sociotechnical environments enabled by them. 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'.[130] Helga Nowotny suggests that

> having to run faster in order to stay in one and the same spot exposes a different experience of progress, which in a relative state of being ahead can demonstrate an equal state of being behind.[131]

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'.[132] Crucially, Schneier observes, this gap increases when there is both '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

---

[129] Adam Shostack, 'The Evolution of Information Security', The Next Wave: The National Security Agency's Review of Emerging Technologies 19, no. 2 (2012): 7.
[130] Marshall McLuhan, The Mechanical Bride: Folklore of Industrial Man (Corte Madera, CA: Ginkgo Press, 2002/1951), 34.
[131] Helga Nowotny, Time: The Modern and Postmodern Experience (Cambridge: Polity Press, 1994), 49.
[132] Bruce Schneier, 'Our New Regimes of Trust', The SciTech Lawyer 9, nos. 3-4 (2013), reproduced at http://www.schneier.com/blog/archives/2013/02/our_new_regimes.html.

government to be, in most cases, successful in relating to it'.[133] When new technologies emerge, either they are left unregulated or attempts are made to regulate them with 'the old, antiquated rules'.[134] More importantly, many argue that governments and their cumbersome bureaucracies are increasingly incapable of responding effectively to internal or external events and processes.[135] The British administration is characterised as 'stodgy', staffed by senior politicians 'frozen in indecision, nervous of making mistakes, but unwilling to delegate'.[136] Recent American foreign policy, argues one author, is filled with 'bureaucrats who were paralyzed instead of energized by the demand for what Churchill used to call "action this day"'.[137]

In politics, to accuse an opponent of 'indecision' or 'dithering' is to suggest weakness, complacency and the inability to make crucial decisions befitting the office entrusted to that person.[138] Yet these are merely tactical ephemera against the backdrop of greater institutional lethargy to which all politicians are subject. Bureaucratic torpor has long been the cause 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,

[133] Ira Magaziner, 'Democracy and Cyberspace: First Principles', Democracy and Digital Media Conference, 8 May 1998, Cambridge, MA, quoted in James A. Lewis, 'Sovereignty and the Role of Government in Cyberspace', Brown Journal of World Affairs 16, no. 2 (2010): 55.
[134] Lewis, 'Sovereignty', 63.
[135] Neville Bolt, 'Unsettling Networks', The RUSI Journal 154, no. 5 (2009): 34-39.
[136] Charles Guthrie, 'Dumbed-Down Defenders of Their Own Turf', The Times, 27 August 2009, quoted in ibid., 38.
[137] Joshua Cooper Ramo, The Age of the Unthinkable: Why the New World Order Constantly Surprises Us and What We Can Do About It (New York: Little, Brown and Company, 2009), 37.
[138] Male politicians often respond to such charges with renewed (and stage-managed) displays of virility, like the post-Kursk (re)construction of Russian President Vladimir Putin as a 'man of action'; Helena Goscilo, 'Putin's Performance of Masculinity: The Action Hero and Macho Sex-Object', in Putin as Celebrity and Cultural Icon, ed. Helena Goscilo (New York: Routledge, 2013), 180-205.

and other institutions', both national and international.[139] In this light, policy-making will always tend to be a somewhat slow process.

It is not entirely clear why 'slow' policy should 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.[140] Robert Hassan notes the 'abbreviated thinking' expressed by such policy and that it often pertains due to the 'pressure of social acceleration'.[141] It might be argued that the rate of change is so great that the subjective experience of relative deceleration is qualitatively more intense now than at any previous historical moment.[142] The political pressures 'to secure' may or may not be more persistent than at any other time but the experience of technological deceleration is radically and uniquely disorienting.

Paul Virilio, the French urbanist and social theorist described by one of his principal Anglophone interlocutors as 'the only contemporary radical philosopher of speed',[143] argues that the corollary of speed is inertia: 'when absolute speed, that is the speed of light, is put to work, then one hits a wall, a barrier, which is the barrier of light':

> From that moment onwards, it is no longer necessary to make any journey: one has already arrived …. The world is reduced, both in terms of surface and extension, to nothing, and this results in a kind of incarceration, in a stasis, which means that it is no

[139] Ian Hosein, 'The Sources of Laws: Policy Dynamics in a Digital and Terrorized World', The Information Society: An International Journal 20, no. 3 (2004): 187.
[140] The reactions of the US and its allies to 9/11 have occasioned much reflection on this thesis. See, Richard English, Terrorism: How to Respond (Oxford: Oxford University Press, 2009).
[141] Hassan, Empires of Speed, 98.
[142] Rosa, 'Social Acceleration'.
[143] John Armitage, 'Accelerated Aesthetics: Paul Virilio's The Vision Machine', Angelaki: Journal of the Theoretical Humanities 2, no. 3 (1997): 206.

> longer necessary to go towards the world, to journey, to stand up, to depart, to go to things. Everything is already there.[144]

This vision of a technologized 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 such inertia does not yet exist, only acceleration and deceleration. This 'realm of mobility and anticipation', as Virilio calls it,[145] 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'.[146] Elsewhere, the report quoted earlier government policy to the effect that '[e]vents in cyberspace can happen at immense speed, outstripping traditional responses'.[147] 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'.[148] Stated baldly, the 'pace of events can make existing defences and responses look slow and inadequate.[149] This does not prevent government from aspiring to keep pace: 'In a domain where technology and change are fast-moving, responding effectively

[144] John Armitage, 'From Modernism to Hypermodernism and Beyond: An Interview with Paul Virilio', Theory, Culture & Society 16, nos. 5-6 (1999): 39-40; Paul Virilio, Polar Inertia (London: Sage, 2000/1990).
[145] Armitage, 'From Modernism', 39.
[146] House of Commons Defence Committee, Defence and Cyber-Security, vol. 1, HC 106 (London: The Stationery Office, January 2013), 7.
[147] Ibid., 13.
[148] Ibid., 26.
[149] Cabinet Office, Cyber Security Strategy, 18.

will require a consistent and extensive effort',[150] involving 'people who have a deep understanding of cyberspace and how it is developing'.[151] 'We will need very agile policy decision-makers to keep up with the reality of the threats facing us'.[152] 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'.[153] The first dimension of lag is that the acceleration of sociotechnical change means existing policies can never keep pace.

The second aspect is the likelihood that any policies implemented will fall short of being able to cope with sociotechnical change. Summarised by Johannes Bauer and Michel van Eeten, a 'critical weakness of any attempt to legislate or regulate security is that specific measures may be outsmarted by new attack technologies quickly'.[154] As long ago as 2003, the US recognised that its National Strategy to Secure Cyberspace is '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'.[155] 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.[156]

[150] Ibid., 5.
[151] Ibid., 29.
[152] House of Commons Defence Committee, Defence and Cyber-Security, 26.
[153] HM Government, Cyber Security Strategy, 19-20.
[154] Johannes M. Bauer and Michel J.G. van Eeten, 'Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options', Telecommunications Policy 33, nos. 10-11 (2009): 716.
[155] White House, National Strategy, 2.
[156] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, On Cyber Warfare (London: Chatham House, 2010), 29.

One cannot help but think this is an illusion to Hillaire Belloc's satirical poem on imperialism, 'The Modern Traveller'.[157] 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 such 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,[158] although this did not appear in the UK cyber security strategy published shortly afterwards and for which the OCSIA was principally responsible.[159]

One experienced Washington insider has suggested that the pace of change is rapid but 'not blinding or impossible to describe and manage'.[160] This is because, as 'technologies mature and governments gain experience with them, they are brought into the ambit of societal control'.[161] 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.[162]

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—

[157] Hillaire Belloc, The Modern Traveller (London: Edward Arnold, 1898), 41.
[158] OCSIA presentation, London Conference on Cyberspace, 2 November 2011.
[159] Cabinet Office, Cyber Security Strategy.
[160] Lewis, 'Sovereignty', 56.
[161] Ibid., 63.
[162] White House, Cyberspace Policy Review, C12.

exemplified by a shift from bottom-up voluntarism to top-down policies coordinated by the executive[163]—can only ever be aspirational. Certainly, this ambition registers in UK cyber crime policy, in which 'our response should not only keep pace but aim to stay several steps ahead'.[164]

In a more 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'?[165] Policymakers and those who rely on their guidance—military, intelligence, security agencies, businesses, citizens, etc.—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'.[166] 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'.[167] 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'.[168]

---

[163] Richard J. Harknett and James A. Stever, 'The New World of Cybersecurity', Public Administration Review 71, no. 3 (2011): 455-460.
[164] Home Office, Cyber Crime Strategy, 6.
[165] Hassan, Empires of Speed, 17, emphasis added.
[166] Virilio, Open Sky, 25. Also, the 'timeless time' of Manuel Castells, The Information Age: Economy, Society, and Culture, vol. 1: The Rise of the Network Society, 2nd. edn. (Chichester: Wiley-Blackwell, 2010/1996), xl-xli.
[167] Paul Virilio, L'Insécurité du Territoire, 2nd. edn. (Paris: Galilée, 1993/1976), 283, quoted in Ian James, Paul Virilio (London: Routledge, 2007), 100-101.
[168] Paul Virilio and Philippe Petit, Politics of the Very Worst: An Interview by Philippe Petit, ed. Sylvère Lotringer (New York: Semiotext(e)), 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'.[169] 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.[170] What the concept of 'real time' does reveal 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. Although operational cyber security is highly automated, high-level political decisions are still a human preserve, even if, as in the US, cyber security legislation and strategic decision-making are sometimes vested in the body of the President rather than in Congress.[171] In this case, the justification is that normal legislative processes have failed—in particular, the collapse of the Cyber Security Act (2012)—and executive fiat is necessary to short-circuit the impasse caused by the decelerative lag between cyber security problem and solution.[172] This has led to accusations that the executive is seeking to circumvent the legislative process entirely, to the detriment of security and democracy.[173] This situation offers sustenance to the diagnosis of William Scheuerman:

---

[169] Nicholas Zurbrugg, 'Virilio, Stelarc and "Terminal" Technoculture', Theory, Culture & Society 16, nos. 5-6 (1999): 193, also cited in James, Virilio, 95; also, William E. Connolly, 'Speed, Concentric Cultures, and Cosmopolitanism', Political Theory 28, no. 5 (2000): 596-618.

[170] For a recent critique, see Raymond L.M. Lee, 'Global Modernity and Temporal Multiplicity', KronoScope 12, no. 1 (2012): 31-51. 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"'; H.G. Wells, Work, 122, 144. This link is acknowledged in Aaron Worth, 'Imperial Transmissions: H.G. Wells, 1897-1901', Victorian Studies 53, no. 1 (2010): 65-89.

[171] White House, Improving Critical Infrastructure Cybersecurity, Executive Order 13636, 12 February 2013; White House, Critical Infrastructure Security and Resilience, Presidential Policy Directive 21, 12 February 2013.

[172] Mark Clayton, 'Senate Cybersecurity Bill Fails, So Obama Could Take Charge', Christian Science Monitor, 16 November 2012. Since October 2012, the President is officially solely responsible for deciding when and how strategic 'cyber weapons' are used.

[173] Morgan Little, 'Executive Order on Cyber Security Builds Steam Amid Criticisms', Los Angeles Times, 2 October 2012.

> 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.[174]

Given the difficulties in steering legislative proposals through a deeply divided Congress, it is unsurprising 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.[175] This is the decelerative temporality at the heart of the politics of cyber security.

## 3.5 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 a complex interplay between measurable indices of sociotechnical change and the subjectivities of individual and collective human experience. This heterogeneous zone of dissonant 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

[174] William E. Scheuerman, Liberal Democracy and the Social Acceleration of Time (Baltimore, MD: Johns Hopkins University Press, 2004), xiv, quoted in Hassan, Empires, 165; also, Jean Chesneaux, 'Speed and Democracy: An Uneasy Dialogue', Social Science Information 39, no. 3 (2000): 407-420.

[175] 'Modernity is the transient, the fleeting, the contingent; it is one half of art, the other being the eternal and the immovable'; Charles Baudelaire, 'The Painter of Modern Life', Selected Writings on Art and Artists (Cambridge: Cambridge University Press, 1981), 403.

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 technologized world makes it hard enough to draft and implement policy without the increased rate of change itself making some policy proposals merely 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'.[176]

Cyber security would seem to be pervaded by a profound sense of frustration and disorientation at being trapped in an accelerating present, cut off from history and with no way of 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.[177] This is an historical a-consciousness emerging—in the philosophy of history—from the ashes of modernity and the unlamented death of postmodernism. Virilio articulates this dehistoricised perspective when he writes that real time marks the 'switch from the extensive time of history

[176] Rosa, 'Social Acceleration', 102; but see Vieira, 'Connecting', 382, for a dissenting perspective.
[177] Bruce Sterling, 'Atemporality for the Creative Artist', Transmediale 10, Berlin, 6 February 2010.

to the intensive time of momentariness without history'.[178] The 'open horizon' of modernity has been foreshortened in a headlong rush to the future, which 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.[179] 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 'culture of the annihilation of time, which is tantamount to the cancelling of the human adventure'.[180] 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.

[178] Paul Virilio, 'The Last Vehicle', in The Paul Virilio Reader, ed. Steve Redhead (New York: Columbia University Press, 2004), 119.
[179] Nowotny, Time, 51; also, Carmen Leccardi, 'New Temporal Perspectives in the "High-Speed Society"', in Hassan and Purser, 24/7, 28-31.
[180] Castells, Rise of the Network Society, xliii.

# 4 IMAGINING THE FUTURE

Catastrophe generates the beasts it needs.[1]

On what principle is it that, when we see nothing but improvement behind us, we are to expect nothing but deterioration before us?[2]

## 4.1 Introduction: Future and Futurity

Saint Augustine, writing in the last years of the fourth century AD, recognised that the future is not merely something that stretches ahead of us and which remains to be discovered. 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.[3] 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'.[4] 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'.[5] 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.

---

[1] China Miéville, London's Overthrow (London: Westbourne Press, 2012), 57.
[2] Thomas Babington Macaulay, 'Southey's Colloquies on Society (Jan. 1830)', Critical and Historical Essays Contributed to the Edinburgh Review, vol. 1 (London: Longman, Green, and Co., 1903), 266.
[3] Augustine, Confessions (Oxford: Oxford University Press, 1992), XI.37.
[4] Edmund Burke, Thoughts on the Cause of the Present Discontents, 3rd. edn. (London: J. Dodsley, 1770), 3.
[5] Augustine, Confessions, XI.37.

The previous chapter suggested that the future, in some historical and philosophical sense, has become 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 selves. More than this alone, the present period—which is variously labelled 'late modernity', 'high modernity', 'supermodernity', 'hypermodernity', 'transmodernity' or 'postmodernity'—has a distinctly eschatological sensibility that filters the present through the lens not merely of the future but of the final events of the world.[6]

This shift from optimistic modernity to pessimistic postmodernity has occurred over a century defined by war and trauma.[7] The positive social futurism of Victorian and Edwardian intellectuals was deeply affected, argues Richard Overy, by World War I, a disastrous adventure that enervated national spirit and dampened prior expectations of social progress.[8] This 'domestic malaise' was further exacerbated by developing concerns over demography, economy and political turmoil, a depressive atmosphere that so sensitised the British public that the 'escape into war' in 1939 came as something of an apocalyptic release.[9] After 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), people could finally begin to imagine

[6] I retain 'postmodernity', not through authorial belief in a decisive disjuncture with modernity but on account of its relative familiarity and because it reflects upon the nature of modernity as much as it does on what postmodernity itself might be; Barry Smart, Postmodernity (London: Routledge, 1992), 151-152.
[7] Pessimism, of course, has a much richer heritage than this statement implies; see, Joshua Foa Dienstag, Pessimism: Philosophy, Ethic, Spirit (Princeton, NJ: Princeton University Press, 2006).
[8] Richard Overy, The Morbid Age: Britain Between the Wars (London: Allen Lane, 2009).
[9] Ibid., 384.

a post-war world free of tyranny.[10] This feeling quickly 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'.[11] 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. 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 a space 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

[10] On these turning points, see Gerhard L. Weinberg, A World at Arms: A Global History of World War II (Cambridge: Cambridge University Press, 1994).
[11] Donna U. Gregory, 'The Dictator's Furnace', Peace Review: A Journal of Social Justice 1, no. 1 (1989): 12.

Are full of passionate intensity.[12]

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.[13] 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, such as the possibility that the Large Hadron Collider would conjure from the fabric of spacetime a black hole capable of swallowing up the Earth.[14] 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'.[15]

Media communicate other worries catalysed by science, as in our growing awareness of the transits and possible collisions of near-Earth objects (NEO) 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.[16] 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 1200

[12] William Butler Yeats, 'The Second Coming', The Collected Poems of W.B. Yeats (Ware: Wordsworth Editions, 2008), 158.
[13] Radoslav S. Dimitrov, 'Inside Copenhagen: The State of Climate Governance', Global Environmental Politics 10, no. 2 (2010): 18-24.
[14] Max Tegmark and Nick Bostrom, 'Is a Doomsday Catastrophe Likely?', Nature 438, no. 754 (2005): 754.
[15] Andrew Hoskins and Ben O'Loughlin, War and Media: The Emergence of Diffused War (Cambridge: Polity, 2010), 2. This same environment means it is ever harder to 'forget' the past; Andrew Hoskins, 'Media, Memory, Metaphor: Remembering and the Connective Turn', Parallax 17, no. 4 (2011): 19-31.
[16] BBC News, 'Asteroid 2012 DA14 in Record-Breaking Earth Pass', 15 February 2013.

people.[17] As one newspaper columnist remarked of these coincidental events, 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'.[18] 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 it in advance. Improved knowledge of our galactic neighbourhood has increased astronomical awareness and fostered a heightened sense of the prospects of catastrophe and of existential finitude.[19] There are many ways to imagine 'TEOTWAWKI'—The End of the World As We Know It.[20] We appear to be, as John Gray suggests, 'a culture transfixed by the spectacle of its own fragility'.[21]

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.[22] Perceptions of dystopia and decline shape narratives through which political change is effected and this chapter concentrates on one manifestation of these rather sombre—although often

[17] Daily Telegraph, 'Russian Meteor Exploded with Force of 30 Hiroshima Bombs', 16 February 2013.
[18] Roz Kaveney, 'The Meaning of Meteors', The Guardian, 15 February 2013.
[19] Due to widespread acceptance of the 'heat-death' of the universe, 'physical eschatology' is now a mainstream scientific concern; Helge S. Kragh, Conceptions of Cosmos—From Myths to the Accelerating Universe: A History of Cosmology (Oxford: Oxford University Press, 2007), 237-238.
[20] This common Internet slang probably originates with American band REM's song, 'It's the End of the World as We Know It (And I Feel Fine)'; REM, Document (IRS Records, 1987).
[21] John Gray, 'The Violent Visions of Slavoj Žižek', New York Review of Books, 12 July 2012.
[22] Ryan Anthony Vieira, '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 (2011): 386.

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 the '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.

## 4.2 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. He opened with some comments about the two 'types of mind … to be distinguished chiefly by their attitude toward time, and more particularly by the relative importance they attach and the relative amount of thought they give to the future':[23]

[23] H.G. Wells, The Discovery of the Future (New York: B.W. Huebsch, 1913), 4.

> The first of these two types of mind [is] the type of the majority of living people, is that which seems scarcely to think of the future at all, which regards it as a sort of blank non-existence upon which the advancing present will presently write events. The second type [is] a more modern and much less abundant type of mind, thinks constantly and by preference of things to come, and of present things mainly in relation to the results that must arise from them. The former type of mind [is] retrospective in habit, and it interprets the things of the present, and gives value to this and denies it to that, entirely with relation to the past. The latter type of mind is constructive in habit, it interprets the things of the present and gives value to this or that, entirely in relation to things designed or foreseen.[24]

Wells proceeded to describe the former mind as 'legal or submissive' and the latter as 'legislative, creative, organizing or masterful [which] sees the world as a great workshop, and the present as no more than material for the future.'[25]

Doubtless, this is the sort of panegyric to technological modernism in which those charged with securing society would wish to recognise their own talents as visionary agents blessed with no minor oracular powers. These future-minded professionals are characters in 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.[26] 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

[24] Ibid., 4-5.
[25] Ibid., 5-6.
[26] Matt Carr, 'Slouching Towards Dystopia: The New Military Futurism', Race & Class 51, no. 3 (2010): 13-32.

interaction.[27] The demise of the Soviet Union destabilised this ossified superpower enmity and ushered in a dynamic world of rapidly evolving risk and threats. 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.[28]

On 11 September 2001, this thesis seemed to have been confirmed, 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 new willingness amongst the US national security establishment to consider further "strategic shocks" by "imagining 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'.[29] Those charged now 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'.[30] 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'.[31] The new military futurism intends to counter exactly the 'submissive' mindset identified by Wells, which

[27] This is not to oversimplify Cold War dynamics, however; see, John Mueller, Quiet Cataclysm: Reflections on the Recent Transformation of World Politics (New York: HarperCollins, 1995), 14-16.
[28] Herfried Münkler, The New Wars (Cambridge, Polity Press, 2005); Mary Kaldor, New and Old Wars: Organized Violence in a Global Era, 2nd. edn. (Cambridge: Polity Press, 2006/1999).
[29] Carr, 'Slouching', 16.
[30] Ibid., 18.
[31] Ibid.

views the future as 'a perpetual source of convulsive surprises, as an impenetrable, incurable, perpetual blankness'.[32]

However, this new military futurism is not the body of knowledge envisioned by Wells when 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'.[33] 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'.[34] 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'.[35] 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. 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 mind-set to the security imaginary more broadly, as there are affinities with the ways in which cyber security futures are imagined. However,

---

[32] Wells, Discovery, 21.
[33] Ibid., 35.
[34] Claudia Aradau and Rens van Munster, Politics of Catastrophe: Genealogies of the Unknown (London: Routledge, 2011), 69-70.
[35] Ibid., 70. Science and imagination are not mutually exclusive: 'Facts and ideas are dead in themselves and it is the imagination that gives life to them'; W.I.B. Beveridge, The Art of Scientific Investigation, rev. edn. (New York: W.W. Norton and Company, Inc., 1957/1950), 58. Similarly, Dawkins supports imagination as a way of countering the 'anaesthetic of familiarity, a sedative of ordinariness', to which we are habituated and which 'dulls the senses and hides the wonder of existence'; Richard Dawkins, Unweaving the Rainbow: Science, Delusion and the Appetite for Wonder (London: Penguin Books, 1998), 6.

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, such as the radio, telegraph and telephone.[36] He notes the genealogy of anxiety accompanying the development of interconnected and interdependent infrastructures in modern industrial societies, worries consistent with general apprehension about the impact of new technologies on society. As Marshall McLuhan observed in 1967 of new developments in communications, 'wherever a new environment goes around an old one there is always new terror'.[37]

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, social alienation, to mention but a few, all of which have induced periodic public spasms of moral panic.[38] For 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

[36] Sean Lawson, 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats', Journal of Information Technology & Politics 10, no. 1 (2013): 86-103.
[37] Canadian Broadcasting Corporation, 'Marshall McLuhan in Conversation with Norman Mailer', The Way It Is, 26 November 1967.
[38] Alice Marwick, 'To Catch a Predator? The MySpace Moral Panic', First Monday 13, no. 6 (2008), n.p.; Adam Thierer, 'Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle', Minnesota Journal of Law, Science & Technology 14, no. 1 (2013): 309-386.

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 standard expression of this orientation:

> [Cyber security is about] our struggle to have our cake and eat it too—about how we try to reap the benefits in productivity and information sharing that come from a globalized web of cyber connections while somehow managing to avoid (or at least reduce) the damage done by malfeasant actors who seek to take advantage of that globalized web for their own reasons.[39]

On 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'.[40]

However, it is the darker visions of possible security futures that give principal sustenance to the cyber security imaginary. As Carr asserts, American military futurism is one response to the apparent decline of the United States as the pre-eminent political—if not military—power.[41] 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. This taps into existing stereotypes, cultural categories 'whose subjective resources can be quite easily activated'.[42] 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 racialized 'Yellow Peril',

---

[39] Paul Rosenzweig, Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World (Santa Barbara, CA: ABC-CLIO, 2013), 2.
[40] HM Government, Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, Cm. 7948 (Norwich: The Stationery Office, October 2010), 47.
[41] Carr, 'Slouching'.
[42] Alain Badiou, Infinite Thought: Truth and the Return to Philosophy (London: Continuum, 2005), 114.

although one should not dismiss China's stated strategic aims or the demonstrable activities of Chinese entities in this space.[43] 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'.[44]

## 4.3 Catastrophe and Apocalypse

In postmodernity, 'the future looks less like the past than ever before and has in some basic ways become very threatening'.[45] In the cyber security imaginary, we might suggest, 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. It is a key discursive strategy in cyber security 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.[46] Given the historical dearth of comparable events, these events are necessarily the product of

[43] On US-China cyber security rhetoric and national stereotyping, see Stephen John Hartnett, 'Google and the "Twisted Cyber Spy" Affair: US-Chinese Communication in an Age of Globalization', Quarterly Journal of Speech 97, no. 4 (2011): 411-434. On the 'Yellow Peril', see Doobo Shim, 'From Yellow Peril through Model Minority to Renewed Yellow Peril', Journal of Communication Inquiry 22, no. 4 (1998): 385-409.
[44] Carr, 'Slouching', 18.
[45] Ulrich Beck, Anthony Giddens and Scott Lash, Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order (Cambridge: Polity Press, 1994), vii.
[46] See Chapter Five.

the security imaginary and 'remain fiction, not to say science fiction'.[47] Although we cannot pursue here the rich history of science fiction as a genre instrumental to national security thinking,[48] it is necessary to note that the sorts of catastrophes which populate the science-fictional imagination as applied to security are 'both the stuff of Hollywood films and the product of expert imagination'.[49]

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.[50] 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'.[51] These scenarios are examples of a tendency in cyber security towards 'hypersecuritisation', in which discourse 'hinges on multi-dimensional 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'.[52] Richard Clarke and Robert Knake's book, Cyber War (2010) contains a five-page description of what could happen if cyber security is not sufficiently addressed in the present.[53] As 'cyber warriors' assault the critical national information infrastructures of the United States, aircraft fall from the sky, trains are derailed in their dozens, cars crash as traffic control networks go down, 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

[47] Thomas Rid, Cyber War Will Not Take Place (London: Hurst & Company, 2013), 4; also, Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008), 56-57.
[48] Charles E. Gannon, 'Imag(in)ing Tomorrow's Wars and Weapons', Peace Review: A Journal of Social Justice 21, no. 2 (2009): 198-208; Patrick Jagoda, 'Speculative Security', in Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 21-35.
[49] Aradau and van Munster, Politics of Catastrophe, 69.
[50] Dunn Cavelty, Cyber-Security, 2-4.
[51] Ibid., 3.
[52] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly 53, no. 4 (2009): 1164, original emphasis.
[53] Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (New York: Ecco, 2010), 64-68.

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.

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.[54] Infrastructure failure might not just cascade through physical infrastructures but could ripple into the affective realm.[55] It 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'.[56] It is not 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'.[57] 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'.[58]

More important than whether such catastrophic events will happen or not is that by definition they have not yet happened. That is, they are always in the future, whether they eventually occur in some future present or not. Read through the lens of securitisation theory—which

[54] Richard G. Little, 'Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures', Journal of Urban Technology 9, no. 1 (2002): 109-123.
[55] Following Massumi's interpretation of Deleuze and Guattari (and before them, Spinoza), 'affect' is used here as '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'; Gilles Deleuze and Félix Guattari, Capitalism and Schizophrenia, vol. 2, A Thousand Plateaus (London: Continuum, 2004/1980), xvii.
[56] Philip Bobbitt, Terror and Consent: The Wars for the Twenty-First Century (London: Penguin, 2008), 96.
[57] J. Peter Burgess, 'Social Values and Material Threat: The European Programme for Critical Infrastructure Protection', International Journal of Critical Infrastructures 3, nos. 3-4 (2007): 481.
[58] Howard A. Schmidt, Patrolling Cyberspace: Lessons Learned from a Lifetime in Data Security (North Potomac, MD: Larstan Publishing, Inc., 2006), 172.

stresses the speaking-into-being of security threats through which to mobilise political resources—these constructed 'cyber doom' scenarios perform political work.[59] As Myriam Dunn Cavelty concludes in her exhaustive analysis of US cyber security policy, 'in theory, it does not matter whether the threat is real or not: what matters is that decision-makers consider cyber-attacks a real threat and act accordingly'.[60] This is not to ignore the practical ramifications of addressing 'real' security issues, nor of ignoring them, but it does stress that these future scenarios can be nothing other than imaginative constructs, no matter how 'expert' that imagination is. The question here is to examine further the political aspects of the temporality of these constructions of catastrophe that are not reducible merely to their interpretations as securitising speech acts. In their role as future events through which present politics are shaped, cyber catastrophes represent an eschatological dimension of cyber security and 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.

Although the present enquiry attempts to delineate 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 explicit references to religious apocalypse in cyber security discourses. 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 suggests, is 'a cyber attack that could wreak havoc on the nation by bringing down critical information infrastructures'.[61] So pervasive is the

[59] For a recent review of academic work on how cyber security issues are securitised, threats constructed and political resources mobilised, see Myriam Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', International Studies Review 15, no. 1 (2013): 105-122.
[60] Dunn Cavelty, Cyber-Security, 143.
[61] Bernadette Schell and Clemens Martin, Webster's New World Hacker Dictionary (Indianapolis, IN: Wiley Publishing, Inc., 2006), 78.

contemporary 'fear' of 'devastating viruses and worms' that the period from 2001 onwards is presented as the 'Fear of a Cyber Apocalypse Era'.[62] It is 'only a matter of time', we read, 'before cyberterrorists are able to unleash a cyber apocalypse'.[63] When it happens, this cataclysmic event will 'make 9/11 look like a tea party'.[64]

One commentator, inviting professional fraternity, wrote, '"Cyber-geddon" is imminent. I am hardly alone'.[65] 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'.[66] 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'.[67] Although these professionals are in a minority in voicing their fears that a literal 'cybergeddon'—whatever that actually means—is imminent, and many others are openly skeptical, this does not alleviate a widespread sense of fatalism in cyber security discourses.[68] The 'sky is falling', writes one defence information security professional, 'but very slowly'.[69]

These Biblical allusions are not uncommon but should not be read in a superficial sense: 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.[70] The ubiquitous sense of doom is a key indicator of a more entrenched apocalyptic aspect of cyber

[62] Ibid., xxv.
[63] Kelly A. Gable, 'Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent', Vanderbilt Journal of Transnational Law 43 (2010): 118.
[64] The Economist, 'Hype and Fear', 8 December 2012, 62.
[65] Adam Levin, 'How the SEC Almost Shut Down Wall Street' Huffington Post, 15 November 2012.
[66] Preet Bharara, 'Asleep at the Laptop', The New York Times, 4 June 2012.
[67] Tova Cohen and Maayan Lubell, 'Nations Must Talk to Halt "Cyber Terrorism"—Kaspersky', Reuters, 6 June 2012.
[68] Misha Glenny, 'Virtual Warfare in Race to Avoid "Doomsday"', The Guardian, 17 May 2011; Jason Healey, 'The Five Futures of Cyber Conflict and Cooperation', Georgetown Journal of International Affairs 11, no. 1 (2010): 110-117.
[69] Kenneth Geers, 'The Cyber Threat to National Critical Infrastructures: Beyond Theory', Information Security Journal: A Global Perspective 18, no. 1 (2009): 4.
[70] Ian Stronach, John Clarke and Jo Frankham, 'Economic "Revelations" and the Metaphors of the Meltdown: An Educational Deconstruction', British Educational Research Journal, forthcoming, fn.14.

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.[71]

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.[72] The historical details and specificity of each entity in this roll-call of malware, sabotage operations, government exercises, countries and espionage programs is less important than their construction as discrete 'events' that populate and corroborate the apocalyptic narrative. In cyber war narratives, a particular example of the cyber security apocalypse, these events become 'signifiers of the no-longer-future-but-reality of cyber war'.[73] 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 in which isolated events impart an increasingly cohesive structure to the temporality of the present.[74] 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'.[75]

---

[71] Thomas Robbins and Susan J. Palmer, 'Patterns of Contemporary Apocalypticism in North America', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements (New York: Routledge, 1997), 4-5.

[72] Y2K is occasionally mentioned and is a computer-related 'event' interpreted also as a sign of a more general impending apocalypse, or even the Apocalypse itself; Nancy A. Schaefer, 'Y2K as an Endtime Sign: Apocalypticism in America at the Fin-de-Millennium', The Journal of Popular Culture 38, no. 1 (2004): 82-105; Karen Pärna, 'Digital Apocalypse: The Implicit Religiosity of the Millennium Bug Scare', in Religions of Modernity: Relocating the Sacred to the Self and the Digital, eds. Stef Aupers and Dick Houtman (Leiden: Brill, 2010), 239-259.

[73] Dunn Cavelty, 'Cyber-Bombs', 117.

[74] Marc R. Beissinger, Nationalist Mobilization and the Collapse of the Soviet State (Cambridge: Cambridge University Press, 2002), 27.

[75] James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', Survival 53, no. 1 (2011): 23-40.

Prophets tend to be self-appointed and there has been 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',[76] 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'.[77] These scenarios are often the products of the 'expert imagination' and perhaps should not be dismissed lightly, given the possible consequences of doing so.[78] Again, the framing of apocalypse is of most interest, particularly with direct reference to those who self-identify as prophets, like 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.[79]

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.[80] 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

---

[76] Horace Walpole, 'Letter to Thomas Walpole the Younger, Saturday 19 February 1785', Horace Walpole's Correspondence, vol. 36, ed. W.S. Lewis (New Haven, CT: Yale University, 1973), 233.
[77] Thomas Rid, 'Cyber War Will Not Take Place', Journal of Strategic Studies 35, no. 1: 6. As Rid is aware, the importance of Cassandra is not that people thought her a false prophet but that her correct predictions were ignored.
[78] Hansen and Nissenbaum, 'Digital Disaster', 1164. Richard Clarke, currently a first-rank cyber doom-monger, was better known previously as 'the Cassandra of the war on terror', whose warnings of a 9/11-type attack on the US were ignored; Paul Harris, 'Living with 9/11: The Anti-Terror Chief', The Guardian, 6 September 2011. Also, Lee Clarke, Worst Cases: Terror and Catastrophe in the Popular Imagination (Chicago, IL: University of Chicago Press, 2006).
[79] Eugene Kaspersky, 'Cassandra Complex … Not For Much Longer', Nota Bene, 17 March 2012.
[80] Annual cyber security spending may already have reached $80-150 billion per annum; Ronald J. Deibert and Rafal Rohozinski, 'The New Cyber Military Industrial Complex' The Globe and Mail, 28 March 2011.

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.[81] They do 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'.[82] They have in common that 'the error revealed by the non-fulfillment of such an expectation itself [becomes] proof that the next forecast of the End of the World [is] even more probable'.[83] 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' remains firm.

The level of 'apocalyptic intensity' already elevated through the reading of signs can be heightened further by making predictions that are 'imminent but indeterminate', creating 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'.[84] This leaves futuristic scenarios deliberately 'shrouded in a cloud of speculation'.[85] This is an established tactic of national 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.[86] In common with other forms of security, cyber security

[81] This 'unfalsifiable cyber-augury' has been identified in other areas of 'guru'-led Internet prediction; Steven Poole, 'Invasion of the Cyber Hustlers', New Statesman, 6 December 2012.
[82] Daniel Wojcik, The End of the World as We Know It: Faith, Fatalism, and Apocalypse in America (New York: New York University Press, 1997), 148. In national security circles, Erskine Childers described such a person as a 'meddlesome alarmist, who veils ignorance under noisiness, and for ever wails his chant of lugubrious pessimism'; Erskine Childers, The Riddle of the Sands: A Record of Secret Service (London: Penguin, 1995/1903), 98.
[83] Reinhart Koselleck, Futures Past: On the Semantics of Historical Time (New York: Columbia University Press, 2004/1979), 265.
[84] David G. Bromley, 'Constructing Apocalypticism: Social and Cultural Elements of Radical Organization', in Robbins and Palmer, Millennium, 36.
[85] Dunn Cavelty, Cyber-Security, 4.
[86] R.B.J. Walker, 'The Subject of Security', in Critical Security Studies: Concepts and Cases, eds. Keith Krause and Michael C. Williams (London: Routledge, 1997), 63.

invokes 'realities and necessities that everyone is supposed to acknowledge, but also vague generalities about everything and nothing'.[87] Ignorance, it seems, can sometimes be strategic.[88]

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.[89] These scripts of the future gain explanatory power when events and scenarios appear to converge and potentially increase the volatility of those subscribing to such an outlook, particularly if already psychologically stressed.[90] Given the tendency to construct apocalypse in dualist terms, millenarian scripts usually have entities playing each of the 'good' and 'bad' roles. In this way, as happened at Waco in 1993, the actions of government may cause it to play one of those roles, acting in ways already 'scripted' in advance, unwittingly bringing about exactly the apocalypse 'predicted' by believers.[91]

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:

---

[87] Ibid.
[88] Linsey McGoey, 'Strategic Unknowns: Towards a Sociology of Ignorance', Economy & Society 41, no. 1 (2012): 1-16.
[89] Robbins and Palmer, 'Patterns', 5.
[90] Ibid.
[91] Michael Barkun, 'Millenarians and Violence: The Case of the Christian Identity Movement', in Robbins and Palmer, Millennium, 256. See, Christopher Keep, '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, 1995), 262-274; Stuart A. Wright, 'Anatomy of a Government Massacre: Abuses of Hostage-Barricade Protocols during the Waco Standoff', Terrorism & Political Violence 11, no. 2 (1999): 39-68.

> For those new to cybersecurity, all worms and viruses look catastrophic …. Like the monsters in your imagination, these phantoms can take on a persona of an unrelenting danger that easily surpasses their true capabilities. We must guard against this.[92]

Sometimes these beasts are real but as 'ominous as the dark side of cyberspace may be, our collective reactions to it are just as ominous—and can easily become the darkest driving force of all should we over react'.[93] 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.

## 4.4 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.[94] Lewis cites the apocalypse movie 2012 (dir. Roland Emmerich, 2009), in which Los Angeles is spectacularly destroyed by earthquake and consigned to the ocean. Los Angeles' 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

---

[92] Schmidt, Patrolling Cyberspace, 124-125.
[93] Ronald J. Deibert, 'The Growing Dark Side of Cyberspace (…and What To Do About It)', Penn State Journal of Law & International Affairs 1, no. 2 (2012): 261.
[94] Jeff Lewis, Global Media Apocalypse: Pleasure, Violence and the Cultural Imaginings of Doom (Basingstoke: Palgrave Macmillan, 2012), 97.

Davis as 'Doom City', permanently on the edge of disaster.[95] 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 20th century.[96] 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.[97] However, Los Angeles' marginal existence means it is destined one day to be destroyed, at least in part, 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 suggest humanity's complicity in its own downfall rather than a mere dumb recipient of cosmic ill fortune.[98] Like other commentators on the American condition, 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'.[99] Thoreau's analysis of modernisation does not restrict itself to the effects of man on nature. In one striking passage, he writes of the impact of man's technology on man, 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

[95] Mike Davis, Ecology of Fear: Los Angeles and the Imagination of Disaster (New York: Vintage Books, 1999).
[96] Ibid., 276.
[97] See, William M. Tsutsui, '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, NJ: Princeton University Press, 2010), 104-126; Anthony Taylor, London's Burning: Pulp Fiction, the Politics of Terrorism and the Destruction of the Capital in British Popular Culture, 1840-2005 (London: Continuum, 2012).
[98] Raymond Murphy, 'Nature's Temporalities and the Manufacture of Vulnerability: A Study of a Sudden Disaster with Implications for Creeping Ones', Time & Society 10, nos. 2-3 (2001): 329-348.
[99] Davis, Ecology of Fear, 15.

> few are riding, but the rest are run over,—and it will be called, and will be, 'A melancholy accident'.[100]

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'.[101] Rather than cancel the event, the railway directors decided to proceed, in order to show that the incident was 'a mere accident, and had not happened through any fault of the machinery'.[102] 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'.[103] The verse of one contemporary poet reflected this conclusion, recording that Huskisson by 'unforeseen mischance was over-run'.[104] 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.[105]

This perspective is familiar to critics of technology, from the machine-breaking Luddites of the 19th century to the anarchists and primitivists of the 20th and 21st centuries, who see in technology the seeds both of its own downfall and of society itself. George Woodcock observed that it is 'a frequent circumstance of history that a culture or civilization develops the

---

[100] Henry David Thoreau, Walden (London: Walter Scott, 1888/1854), 52.
[101] For example, The Times, 'Dreadful Accident to Mr. Huskisson', 17 September 1830, quoted in William Pietz, 'Death of the Deodand: Accursed Objects and the Money Value of Human Life', RES: Anthropology & Aesthetics 31 (1997): 99.
[102] Ibid.
[103] The Times, 'Death of Mr. Huskisson', 18 September 1830, quoted in Pietz, 'Death of the Deodand', 99.
[104] Thomas Baker, The Steam Engine; or, The Powers of Steam. An Original Poem in Ten Cantos (London: J.S. Hodson, 1857), canto X.3, p. 189, quoted in Peter Viereck, 'The Poet in the Machine Age', Journal of the History of Ideas 10, no. 1 (1949): 91.
[105] Or through the malignant intent of inanimate objects, belief in the existence of which was parodied as the French philosophy of Resistentialisme—'les choses sont contre nous'; Paul Jennings, 'Report on Resistentialism', The Spectator 180, no. 6252 (1948): 491. Also, Daniel C. Dennett, Elbow Room: The Varieties of Free Will Worth Wanting (Oxford: Oxford University Press, 1984), 61-62.

device that will later be used for its destruction'.[106] 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.[107] 'Technology' is seen as a unitary if internally heterogeneous entity, possessive of an auto-generative 'life force', a view shared with some contemporary technophiles.[108] Moreover, once en train, 'technological progress marches in only one direction; it can never be reversed'.[109] 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.[110]

Wolfgang Schivelbusch suggests 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.[111] 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, 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'.

---

[106] George Woodcock, 'The Tyranny of the Clock', in The Anarchist Reader, ed. George Woodcock (Hassocks: Harvester Press, 1977), 133.
[107] Theodore Kaczynski, Industrial Society and Its Future (1995).
[108] Kevin Kelly, What Technology Wants (New York: Viking, 2010).
[109] Kaczynski, Industrial Society, paragraph 129.
[110] Uri Gordon, 'Anarchism and the Politics of Technology', WorkingUSA: The Journal of Labor & Society 12, no. 3 (2009): 489-503.
[111] Wolfgang Schivelbusch, The Railway Journey: The Industrialization of Time and Space in the 19th Century (Berkeley, CA: University of California Press, 1986/1977), 131.

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, because they are not only 'unexpected', 'incomprehensible' and 'uncontrollable' but also 'unavoidable'.[112] Far from ameliorating 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.[113] 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'.[114] Even if we could somehow attain perfect 'system knowledge', we can 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.[115] 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. As Perrow, Schivelbusch and others also recognised, to 'invent the train is to invent derailment; to invent the ship is to invent the shipwreck'.[116] 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

---

[112] Charles Perrow, 'Normal Accident at Three Mile Island', Society 18, no. 5 (1981): 17-26.
[113] Charles Perrow, Normal Accidents: Living with High-Risk Technologies, 2nd. edn. (Princeton, NJ: Princeton University Press, 1999/1984). This is also a thesis proposed by Beck et al, Reflexive Modernization, vii.
[114] Perrow, Normal Accidents, 11.
[115] Rae Zimmerman, 'Social Implications of Infrastructure Network Interactions', Journal of Urban Technology 8, no. 3 (2001): 97-119.
[116] Paul Virilio and James Der Derian, '"Is the Author Dead?"—An Interview with Paul Virilio', in The Virilio Reader, ed. James Der Derian (Malden, MA: Blackwell Publishers, 1998), 20.

the absolute velocity of electromagnetism. When this occurs, the accident is no longer local but 'general', as radioactive fallout and information circulate globally.[117]

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'; 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'.[118] Virilio saw in the 1987 stock market crash 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.[119] 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.[120] In the previous chapter, we encountered Virilio's conception of speed and 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'.[121]

---

[117] Paul Virilio, Open Sky (London: Verso, 1997/1995), 70.

[118] Paul Virilio and Philippe Petit, Politics of the Very Worst: An Interview by Philippe Petit, ed. Sylvère Lotringer (New York: Semiotext(e), 1999/1996), 91.

[119] Paul Crosthwaite, 'The Accident of Finance', in Virilio Now: Current Perspectives in Virilio Studies, ed. John Armitage (Cambridge: Polity, 2011), 177-199.

[120] Paul Virilio, Gérard Courtois and Michel Guerrin, 'Le Krach Actuel Représente l'Accident Intégral par Excellence', Le Monde, 18 October 2008, author's translation; also, Eric Wilson, 'Criminogenic Cyber-Capitalism: Paul Virilio, Simulation, and the Global Financial Crisis', Critical Criminology 20, no. 3 (2012): 249-274. On apocalyptic discourses in finance journalism during this period, see Stronach et al, 'Economic "Revelations"'.

[121] Kimberly Hutchings, Time and World Politics: Thinking the Present (Manchester: Manchester University Press, 2008), 131. 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. It could have been avoided by alternative political action, the possibilities of which, under conditions of the technological accident, Virilio mostly discards; Raymond Aron, 'The Dawn of Universal History', Politics and History, ed. Miriam Bernheim Conant (New Brunswick, NJ: Transaction Publishers, 1984/1978), 224.

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.[122] 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 it's a systemic crash that's purely accidental, what do you do?'[123] Virilio echoes here one of the key—and historically most intractable—epistemological concerns at the core of cyber security practice and politics: the 'attribution problem'.[124]

The 'problem' is simultaneously evidentiary and technical, normative and legal, political and strategic, 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 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

[122] US Commodity Futures Trading Commission and US Securities and Exchange Commission, 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, September 2010).
[123] Paul Virilio, The Great Accelerator (Cambridge: Polity, 2012/2010), 79-80.
[124] Few cyber security discussions ignore the attribution problem. Extensive treatments include: Susan W. Brenner, Cyberthreats: The Emerging Fault Lines of the Nation State (New York: Oxford University Press, 2009), 71-161; Martin C. Libicki, Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND Corporation, 2009); Rid, Cyber War, 139-162.

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, such as 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 and seeks to create and exploit the 'strategic ambiguity' 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.[125] What matters more than establishing the cause of an

[125] On the emergence of resilience as a concept, see Jeremy Walker and Melinda Cooper, 'Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation', Security Dialogue 42, no. 2 (2011): 143-160.

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'.[126] Cyber security is not only about 'strengthening defences' to prevent attacks but also 'improving resilience and diminishing the impact of cyber attacks'.[127] 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. Although we know that the accident will occur, 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.[128] 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'.[129]

---

[126] Yacov Y. Haimes, Kenneth Crowther and Barry M. Horowitz, 'Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems', Systems Engineering 11, no. 4 (2008): 291.
[127] Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (London: Cabinet Office, 2011), 39.
[128] Myriam Dunn Cavelty and Jennifer Giroux, '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, forthcoming).
[129] Bruce Schneier, 'Our Security Models Will Never Work—No Matter What We Do', Wired, 14 March 2013.

Resilience as a response to an epistemological shortfall discounts causality and intent and implicitly recognises 'an inherent ontological insecurity within computer systems'.[130] The pioneering computer scientist Grace Hopper remarked, 'Life was simple before World War II. After that, we had systems'.[131] With these systems came 'bugs', two categories of which were soon formalised.[132] 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 as the 'garbage in, garbage out' principle.[133] Removing all bugs from a large system ('debugging') is, unfortunately for the computer security professional, 'provably impossible'.[134] 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.[135]

No information system can claim to be wholly secure, a condition recognised over four decades ago: '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'.[136] 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. Whether humans or machines cause 'cyber' accidents is less important than understanding that people and machines are embedded in systems that make accidents inevitable and unavoidable. In their eschatological dimensions, the accident and the

---

[130] Hansen and Nissenbaum, 'Digital Disaster', 1160.
[131] Philip Schieber, 'The Wit and Wisdom of Grace Hopper', The OCLC Newsletter 167 (1987), n.p.
[132] Stanley Gill, 'The Diagnosis of Mistakes in Programmes on the EDSAC', Proceedings of the Royal Society A 206, no. 1087 (1951): 538-554.
[133] William Lidwell, Kritina Holden and Jill Butler, Universal Principles of Design, rev. edn. (Gloucester, MA: Rockport Publishers, 2010/2003), 112-113.
[134] Paul N. Edwards, The Closed World: Computers and the Politics of Discourse in Cold War America (Cambridge, MA: MIT Press, 1996), 291; Donald Mackenzie and Garrel Pottinger, 'Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the US Military', IEEE Annals of the History of Computing 19, no. 3 (1997): 41-59.
[135] Michael Näf, 'Ubiquitous Insecurity? How to "Hack" IT Systems', Information & Security 7 (2001): 104-118.
[136] Bernard Peters, 'Security Considerations in a Multi-Programmed Computer System', Proceedings of the 1967 Spring Joint Computer Conference 30 (1967): 283.

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'.[137] 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.

## 4.5 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'.[138] 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' has become not only a staple of popular culture but is congruent with secular and religious imaginings of 'the end'. Indeed, the 'world after the world, the post-apocalypse, is usually the true object of the apocalyptic writer's concern',

[137] Klaus R. Scherpe, 'Dramatization and De-dramatization of "the End": The Apocalyptic Consciousness of Modernity and Post-Modernity', Cultural Critique 5 (1986): 96, original emphasis.
[138] Jean Baudrillard, 'The End of the Millennium or the Countdown', Economy & Society 26, no. 4 (1997): 448.

whether imagined as 'paradise or wasteland'.[139] 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'.[140] 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'.[141] 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'.[142] Virilio does not dispense with a secular apocalyptic reading of the accident, however, especially in his insistence on 'exposing the accident' as a way of understanding technologized society and thereby to query and resist its political foundations.[143] 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'.[144] 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.[145] Elsewhere, Virilio has

---

[139] James Berger, After the End: Representations of Post-Apocalypse (Minneapolis, MN: University of Minnesota Press, 1999), 6.
[140] James A. Aho, 'The Apocalypse of Modernity', in Robbins and Palmer, Millennium, 65.
[141] Mark Featherstone, 'Virilio's Apocalypticism', CTheory, 16 September 2010.
[142] Paul Virilio, The Original Accident (Cambridge: Polity, 2007/2005), 28. This is presumably also the sense intended when he says, 'this new notion of the accident has nothing to with the Apocalypse'; Virilio and Petit, Politics of the Very Worst, 93; also, Paul Virilio and Nicholas Zurbrugg, 'Not Words But Visions! Interview with Nicholas Zurbrugg (1998)', in Virilio Live: Selected Interviews, ed. John Armitage (London: Sage, 2001), 156.
[143] Virilio, Original Accident, 29.
[144] Antoine Bousquet, 'Time Zero: Hiroshima, September 11 and Apocalyptic Revelations in Historical Consciousness', Millennium: Journal of International Studies 41, no. 2 (2006): 756.
[145] Hutchings, Time, 141.

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'.[146]

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'.[147] In this case, infrastructure is the physical and organisational substructure essential for the maintenance and progressive functionality of society as a whole. Although 'infrastructure' is itself a 20th-century coinage, what we today would classify as infrastructures are attested archaeologically, such as 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 solely pragmatic contributions to the common good but symbolic and constitutive of political power and control, and expressions 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'.[148]

---

[146] Paul Virilio and John Armitage, 'The Third War: Cities, Conflict and Contemporary Art: Interview with Paul Virilio, in Armitage, Virilio Now, 39.
[147] 'Infrastructure', OED Online, December 2012.
[148] Stephen Graham and Simon Marvin, Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition (London: Routledge, 2001), 41.

Infrastructure, even in today's managerial political climate, may still be an expression and source of this civic spirit.[149] 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' includes a new 'cloaca maxima' for the city.[150]

Information infrastructures are not only just unseen but un-cognised: for most people, the existence of infrastructures is 'more or less imaginary'.[151] 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'.[152]

> Internet infrastructure, and its use, is often taken for granted because, unlike roads or railways, it is largely invisible—buried underground, snaking across ocean floors, hidden inside wall conduits, or floating unseen in orbit above us. Indeed, given its invisibility, it is easy to assume that it is as ethereal and virtual as the information and communication that it supports.[153]

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'.[154] This physical

---

[149] Stanley Greenberg, Invisible New York: The Hidden Infrastructure of the City (Baltimore, MD: Johns Hopkins University Press, 1998). On the decline of the infrastructural ideal, see Maria Kaika and Erik Swyngedouw, 'Fetishizing the Modern City: The Phantasmagoria of Urban Technological Networks', International Journal of Urban & Regional Research 24, no. 1 (2000): 121-138.

[150] Boris Johnson, 'It Will Take a Super-Sewer to Get London Out of This Mess', Daily Telegraph, 12 September 2011.

[151] Burgess, 'Social Values', 476.

[152] Joseph W. Bazalgette, On the Main Drainage of London and the Interception of the Sewage from the River Thames (London: William Clowes and Sons, 1865), 3.

[153] Martin Dodge and Rob Kitchin, '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, 2004), 160.

[154] Stephen Graham and Nigel Thrift, 'Out of Order: Understanding Repair and Maintenance', Theory, Culture & Society 24, no. 3 (2007): 2.

manifestation of 'virtual' infrastructures is a key component of the violent scenarios described by apocalyptic cyber security discourses and, following Heidegger, 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.[155] The personal computer, for instance, is taken entirely for granted until it malfunctions:

> The trustworthy world that developed around the computer …. is abruptly destroyed …. Its transparency is transformed into opacity. The computer can no longer be utilized in the practice of writing, but abruptly demands interaction with itself. The relation with the world around the computer that took place 'through' it is disturbed. Only when it starts up again and everything works without a hitch is the world that was destroyed again restored.[156]

We can scale this concern with the proper functioning of information technology to the societal level. The coupling of electrical and electronic infrastructures is revealed in its messy complexity by cascading failures:

> Together this infrastructure materially represents and sustains the trompe l'oeil of otherworldly immateriality while simultaneously depending upon a physical assemblage of wires, plugs, and sockets to distribution lines and poles, transformers,

[155] Graham Harman, 'Technology, Objects and Things in Heidegger', Cambridge Journal of Economics 34, no. 1 (2010): 19. The core of Heidegger's analysis is in Martin Heidegger, Being and Time, rev. edn. (Albany, NY: State University of New York Press, 2010/1927), 66-71.
[156] Peter-Paul Verbeek, What Things Do: Philosophical Reflections on Technology, Agency, and Design (University Park, PA: Pennsylvania State University Press, 2004), 79-80, quoted in Graham and Thrift, 'Out of Order', 3.

> transmission towers and electrical power plants. Without these extensions, Cyberspace [sic] would cease to exist.[157]

Whether by accident or by design, the failure of the electrical system reveals itself and also that it 'has no substitute, and all other infrastructures depend on it'.[158] 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'.[159] These revelatory events lay bare the material anatomy, psychological dependencies and functional relations of infrastructures that are embedded, transparent and ordinarily 'invisible'.[160] Referring once more to the fictional destruction of cities like Los Angeles, through 'such provocative transformations, we gain insight into the city we know'.[161]

They also reveal aspects of temporality that ordinarily remain hidden and—literally—unthought. Time is always being embedded in objects and artefacts, in which are enfolded 'heterogeneous temporalities'.[162] 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

---

[157] Brian Caroll, 'Seeing Cyberspace: The Electrical Infrastructure as Architecture', in The Cities of Everyday Life, eds. Ravi Vasudevan, Ravi Sundaram, Jeebesh Bagchi, Monica Narula, Geert Lovink and Shuddhabrata Sengupta (Delhi: Centre for the Study of Developing Societies, 2002), 250, originally quoted in Graham and Thrift, 'Out of Order', 13.
[158] Geers, 'Cyber Threat', 4.
[159] Leonard Kleinrock, 'An Internet Vision: The Invisible Global Infrastructure', Ad Hoc Networks 1, no. 1 (2003): 11.
[160] Susan Leigh Star, 'The Ethnography of Infrastructure', American Behavioral Scientist 43, no. 3 (1999): 377-391.
[161] James Sanders, Celluloid Skyline: New York and the Movies (New York: Alfred A. Knopf, 2001), 9.
[162] Bruno Latour, 'Morality and Technology: The End of the Means', Theory, Culture & Society 19, nos. 5-6 (2002): 248-249. This is also a central theme of Ian Hodder, Entangled: An Archaeology of the Relationships Between Humans and Things (Chichester: Wiley-Blackwell, 2012).

silently did and said'.[163] Failures 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.[164] 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, corporate pay, and so on.[165] 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', accidents often reveal the hidden politics that allow catastrophes to develop and, like Deepwater Horizon and Fukushima, literally explode into public consciousness.[166]

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 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: 'The world is to be understood in terms of what is to come rather than what has been …. the future is given greater eminence, and both past and present recede in importance.[167] Very often, the present is 'reduced to simply a gateway moment leading to the future'.[168] However, apocalypse is also a necessary event, without which a better future will not arrive; not only is

[163] Bruno Latour, 'Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts', in Shaping Technology / Building Society: Studies in Sociotechnical Change, eds. Wiebe E. Bijker and John Law (Cambridge, MA: MIT Press, 1992), 233.
[164] Although Y2K was not catastrophic, its problematisation revealed a 'hangover from previous decisions made in the growth of a system'; Hodder, Entangled, 100.
[165] Kaika and Swyngedouw, 'Fetishizing the Modern City', 136.
[166] John Keane, 'Silence and Catastrophe: New Reasons Why Politics Matters in the Early Years of the Twenty-First Century', The Political Quarterly 83, no. 4 (2012): 660-668.
[167] Bromley, 'Constructing Apocalypticism', 36.
[168] Ibid.

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.[169]

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 tendencies'.[170] 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 contingent upon bad things always being done by bad people. This Hobbesian inflection is explicit in the assertion that the biggest global cyber security challenge is preventing bellum omnium contra omnes in cyberspace.[171] To do further violence to Hobbes, these are visions of a 'perpetuall cyber warre' of all against all and where, wonders one author, is the Leviathan empowered by citizens to deliver us from this parlous state of nature?[172]

For some people, 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.[173] In recent history, we can detect this autopoietic apocalypticism in American reactions to 9/11 as clearly as in the jihadist beliefs of those who prosecuted the 9/11 attacks themselves.[174] 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

[169] Jeff Bliss, 'US Unprepared for "Cyber War", Former Top Spy Official Says', Bloomberg Businessweek, 23 February 2010; Jack Goldsmith and Melissa Hathaway, 'The Cybersecurity Changes We Need', Washington Post, 29 May 2010.
[170] Catherine Wessinger, 'Millennialism With and Without the Mayhem', in Robbins and Palmer, Millennium, 50.
[171] Rex Hughes, 'A Treaty for Cyberspace', International Affairs 86, no. 2 (2010): 525.
[172] Ryan T. Kaminski, 'Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions', in Conference on Cyber Conflict Proceedings 2010, eds. Christian Czosseck and Karlis Podins (Tallinn: CCD COE Publications, 2010), 79-94.
[173] David C. Rapoport, 'Messianic Sanctions for Terror', Comparative Politics 20, no. 2 (1988): 195-213.
[174] Lewis, Global Media Apocalypse, 12.

a global caliphate.[175] Aside from such 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'.[176] Although the Y2K 'technocalypse' did not happen in the manner prophesied, for instance, it catalysed political, technical and social changes to extant practices and beliefs, not least by implanting 'seeds of technological doubt' in mainstream culture.[177] Concerns that similar intercalary time and date problems may occur in 2038, 2042 and 2107 are mediated partially through 'lessons learnt' from the 'non-event' of Y2K.[178] Non-catastrophic events can have material and cognitive effects just as enduring as catastrophes.[179]

## 4.6 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'. 'Not all events are made equal', however, and some 'fail to exercise much of an impact at all or are barely noticed'.[180] 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, whilst of immediate concern to the information security professional, may not rise to the level of a collective security issue unless identified and

[175] John Gray, Black Mass: Apocalyptic Religion and the Death of Utopia (London: Allen Lane, 2007).
[176] Richard Landes, Whilst God Tarried: Disappointed Millennialism and the Genealogy of the Modern West (New York: Basic Books, 1998), 2, quoted in Andrea H. Tapia, 'Technomillennialism: A Subcultural Response to the Technological Threat of Y2K', Science, Technology, & Human Values 28, no. 4 (2003): 484.
[177] Tapia, 'Technomillennialism', 509. Also, Johan Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', Journal of Contingencies & Crisis Management 9, no. 4 (2001): 211-222.
[178] As are other processes that alter the chronos of Internet time. See, Poul-Henning Kamp, 'The One-Second War', Communications of the ACM 54, no. 5 (2011): 44-48. On the 'revelation' of Y2K, see Caroline M. Schwaller, 'Year 2000. A Date with Destiny. Apocalypse as "The End" or as "Revelation"?', Space & Culture 1, no. 2 (1997): 37-49.
[179] On the material persistence of catastrophes, see Stewart Williams, 'Rendering the Untimely Event of Disaster Ever Present', Landscape Review 14, no. 2 (2012): 86-96. Also, Kai Erikson, A New Species of Trouble: The Human Experience of Modern Disasters (New York: W.W. Norton & Company, 1994).
[180] Beissinger, Nationalist Mobilization, 15.

communicated as one. As extant studies have shown, cyber security has a diverse 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. 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'.[181]

Were such an event to occur we might characterise it as an accident sensu Virilio, or per James Der Derian's 'global event', 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'.[182] William Sewell suggests that some events have a 'transformative power' beyond the politics of government alone, shaping history and 'changing people's possibilities for meaningful action.[183] 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.[184] It is also an attempt to foster policies and practices that would enable a tolerable level of post-catastrophic survival and might be

[181] Lauren Martin and Stephanie Simon, 'A Formula for Disaster: The Department of Homeland Security's Virtual Ontology', Space & Polity 12, no. 3 (2008): 294. See also, Chapter 6.
[182] James Der Derian, 'Global Events, National Security, and Virtual Theory', Millennium: Journal of International Studies 30, no. 3 (2001): 674.
[183] William H. Sewell, Jr., 'Collective Violence and Collective Loyalties in France: Why the French Revolution Made a Difference', Politics & Society 18, no. 4 (1990): 548, cited in Beissinger, Nationalist Mobilization, 15.
[184] See, Philippe Bourbeau, 'Resiliencism: Premises and Promises in Securitisation Research', Resilience: International Policies, Practices and Discourses 1, no. 1 (2013): 3-17.

considered in a more positive, and possibly emancipatory, light.[185] 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'.[186]

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.[187] 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'.[188] 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'.[189] Or, indeed, if this symbolic order is contemporary politics, blamed by prophets of cyber apocalypse for inaction and inadequacy in the face of existential threat.[190] This desire for political transformation is surely at the heart of the apocalyptic narrative through which cyber security futures are so often imagined.

---

[185] David Chandler, 'Resilience and Human Security: The Post-Interventionist Paradigm', Security Dialogue 43, no. 3 (2012): 213-229.

[186] Joost van Loon, 'Imminent Immanence: The Time-Politics of Speed and the Management of Decline', Time & Society 9, nos. 2-3 (2000): 347-348.

[187] See, for example, the diversity of apocalyptic movements in Norman Cohn, The Pursuit of the Millennium: Revolutionary Millenarians and Mystical Anarchists of the Middle Ages (London: Pimlico, 2004/1957).

[188] Jean-François Lyotard, 'The Sign of History', in Post-Structuralism and the Question of History, eds. Derek Attridge, Geoff Bennington and Robert Young (Cambridge: Cambridge University Press, 1987), 179, quoted in Richard Dellamora, 'Introduction', in Postmodern Apocalypse: Theory and Cultural Practice at the End, ed. Richard Dellamora (Philadelphia, PA: University of Pennsylvania Press, 1995), 2.

[189] Scherpe, 'Dramatization', 98-99.

[190] People tell such stories 'not only to shift the blame but to enable themselves to appear to be able to remedy the problem'; Deborah A. Stone, 'Causal Stories and the Formation of Policy Agendas', Political Science Quarterly 104, no. 2 (1989): 297.

The poet Octavio Paz identifies accidents in the Virilian sense as 'cogs of the historic order'.[191] 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. Although we have identified historical events as 'signs' leading to the cyber apocalypse, by their nature none attain the practical or symbolic level of catastrophe. However, cyber security discourses do make explicit 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.

[191] Octavio Paz, 'Order and Accident', Conjunctions and Disjunctions (New York: Viking Press, 1974/1969), 112. Also, Der Derian, 'Global Events'.

# 5 ARGUING THROUGH THE PAST

If I am anxious about a past misfortune,
then this is not because it is in the past
but because it may be repeated.[1]

## 5.1 Introduction: Past, Present and the Appeal to History

In Chapter Two, we encountered numerous difficulties in ascribing definitive (meta)physical ontological status to past, present and future and 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.[2] Our common experience is that this is always so and our common sense—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, and a 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

[1] Søren Kierkegaard, The Concept of Anxiety, eds. Reidar Thomte and Albert B. Anderson (Princeton, NJ: Princeton University Press, 1980/1844), 91.
[2] Unlike physical equations, in which the 'future and the past seem physically to be on a completely equal footing'; Roger Penrose, The Emperor's New Mind: Concerning Computers, Minds and the Laws of Physics (Oxford: Oxford University Press, 1989), 392.

the present and the past.[3] 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'.[4] The imagined past is 'a static world beyond commodified clock time, outside of history, progress and change'.[5] These narratives ignore that the past is continually remade in the present as part of the normal operations of 'history, progress and change'.[6] For most purposes, it matters little if there is or there is not a physical 'world' called 'the past' with which 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 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.[7] 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.[8] 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'.[9] In the 19th century, antiquarians

[3] Barry Hindess, 'The Past is Another Culture', International Political Sociology 1, no. 4 (2007): 330.
[4] Peter F. Cannavò, 'Ecological Citizenship, Time, and Corruption: Aldo Leopold's Green Republicanism', Environmental Politics 21, no. 6 (2012): 866.
[5] Glenn Jordan, 'Flight from Modernity: Time, the Other and the Discourse of Primitivism', Time & Society 4, no. 3 (1995): 283.
[6] Ibid.
[7] Stephen Toulmin and June Goodfield, The Discovery of Time (London: Hutchinson & Co., 1965), 141-170; Stephen Jay Gould, Time's Arrow, Time's Cycle: Myth and Metaphor in the Discovery of Geological Time (Cambridge, MA: Harvard University Press, 1987).
[8] Formal geology began in Enlightenment Europe but various Chinese from the third century AD onwards were geologists of a sort, although their theories did not have the same domestic impact as those of later Europeans; Joseph Needham, Science and Civilization in China, vol. III: Mathematics and the Sciences of the Heavens and Earth (Cambridge: Cambridge University Press, 1959), chapter 23, esp. pp. 612-614.
[9] J.M.I. Klaver, Geology and Religious Sentiment: The Effect of Geological Discoveries on English Society and Literature Between 1829 and 1859 (Leiden: Brill, 1997), xi.

applied geological techniques to the history of humankind itself, adding through the new field of archaeology 'the testimony of things' to the textual evidence, and which 'very soon exploded any simple, uni-directional theory of historical development'.[10] Although narrow interpretations of ancient remains in Egypt and the Near East in particular would often seem to corroborate Biblical narratives, eventually the weight of 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 'only one, rather minor strand' of human history.[11]

For archaeologists, neither things nor the pasts from which they originally derive are fixed or stable. Although many archaeological artefacts are surprisingly durable, and must be so for them to re-emerge 'artefactually' in the present, their meanings may change through later reuse and reinterpretation and are never fixed. 'Things', writes Ian Hodder, are assembled: for 'a period of time matter, energy and information are brought together into a heterogeneous bundle' we call a thing, entangled in a web of connections with other things and the particular species of thing we call 'human'.[12] This dynamic approach to thingness is consistent with an interpretation of the archaeological record as not cleanly demarcated from the archaeologist. There is an interpretive problem with the 'resurrection and irruption into the present of material remains from the past' but this is a problem only made worse by insisting on an artificial boundary between past and present.[13] The past is a 'palimpsest of multiple events and time-scales', a multi-temporality that includes the past and the present.[14] We might even argue that all archaeology, even if it is about the past, is actually of the present.[15] The present 'opens onto all the pasts that have preceded present time and that are recorded in it'.[16]

[10] Toulmin and Goodfield, Discovery of Time, 237.
[11] Ibid., 238.
[12] Ian Hodder, Entangled: An Archaeology of the Relationship Between Humans and Things (Chichester: Wiley-Blackwell, 2012), 8.
[13] Gavin Lucas, The Archaeology of Time (London: Routledge, 2005), 36-37.
[14] Ibid., 38.
[15] Ibid., 121.
[16] Laurent Olivier, The Dark Abyss of Time: Archaeology and Memory (Lanham, MD: AltaMira Press, 2011), 53.

Integral to this perspective on the past is that the past is interpreted in the present. Although we might begin to understand the original functionality or meaning of an artefact discarded millennia ago, we can never escape our own interpretive subjectivity in the present. As Laurent Olivier notes, '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'.[17] 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.[18] This approach remains common in many countries, in which there is a long-observed tendency 'to glorify the "primitive vigour" and creativity of people assumed to be national ancestors rather than to draw attention to their low cultural status'.[19] In late 20th-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'.[20] 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.[21] Given its potential for political manipulation, archaeology is 'a discipline almost in wait of state interference'.[22]

---

[17] Ibid., 60.
[18] Bruce G. Trigger, A History of Archaeological Thought (Cambridge: Cambridge University Press, 1989), 163-167.
[19] Ibid., 174.
[20] Margarita Díaz-Andreu, 'Constructing Identities Through Culture: The Past in the Forging of Europe', in Cultural Identity and Archaeology: The Construction of European Communities, eds. Paul Graves-Brown, Siân Jones and Clive Gamble (London: Routledge, 1996), 56-57.
[21] BBC News, 'King Richard III Burial Row Heads to High Court', 1 May 2013.
[22] Philip L. Kohl and Clare Fawcett, 'Archaeology in the Service of the State: Theoretical Considerations', in Nationalism, Politics, and the Practice of Archaeology, eds. Philip L. Kohl and Clare Fawcett (Cambridge: Cambridge University Press, 1995), 8.

So too 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 (1949). 'Is there somewhere or other a place, a world of solid objects, where the past is still happening?'[23] 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 an 'error', a hidden belief in the existence of a reality outside of the Party, a reality that might afford the possibilities of individual human remembering. However, Reality only exists in 'the mind of the Party, which is collective and immortal. Whatever the Party holds to be truth, is truth'.[24] 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 imagined history. The uses of history and appeals to the past are at the core of the construction of statehood and nationhood.[25] 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'.[26] This chapter intends to excavate some of these 'chains' linking the past to the cyber security present in the service of

[23] George Orwell, Nineteen Eighty-Four (London: Heinemann, 1965/1949), 192.
[24] Ibid., original emphasis.
[25] Benedict Anderson, Imagined Communities: Reflections on the Origin and Spread of Nationalism, rev. edn. (London: Verso, 2006/1983).
[26] Carmen Leccardi, 'New Temporal Perspectives in the "High-Speed Society"', in 24/7: Time and Temporality in the Network Society, eds. Robert Hassan and Robert E. Purser (Stanford, CA: Stanford Business Books, 2007), 33.

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 Three proposed that cyber security is sufficiently preoccupied with the uniqueness of the present that it tends to ignores both its own history and the historicity of the present. In Chapter Four, 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. These data are culled from industry, media and government reports and used to illustrate particular arguments in the main text and represent highly formalised and decontextualized 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 in discussions of contemporary ICTs. They are not intended to 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? As the foregoing examples illustrate, 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 language examined previously, it is not only events of the recent past 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. Although the apocalyptic reading of Megiddo as the future site of Armageddon is fanciful and not supported clearly by scripture or doctrine, 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 such 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 suggest there are normative constraints on Western

public officials uttering clearly Biblical-sounding apocalyptic discourses 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.[27] 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.[28] 'It is later than we think', he remarked, in direct reference to the temporal proximity of the end-times,[29] although he would later claim not to have allowed his eschatological beliefs to influence policy decisions, let alone influence plans for nuclear war.[30] 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 on-going prosecution, despite its many allusions to 'holy war' and the divinity of its mandate.[31]

Politicians might wish to avoid the slightly hysterical language of Armageddon and religious apocalypse but no such caution exists in their invocation of historical events and processes in political cyber security discourses. Analogies, especially of war, are a commonplace of political

---

[27] Daniel Wojcik, The End of the World as We Know It: Faith, Fatalism, and Apocalypse in America (New York: New York University Press, 1997), 29-30.

[28] Martin L. Cook, 'Christian Apocalypticism and Weapons of Mass Destruction', Ethics and Weapons of Mass Destruction: Religious and Secular Perspectives, eds. Sohail H. Hashmi and Steven P. Lee (Cambridge: Cambridge University Press, 2004), 200-210.

[29] Ralph Clark Chandler, 'Little Boy, Fat Man, and the Rapture: The Effects of Late Twentieth Century Apostasy on Public Policy', Dialogue 8, no. 1 (1985): 1.

[30] Paul S. Boyer, When Time Shall Be No More: Prophecy Belief in Modern American Culture (Cambridge, MA: Harvard University Press, 1992), 42

[31] Richard Jackson, Writing the War on Terrorism: Language, Politics and Counter-Terrorism (Manchester: Manchester University Press, 2005), 103-105; Peter McLaren, 'George Bush, Apocalypse Sometime Soon, and the American Imperium', Cultural Studies—Critical Methodologies 2, no. 3 (2002): 327-333.

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.[32] 'We are currently at war', reported the BBC in 2012, 'on a battlefield we can't see, with weapons most of us know nothing about'.[33] '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'.[34] 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'.[35] 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'.[36] This is the 'hidden battle', 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'.[37] Stretching historical tolerance still 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'.[38]

These examples are but a small selection of the volume and variety of historical analogies deployed by cyber security actors. The security orientation of these discourses 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. These events are deployed as 'historical analogies', a term which 'signifies an inference that if two or more events

[32] Rex Hughes, 'A Treaty for Cyberspace', International Affairs 86, no. 2 (2010): 523-541.
[33] BBC, 'The One Show', 13 December 2012.
[34] Sky News, bulletin, 8 January 2013.
[35] Ibid.
[36] Mike McConnell, 'To Win the Cyber-War, Look to the Cold War', The Washington Post, 28 February 2010.
[37] CSIS, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (Washington, DC: Center for Strategic and International Studies, 2008), 11.
[38] Wayne Michael Hall, Stray Voltage: War in the Information Age (Annapolis, MD: Naval Institute Press, 2003), x-xi.

separated in time agree in one respect, then they may also agree in another'.[39] 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?[40] 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.[41]

The focus of this chapter is not on the failures of historical analogies but on the political work they perform, which 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'.[42] 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. Although we might not be able to quantify the political efficacy of these analogies, we can begin to see how they might be effective or otherwise, 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?

[39] Yuen Foong Khong, Analogies at War: Korea, Munich, Dien Bhen Phu, and the Vietnam Decisions of 1965 (Princeton, NJ: Princeton University Press, 1992), 6-7.
[40] 'We draw analogies for a reason: to assign value'; Christopher Coker, Warrior Geeks: How 21st Century Technology is Changing the Way We Fight and Think About War (London: Hurst & Company, 2013), 184.
[41] Jenny Kitzinger, 'Media Templates: Patterns of Association and the (Re)construction of Meaning Over Time', Media, Culture & Society 22, no. 1 (2000): 75. [61-84]
[42] Khong, Analogies, 12; Richard E. Neustadt and Ernest R. May, Thinking in Time: The Uses of History for Decision Makers (New York: The Free Press, 1986).

## 5.2 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 20th 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. As Emily Rosenberg notes in her exemplary study of the construction of Pearl Harbor in American memory, 'the near-sacred symbol of Pearl Harbor … "lives" in a thousand guises and symbolizes dozens of often conflicting historical "lessons"'.[43] 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'.[44] 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'.[45]

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'.[46] President, politicians, press and pundits alike 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

[43] Emily S. Rosenberg, A Date Which Will Live: Pearl Harbor in American Memory (Durham, NC: Duke University Press, 2003), 5-6.
[44] Ibid., 6.
[45] Ibid., 7.
[46] Bob Woodward, Bush at War (New York: Simon & Schuster, 2002), 37, cited in Jackson, Writing the War, 27.

perfidious and inhuman foe.[47] 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'.[48]

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.[49] 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 and which have yet to happen, if they ever will.

The earliest reference to an 'electronic Pearl Harbour' appears to be by information security specialist Winn Schwartau, 'the rock manager-turned-preacher of "information warfare"'.[50] In an op-ed for Computerworld magazine in January 1991, Schwartau suggested that for 'a motivated individual or organization, an assault on our information processing capabilities

[47] But, in stark contrast to Pearl Harbor, a deracialised enemy; Deborah J. Schildkraut, 'The More Things Change … American Identity and Mass and Elite Responses to 9/11', Political Psychology 23, no. 3 (2002): 511-535.

[48] Marcia Landy, '"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, 2004), 86.

[49] Maura Conway, '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, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge, 2008), 117; Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008), 130.

[50] Ralf Bendrath, Johan Eriksson and Giampiero Giacomello, 'From "Cyberterrorism" to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace', in International Relations and Security in the Digital Age, eds. Johan Eriksson and Giampiero Giacomello (London: Routledge, 2007), 57.

would be an effective attack on a global Achilles Heel, an electronic Pearl Harbor'.[51] Schwartau continued to popularise the term throughout 1991, including in testimony to a US Congressional Subcommittee on 27 June, whom 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'.[52]

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'.[53] However, Schwartau's long-standing claim to have coined the phrase is bolstered by the publication, in the same month as his Congressional testimony, of his first novel, Terminal Compromise (1991).[54] 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 (2002).[55] The 'electronic Pearl Harbor' is an event described by Schwartau in existential terms:

> the target is one of the most crucial segments of our way of life: Information …. the key building block upon which modern society functions …. the lifeblood of the United States and the world …. a global and a national strategic asset that is currently under attack …. Without information, without the machinery that allows the information to

[51] Winn Schwartau, 'Fighting Terminal Terrorism', Computerworld, 28 January 1991, 23.
[52] Winn Schwartau, Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age (New York: Thunder's Mouth Press, 1994), 43.
[53] Scott Berinato, 'The Future of Security', CIO 17, no. 6 (2003): 72..
[54] Winn Schwartau, Terminal Compromise—Computer Terrorism: When Privacy and Freedom are the Victims (Seminole, FL: Interpact Press, 1991).
[55] Winn Schwartau, Pearl Harbor Dot Com (Seminole, FL: Interpact Press, 2002).

> remain available, a veritable national electronic library, the United States steps back thirty years.[56]

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'.[57]

Since its inception, the term has been used with 'startling frequency' to conjure up 'images of a sudden crippling blow against critical infrastructures resulting in chaos and destruction'.[58] By 1997, it was considered the 'most common analogy' in US military planning discourse, in which it represented a future event which would 'wipe out communications and leave the front-line soldiers, unable to act on their own initiative, helpless'.[59] By 2003, the term was described as 'bromidic', so frequently was it used and so attenuated had its meaning become.[60] Former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism Richard Clarke changed the target set compromised by such attacks to include private companies as well as government and military assets.[61] 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

---

[56] Winn Schwartau, Terminal Compromise—Computer Terrorism: When Privacy and Freedom are the Victims (Seminole, FL: Interpact Press, online version, August 1993), n.p.
[57] Schwartau, Pearl Harbor Dot Com, 442.
[58] Conway, 'Media, Fear and the Hyperreal', 117.
[59] Chris Partridge, 'How to Conquer the World … And Never Leave the Barracks', The Times, 27 August 1997.
[60] Berinato, 'Future of Security', 73.
[61] Dibya Sarkar, 'Cybersecurity Guide Delayed', Federal Computer Week, 11 June 2002; also, Richard A. Clarke, 'Threats to US National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks', DePaul Business Law Journal 12, nos. 1-2 (1999): 33-43.

further by reference to the possibility of multiple 'small-scale' digital Pearl Harbours.[62] Clarke, for example, asserted that 'digital Pearl Harbors are happening every day'.[63] By 2011, the phrase had become 'rather stale from overuse'.[64]

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:

> 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.[65]

The speech was reported 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.[66] 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) and during his confirmation hearing as defense secretary in June 2011.[67] His use of the phrase only attracted

---

[62] Kenneth Geers, 'The Cyber Threat to National Critical Infrastructures: Beyond Theory', Information Security Journal: A Global Perspective 18, no. 1 (2009): 4. See also references to past 'espionage Pearl Harbours'; National Public Radio, 'Assessing the Threat of Cyberterrorism: Interview with James Lewis', Fresh Air, 10 February 2010.

[63] Berinato, 'Future of Security', 73. As Berinato correctly observes: if 'digital Pearl Harbors were happening every day, they wouldn't be Pearl Harbors'.

[64] Frank R. Spellman and Melissa L. Stoudt, Nuclear Infrastructure Protection and Homeland Security (Lanham, MD: Government Institutes, 2011), 124.

[65] Leon Panetta, 'Remarks by Secretary Panetta on Cybersecurity', speech to Business Executives for National Security, New York, 11 October 2012.

[66] Elisabeth Bumiller and Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack', The New York Times, 12 October 2012.

[67] Respectively, Lisa Daniel, 'Panetta: Intelligence Community Needs to Predict Uprisings', American Forces Press Service, 11 February 2011; Anna Mulrine, 'CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack', The Christian Science Monitor, 9 June 2011.

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.[68] 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 in detail.[69] 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'.[70]

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 fearmongering and part of a concerted campaign of American 'scare tactics' intended to give 'Washington bureaucrats greater control over what happens online in the US'.[71] 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-

[68] Leon Panetta, 'Remarks by Secretary Panetta', speech at Georgetown University, Washington, DC, 6 February 2013.
[69] Howard A. Schmidt, Patrolling Cyberspace: Lessons Learned from a Lifetime in Data Security (Potomac, MD: Larstan Publishing, Inc., 2006), 160.
[70] Mark Clayton, '"Cyber Pearl Harbor": Could Future Cyberattack Really Be That Devastating?', The Christian Science Monitor, 7 December 2012. Also, James A. Lewis, 'Cyber Terror: Missing in Action', Knowledge, Technology, & Policy 16, no. 2 (2003): 34-41; James A. Lewis, 'Aux Armes, Citoyens: Cyber Security and Regulation in the United States', Telecommunications Policy 29, no. 11 (2005): 821-830.
[71] RT, 'Panetta Back at It with "Cyber Pearl Harbor" Fear Mongering', 7 February 2013.

attacks from "aggressors"'.[72] Greenwald was correct to note that the defense secretary failed to report that the US 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, mentions of foreign aggression ring rather hollow, an omission noted by other commentators, including The Financial Times.[73]

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.[74] 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 US to discard 'digital Pearl Harbor' as the central metaphor of strategic thought, offering an alternative metaphor, 'a "Manifest Destiny" for the information age'.[75] This idea was neither elaborated nor its ramifications examined further and it is hard to see how this metaphor is any less problematic than that of Pearl Harbor, given its negative connotations of divinely sanctioned American imperialism and territorial expansion.[76] This is especially pertinent because accusations have long been levelled against the United States that it is attempting in some fashion to 'colonise cyberspace' through normative, commercial, military and other means.[77]

---

[72] Glenn Greenwald, 'Pentagon's New Massive Expansion of "Cyber-Security" Unit is About Everything Except Defense', The Guardian, 28 January 2013. This echoes an earlier statement that the analogy works 'to manufacture fear in the simplest and most direct way possible'; Conway, 'Media, Fear', 117.
[73] Geoff Dyer, 'Panetta Warns US of "Cyber Pearl Harbor"', FT.com, 12 October 2012.
[74] John Arquilla, 'Panetta's Wrong About a Cyber "Pearl Harbor"', Foreign Policy, 19 November 2012. Rid also notes that there have been no events bearing 'any resemblance to World War II in the Pacific'; Thomas Rid, 'Cyber Fail', New Republic, 4 February 2013.
[75] John Arquilla and David Ronfeldt, The Emergence of Noopolitik: Toward an American Information Strategy (Santa Monica, CA: RAND Corporation, 1999), 75.
[76] 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'; Carl Schurz, 'Manifest Destiny', Speeches, Correspondence and Political Papers, vol. 5, ed. Frederic Bancroft (New York: The Knickerbocker Press, 1913), 191.
[77] Diana Saco, 'Colonizing Cyberspace: "National Security" and the Internet', in Cultures of Insecurity: States, Communities, and the Production of Danger, eds. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall (Minneapolis, MN: University of Minnesota Press, 1999), 261-291.

However, it illustrates further that analogies are always sought 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'.[78] 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 suggests a degree of deliberateness in their choice of analogy and the likelihood that those who use it are aware of its rhetorical force and the cognitive work that 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.[79] 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 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

[78] Arquilla, 'Panetta's Wrong'.
[79] Berinato, 'Future of Security'.

public outrage led to litigation, regulation and the imposition of security standards on the public and private sectors:

> this notion of an industrywide smartening up [is] based on the assumption that there will be a security incident of such mind-boggling scope and profoundly disturbing consequence …. that conducting business will become inconceivable.[80]

Given the previous discussion of catastrophe in Chapter Four, we can again see the apocalyptic consciousness at work. The digital Pearl Harbour is an event—or a series of tightly bound events constituting an 'accident'—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, desired and desirable.[81]

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.[82]

---

[80] Ibid., 72.

[81] Berinato outlines a 'lockdown' alternative to the 'reform' scenario, in which, post-digital Pearl Harbor, security trumps all other considerations—'Big Brother will arrive fashionably late, but arrive he will'; ibid., 74. Also, Raiford Guins, Edited Clean Version: Technology and the Culture of Control (Minneapolis, MN: University of Minnesota Press, 2009).

[82] Jason Healey, 'Hazard, Outrage and Panetta's Cyber Speech', New Atlanticist, 23 October 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'. 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.[83] 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:

> what 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 galvanise 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.[84]

Physical scenarios are required in order to materialise and make comprehensible the 'virtual' threat and the Pearl Harbor analogy helps to do this by making the 'abstract and distant' 'personal and immediate'.[85] This has the effect of 'waking' America from its cyber security slumber, the 'sleeping metaphor' that has become an integral part of the Pearl Harbor myth, in which innocence and complacency are both embedded—with respect to cyber security, 'it

[83] A point also made by Thomas Rid, Cyber War Will Not Take Place (London: Hurst & Company, 2013), 174.

[84] Arthur K. Cebrowski, 'Forum', Issues in Science & Technology 15, no. 2 (1998). Scholars have also emphasised that a Pearl Harbor-type event is needed to get 'the private sector to develop a keen interest in a more prominent role of the government in IT security'; Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', Information & Security 7: n.p.

[85] This is all the more striking because 'cyber attacks are not creating more vectors of violent interaction; rather they are making previously violent interactions less violent'; Rid, Cyber War, viii; also, Thomas Rid, 'More Attacks, Less Violence', Journal of Strategic Studies 36, no. 1 (2013): 139-142.

seems the "sleeping giant" is again awaiting a public, catastrophic event before awakening'.[86] As Rosenberg notes, when the nation 'suddenly loses its childlike innocence' maturity and manhood, often in the form of military force, follows.[87] Moreover, Pearl Harbor serves to warn of the dangers of not being alert to new Pearl Harbor-type events. 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'.[88] This is precisely the argument of many commentators who argue for the military to take the lead in national cyber defence.

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'.[89] Although we cannot trace definitively causality between use of the analogy and the undoubted increase in US cyber security spending, institutional reorganisation and drives towards 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 this additional perspective.

[86] Clifford S. Magee, 'Awaiting Cyber 9/11', Joint Force Quarterly 70 (2013): 78. See the list of 'wake-up calls' in Jason Healey, ed., A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Washington, DC: Atlantic Council, 2013).
[87] Rosenberg, A Date Which Will Live, 18.
[88] Ibid., 27.
[89] Rosenberg, A Date Which Will Live, 31.

## 5.3 Memory and Identity

Pearl Harbor has been invoked in cyber security for two decades, 'with each cyber incident that reaches the media articulated as proof of its encroaching inevitability'.[90] 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'.[91] For academics too, Pearl Harbor is always imminent and inevitable.[92] However, the final cataclysm that must wake government from its complacency is forever deferred, creating a temporal hiatus filled with fearful anticipation and longing.[93]

Some policymakers do reject the inevitability or necessity of a digital Pearl Harbor and make a distinction between the inevitability of a future attack—'not a matter of if, but when'—and the preventability of a Pearl Harbor-type event. Although attacks will happen, 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, although it is the future that shapes to a great extent the contemporary politics of cyber security. The narrative of imminent and immanent catastrophe is challenged from within political elites themselves and restores a sense of agency to the political present, although the omnipresent threat of future disaster is only deferred rather than cancelled altogether.

---

[90] David Barnard-Wills and Debi Ashenden, 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', Space & Culture 15, no. 2 (2012): 118.

[91] Joseph I. Lieberman and Susan Collins, 'At Dawn We Sleep', The New York Times, 7 December 2012. Also, Peter Hoekstra and Brian Finch, 'The Looming Certainty of a Cyber Pearl Harbor', Politico, 19 February 2013.

[92] Emily Molfino, 'Viewpoint: Cyberterrorism: Cyber "Pearl Harbor" is Imminent', in Cyberspaces and Global Affairs, eds. Sean S. Costigan and Jake Perry (Farnham: Ashgate Publishing, 2012), 75-82.

[93] Former UK Home Secretary John Reid told the BBC that 'the enemy' of cyber security is 'our own complacency'; BBC, 'Newsnight', 29 April 2013.

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. Or, 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 to 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, and what influence does this have on the politics of cyber security? Revisiting Roosevelt's speech in 1942, Rosenberg describes how it tapped into existing structures of national memory and identity:

> In emphasising the 'character' of the attack by Japan and promising that such 'infamy' needed to be followed through to 'inevitable triumph', Roosevelt structured his narrative to recall America's most celebrated frontier legends: Custer's Last Stand and the Alamo. These, too, were terrible defeats that provided rallying cries for overwhelming military counterforce leading to total victory. Memory research confirms that people remember events in ways that fit already familiar patterns and narrative structures. The infamy framework for Pearl Harbor was perhaps so powerful because it already circulated widely in frontier lore.[94]

We might make a similar argument for cyber security, in which the frontier myth is made definitive and foundational of future 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

[94] Rosenberg, A Date Which Will Live, 12.

of anarchy is not absolute'.[95] Because its interests depend upon cyberspace, the US 'cannot allow a regression toward a Wild West of continuous malicious activity'.[96] It calls for 'a cleaner, healthier cyber environment in order to secure a broad range of United States and international interests'.[97] Although the report bases its policy proposals on models of public health, it might easily have built upon 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 foundation of their argument. It does not do so because it is not attempting to dredge up suppressed national memories of aboriginal genocide (bad) but because it is trying to remember the role of pioneer Americans in making the frontiers safe and prosperous (good). In an environment of no borders (the Internet), it is the role of America to ensure no space is left ungoverned, least these interstices harbour enemies that may strike at American interests home or abroad.[98]

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', 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'.[99] 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

---

[95] Greg Rattray, Chris Evans and Jason Healey, 'American Security in the Cyber Commons', in Contested Commons: The Future of American Power in a Multipolar World, eds. Abraham M. Denmark and James Mulvenon (Washington, DC: Center for a New American Security, 2010), 149, 150.

[96] Ibid., 171. On the 'Wild West' metaphor and 'cyberspace', see Paul A. Taylor, Hackers: Crime in the Digital Sublime (London: Routledge, 1999), 157-159.

[97] Ibid., 140. Metaphors of immunisation and sterilisation of computer systems are older than one might expect; for example, Charles Cresson Wood, 'The Human Immune System as an Information Systems Security Reference Model', Computers & Security 6, no. 6 (1987): 511-516.

[98] This is an expression of broader counter-sanctuary discourses, as examined in Michael Innes, ed., Denial of Sanctuary: Understanding Terrorist Safe Havens (Westport, CT: Praeger Security International, 2007).

[99] Helen McLure, 'The Wild, Wild Web: The Mythic American West and the Electronic Frontier', The Western Historical Quarterly 31, no. 4 (2000): 457.

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 notes in a posthumously published essay, 'only Americans live in Marlboro country'.[100] American cultural exports have moved on from movie Westerns and the image of the rugged cowboy is no longer quite the international pin-up it once was. 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 post-9/11.[101] 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"'.[102] 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'.[103] 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.[104] 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.

---

[100] Eric Hobsbawm, 'The American Cowboy: An International Myth?', Fractured Times: Culture and Society in the 20th Century (London: Little, Brown, 2013), 287.
[101] Mark West and Chris Carey, '(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 (2006): 379-412; Ryan Malphurs, 'The Media's Frontier Construction of President George W. Bush', The Journal of American Culture 31, no. 2 (2008): 185-201.
[102] Malphurs, 'Media's Frontier Construction', 195.
[103] James Naughtie, The Accidental American: Tony Blair and the Presidency, rev. edn. (London: Macmillan, 2005), 119.
[104] See, Ed Johnson, '"Cowboy" Blair Raises Eyebrows', Associated Press, 4 September 2002. Blair was later cast as Roy Rogers in Richard Hamilton's well-known satirical portrait, 'Shock and Awe, 2007-2008', http://uploads5.wikipaintings.org/images/richard-hamilton/shock-and-awe-2008.jpg.

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 the analogy has 'immediate resonance and attracts wide understanding',[105] this is probably the case across multiple audiences but it is only in the US that it will elicit what John Arquilla calls its 'surefire emotional effect'.[106] It is hard to imagine it having the same 'resonance' elsewhere. Even amongst the US' Western allies, Pearl Harbor is remembered more as the event that brought the US into 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.[107] As with the original attacks on Pearl Harbor, which showed that the US was not geographically separate from the rest of the world, future Pearl Harbors warn against considering the US invulnerable from foes located 'geographically and morally' outside the US.[108] 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'.[109] 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

[105] Conway, 'Media, Fear and the Hyperreal', 117.
[106] Arquilla, 'Panetta's Wrong'.
[107] Bendrath, 'Cyberwar Debate', n.p; Bendrath et al, 'From "Cyberterrorism" to "Cyberwar"', 58.
[108] Dunn Cavelty, Cyber-Security, 130; Conway, 'Media, Fear and the Hyperreal', 117.
[109] Bendrath, 'Cyberwar Debate', n.p.

'deep, horizontal comradeship'.[110] It assists in constructing such an event as an issue of national, rather than merely 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.[111]

The US is framed as vulnerable but it is also presented as uniquely vulnerable to catastrophic cyber attacks. This is expressed 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.[112] Second, the US is more vulnerable now than it has ever been, with its 'digital underbelly' exposed for all 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'.[113] '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'.[114] The United States is therefore supremely vulnerable in space, where it is an isolated global hegemon, and in time: at no point in its history has it been so open to catastrophic attacks of this nature.

---

[110] Anderson, Imagined Communities, 7.
[111] Lauren Berlant, The Anatomy of National Fantasy: Hawthorne, Utopia, and Everyday Life (Chicago, IL: University of Chicago Press, 1991), 20.
[112] James Adams, 'Virtual Defense', Foreign Affairs 80, no. 3 (2001): 98.
[113] Clarke, 'Threats', 43, 38.
[114] Michael Vatis, 'Cyber Attacks: Protecting America's Security Against Digital Threats', ESDP Discussion Paper ESDP-2002-04 (Cambridge, MA: John F. Kennedy School of Government, Harvard University, 2002), 2.

Pearl Harbor was a moment of extreme vulnerability, as was 9/11, narratives of which frequently invoked 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.[115] 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.[116] 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'.[117]

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.[118] 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, whilst embracing it as a 'forcing issue' to improve cyber security across public and private sectors.[119] 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

[115] Dunn Cavelty, Cyber-Security, 117-121; also, Myriam Dunn Cavelty, 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Journal of Information Technology & Politics 4, no. 1 (2007): 19-36.
[116] Conway, 'Media, Fear and the Hyperreal', 122.
[117] Ibid. Also, Maura Conway, 'Against Cyberterrorism', Communications of the ACM 54, no. 2 (2011): 26-28.
[118] In cyber security discourses, the 'digital', 'electronic' and 'cyber' prefixes are used so promiscuously and with such little rigour that 'they can basically mean everything and nothing', Dunn Cavelty, Cyber-Security, 14.
[119] Sue Cant, '"Cyber 9/11 Risk Warning', Sydney Morning Herald, 22 April 2003.

for any large-scale cyber attack on the US, regardless of perpetrator or intent.[120] 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.[121] 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'.[122]

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, as suggested, 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 most deadly and costliest weather events ever to hit the United States, the official meteorological report

[120] Paul Taylor, 'Former US Spy Chief Warns on Cybersecurity', Financial Times, 2 December 2012.
[121] Ibid.
[122] Janet Napolitano, 'From Cyber to Immigration, Terrorism to Disasters: Securing America in the Next Administration', Wilson Center, Washington, DC, 24 January 2013.

recording simply that the extent, magnitude and effects of the hurricane were 'staggering'.[123] 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.[124] It was perhaps inevitable that Katrina would enter cyber security discourse in the form of 'cyber Katrina' to connote a forthcoming catastrophe.[125]

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.[126] 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.[127] As Sean Lawson has pointed out, 'No natural disaster in the last several years has passed without a government official or civilian "expert" using it to raise fears of cyber threats'.[128] 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.[129] Once again, the cyber disaster is

---

[123] Richard D. Knabb, Jamie R. Rhome and Daniel P. Brown, 'Tropical Cyclone Report: Hurricane Katrina', National Hurricane Center, 20 December 2005, updated 14 September 2011.

[124] The key term here is 'images', as mediated narratives of 'civil unrest' were not entirely congruent with the empirical record; Kathleen Tierney, Christine Bevc and Erica Kuligowski, 'Metaphors Matter: Disaster Myths, Media Frames, and Their Consequences in Hurricane Katrina', The ANNALS of the American Academy of Political & Social Science 604, no. 1 (2006): 57-81.

[125] Keith Epstein, 'Fearing "Cyber Katrina", Obama Candidate for Cyber Czar Urges a "FEMA for the Internet"', Bloomberg Businessweek, 18 February 2009.

[126] Rahul Bhaskar, 'State and Local Law Enforcement is Not Ready for a Cyber Katrina', Communications of the ACM 49, no. 2 (2006): 81-83; Arjen Boin and Allan McConnell, 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience', Journal of Contingencies & Crisis Management 15, no. 1 (2007): 50-59.

[127] Sean Lawson, 'DHS Secretary Napolitano Uses Hurricane Sandy to Hype Cyber Threat', Forbes, 1 November 2012.

[128] Ibid.

[129] Ami J. Abou-Bakr, Managing Disasters through Public-Private Partnerships (Washington, DC: Georgetown University Press, 2013); Thomas A. Birkland, Lessons of Disaster: Policy Change After Catastrophic Events (Washington, DC: Georgetown University Press, 2006).

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.[130] 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 US in cyber security discourses, on account, principally, of its historical pre-eminence in the field of critical infrastructures and their security and protection.[131] 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. Indeed, they may be selected for these, 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 appropriate comparison, although it is rarely, if ever, used today.[132] The Battle of Waterloo (1815) was the decisive encounter of the Anglo-Allied campaign to unseat Napoleon from the French imperial throne, from which the CSIS authors drew inspiration in sketching 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

[130] For example, Sean Lawson, 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats', Journal of Information Technology & Politics 10, no. 1 (2013): 86-103.
[131] Myriam Dunn Cavelty and Kristian Søby Kristensen, 'Introduction: Securing the Homeland: Critical Infrastructure, Risk and (In)security', in Securing 'the Homeland': Critical Infrastructure, Risk and (In)security, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge, 2008), 4.
[132] Conway, 'Media, Fear and the Hyperreal', 125 fn10.

political, military, and economic order'.[133] 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 US because Waterloo does not resonate with American audiences as it might with the British. Tennyson may have constructed Waterloo as that 'world-earthquake',[134] whose tremors are felt even today in the continuing importance of the British victory at Waterloo to the British national psyche, but it means much less to a United States who by June 1815 had only just fought their own war with Britain to a draw, a war in turn mostly forgotten by a British nation preoccupied with Napoleon's challenge to European stability.

Although the two events are very different, Pearl Harbor has as unique a role in American national memory as Waterloo does in the British. There are both archetypal events which still possess the power to shock and inspire, to mobilise popular sentiment, and through which political ends may be pursued. 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 a 1999 article written ahead of both Y2K and the Sydney Olympics.[135] 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 alike 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 similarly intended to arouse a cyber security

[133] CSIS, Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo (Washington, DC: Center for Strategic and International Studies, 1998), 2.
[134] Alfred Tennyson, 'Ode on the Death of the Duke of Wellington (1852)', Poems and Plays, ed. T. Herbert Warren (Oxford: Oxford University Press, 1971), 202-205.
[135] Adam Cobb, 'Electronic Gallipoli?', Australian Journal of International Affairs 53, no. 2 (1999): 133-149.

'consciousness' in its Australian audience. As the concluding section discusses, this search for foundations is characteristic of cyber security's argumentation through the past.

## 5.4 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.[136] 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'.[137] 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 such analogical reasoning portends. There is another facet of this form of representation and argumentation that speaks more fundamentally still to the temporality of cyber security as an expression of its self-image and identity, in which historical analogies 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

[136] On this distinction, see Marita Sturken, Tangled Memories: The Vietnam War, the AIDS Epidemic, and the Politics of Remembering (Berkeley, CA: University of California Press, 1997).
[137] KItzinger, 'Media Templates', 76.

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 demonstrate, it is difficult to communicate and represent cyber security through images alone.[138] As suggested in Chapter Four, 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.[139] 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.[140] 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.[141] 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 suggest, whilst cyber security always mobilises the 'specter of the future', the past is articulated as 'a legitimising reference that underscores the

---

[138] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly 53, no. 4 (2009): 1164-1165.

[139] Albert Borgmann, Holding On to Reality: The Nature of Information at the Turn of the Millennium (Chicago, IL: University of Chicago Press, 1999); Paul Virilio, The Aesthetics of Disappearance (Los Angeles, CA: Semiotext(e), 2009/1980).

[140] Sean Lawson, '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, eds. Christopher Laing, Atta Badii and Paul Vickers (Hershey, PA: IGI Global, 2013), 168-188.

[141] Lewis, 'Aux Armes'; Sean Lawson, 'Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States', First Monday 17, no. 7 (2012), n.p.; Lawson, 'Beyond Cyber Doom'; Clement Guitton, 'Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?', European Security 22, no. 1 (2013): 21-35; Lawson, 'Motivating Cybersecurity'.

gravity of the [present] situation'.[142] 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'.[143] 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'.[144] For Ergma, wrote the journalist who reported her thoughts:

> She spent years studying nuclear energy and watched the world transform as it wrapped itself around the advent of nuclear technology. For her, information warfare is a similar defining moment in world history.[145]

For many, Estonia was a sign of future catastrophe but in this formulation it becomes a foundational event too, an historical anchor that grounds cyber security itself. Was Estonia 'Web War One'? asked journalists and senior defence analysts alike.[146]

---

[142] Hansen and Nissenbaum, 'Digital Disaster', 1164.
[143] Ibid; also, Rid, Cyber War, 174.
[144] Quoted in Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe', Wired 15, no. 9 (2007), 182, cited in Rid, Cyber War, 31. The comparison with Virilio's information accident is striking, which substitutes interactivity for radioactivity but has similarly disruptive, perhaps even destructive, effects; Paul Virilio and Philippe Petit, Politics of the Very Worst: An Interview by Philippe Petit, ed. Sylvère Lotringer (New York: Semiotext(e), 1999/1996), 91.
[145] Davis, 'Hackers'.
[146] Ibid.; Stephen Blank, 'Web War 1: Is Europe's First Information War a New Kind of War?', Comparative Strategy 27, no. 3 (2008): 227-247.

When news of Stuxnet emerged in 2010, comparisons with nuclear weapons were not far behind. 'Stuxnet is the Hiroshima of cyber-war', wrote one journalist in Vanity Fair:

> That is its true significance, and all the speculation about its target and its source should not blind us to that larger reality. We have crossed a threshold, and there is no turning back.[147]

One veteran of the US Department of Homeland Security took great pains to demonstrate why atomic weapons 'were utterly transformative …. Cyberspace is no different', paying close attention to Stuxnet:

> The last time the settled geopolitical worldview was so disrupted, a nuclear explosion devastated Hiroshima. The physical effects of Stuxnet are nowhere near that severe, thankfully. But the cognitive disruptions that will come are just as great. Stuxnet was, figuratively, the first explosion of a cyber atomic bomb.[148]

The search for an originary event upon which to build policy and strategy is evident in such 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 such events in the 'virtual' realm has hampered the quest for strategic 'cyber' deterrence, for example.[149] Repeated attempts have been made to frame contemporary cyber security—in its military and societal dimensions—as a 'new Cold War' but these often founder on inaccuracies and misconceptions, including the inability to identify historically important 'moments' from

[147] Michael Joseph Gross, 'A Declaration of Cyber-War', Vanity Fair, April 2011.
[148] Paul Rosenzweig, Cyber Warfare: How Conflicts in Cyberspace and Challenging America and Changing the World (Santa Barbara, CA: ABC-CLIO, 2013), 2.
[149] Adams, 'Virtual Defense', 106; also, Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', Contemporary Security Policy 33, no. 1 (2012): 148-170.

which this postulated new era might spring.[150] Although such analogies may help in rallying support around a particular issue, 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.

The tendency to reduce the temporally extended to the discrete moment has been identified previously, in 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.[151] In the US, 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'.[152] Narratives that appropriate Pearl Harbor always potentially 'downplay' the longue durée, she writes, ignoring historical specificities to construct identity and politics in the present.[153] 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

[150] For a full discussion of the Cold War metaphor, see Lawson, 'Putting the "War" in Cyberwar'. The quest to analogise cyber security has prompted authors to find other 'beginnings' of the Cold War; for example, Alexander Klimburg, 'Commentary: The Internet Yalta', Center for a New American Security, 5 February 2013.

[151] Also, David Sulek and Ned Moran, 'What Analogies Can Tell Us About the Future of Cybersecurity', The Virtual Battlefield: Perspectives on Cyber Warfare, eds. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 128-130.

[152] Rosenberg, A Date Which Will Live, 188.

[153] Ibid., 188-189. Skinner warns of the 'perpetual danger' of elevating 'the tidiness of our own perceptions and expectations above the possibilities of messy history itself'; Quentin Skinner, 'Meaning and Understanding in the History of Ideas', History & Theory 8, no. 1 (1969): 6-7.

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'.[154] Myth is 'not simply a reflection of an existing reality [but] a source and condition of that reality'.[155] This reminds us 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'.[156] 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'.[157] The contradictions between myth and history are summarised by Raymond Aron:

[154] Andreas Huyssen, Present Pasts: Urban Palimpsests and the Politics of Memory (Stanford, CA: Stanford University Press, 2003), 16.
[155] Craig M. Cameron, American Samurai: Myth, Imagination, and the Conduct of Battle in the First Marine Division, 1941-1951 (Cambridge: Cambridge University Press, 1994), 270, quoted in Theo Farrell, 'Figuring Out Fighting Organisations: The New Organisational Analysis in Strategic Studies', Journal of Strategic Studies 19, no. 1 (1996): 130.
[156] Olivier, Dark Abyss, 9.
[157] Walker, 'History and Structure in the Theory of International Relations', Millennium: Journal of International Relations 18, no. 2 (1989): 170

> Mythologies consist of the substitution of a single factor for the plurality of causes, of lending unconditional value to a desired objective, and of a failure to realize the distance between the dreams of men and the destiny of societies.[158]

There are dangers in this mode of thinking, 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'.[159] 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'.[160] It is no surprise that analogies and metaphors can be important factors in fomenting 'groupthink' and closing off other avenues of intellectual enquiry.[161] As Murray Edelman notes, 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.[162]

The forms of analogical reasoning we choose come with 'practical implications about contents, causes, expectations, norms, and strategic choices'.[163] In information technologies and security, Martin Libicki warns 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

---

[158] Raymond Aron, The Century of Total War (London: Derek Verschoyle, 1954), 97-98.
[159] Glenn D Hook, 'The Nuclearization of Language: Nuclear Allergy as Political Metaphor', Journal of Peace Research 21, no. 3 (1984): 259.
[160] George Lakoff and Mark Johnson, Metaphors We Live By (Chicago, IL: University of Chicago Press, 1980).
[161] Mark Schafer and Scott Crichlow, 'Antecedents of Groupthink: A Quantitative Study', Journal of Conflict Resolution 40, no. 3 (1996): 415-435.
[162] Murray Edelman, The Symbolic Uses of Politics (Urbana, IL: University of Illinois Press, 1964), 124-125.
[163] Davis B. Bobrow, 'Complex Insecurity: Implications of a Sobering Metaphor', International Studies Quarterly 40, no. 4 (1986): 436.

'apt to make their metaphors do their thinking for them'.[164] 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.[165] 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 other studies show, analogies can help political decision-makers both to understand contemporary situations and to justify their political agendas.[166]

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, whilst 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'.[167] In this light, the historical past will continue to be remade in the image of cyber security's present and future.

[164] Martin C. Libicki, Defending Cyberspace and Other Metaphors (Honolulu, HI: University Press of the Pacific, 1997), 6.
[165] See, David J. Betz and Tim Stevens, 'Analogical Reasoning and Cyber Security', Security Dialogue 44, no. 2 (2013): 147-164.
[166] Khong, Analogies at War.
[167] Andrew Hoskins, 'Temporality, Proximity and Security: Terror in a Media-Drenched Age', International Relations 20, no. 4 (2006): 453-466.

# 6 INHABITING THE FUTURE

> The only certain thing about the future is that it will surprise even those who have seen furthest into it.[1]

## 6.1 Introduction: 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, the objective of which was 'to develop a scenario for a coordinated, cross-industry, cyber terrorism event involving mock attacks by computer security experts against critical infrastructure systems in a simulation of state-sponsored cyber warfare attacks'.[2] The exercise concluded that a large-scale event analogous to its historical namesake was unlikely to occur in the future, although the possibility of major disruptions could not be ruled out. It found that 'a group of hackers couldn't single-handedly bring down the United States' national data infrastructure, but a terrorist team would be able to do significant localized damage to US systems'.[3] In particular, it determined that the most vulnerable systems were the Internet and parts of the digital infrastructure of US financial systems.[4] '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 for what may be expected of them should such events occur.

---

[1] Eric Hobsbawm, The Age of Empire, 1875-1914 (London: Abacus, 1994/1987), 340.
[2] Clay Wilson, Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (Washington, DC: Congressional Research Service, April 2005), 9. Note, already in 2001, the conflation of 'cyber terrorism' and 'cyber war(fare).
[3] Margaret Kane, 'US Vulnerable to Data Sneak Attack', CNet News, 13 August 2002.
[4] Wilson, Computer Attack, 10.

A genealogy of these activities would note earlier forms of testing and verification implemented as responses to the multi-user systems that evolved after World War II, which brought non-specialists into computer environments and with them a host of new security problems. In particular, 'time-sharing' practices developed in the 1960s and 1970s drove awareness of and research into computer security, as these allowed multiple users to access a computing resource concurrently, during which time any user's programs and data were held in central memory and hypothetically accessible by any other.[5] Due to the possibilities of malicious behaviour, systems began to need protection from their users and users from each other. Computer scientists and hobbyists alike 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, especially in the defence sector, where 'tiger teams' were routinely deployed as part of software and hardware development and testing.[6]

Unfortunately for systems designers, the tiger teams usually found ways to breach system security, even after the patching of vulnerabilities revealed by earlier testing.[7] 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.[8] The efficacy of

[5] On the development of time-sharing, see Paul E. Ceruzzi, A History of Modern Computing, 2nd. edn. (Cambridge, MA: MIT Press, 2003/1998), 154-158.

[6] Donald Mackenzie and Garrel Pottinger, 'Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the US Military', IEEE Annals of the History of Computing 19, no. 3 (1997): 41-59; Edward Hunt, 'US Government Penetration Programs and the Implications for Cyberwar', IEEE Annals of the History of Computing 34, no. 3 (2012): 4-21.

[7] Mackenzie and Pottinger, 'Mathematics', 46. In 2013, the Pentagon noted these teams still 'invariably' managed to penetrate Department of Defense systems; Defense Science Board, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat (Washington, DC: Department of Defense, January 2013), 28.

[8] Foremost amongst which is 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. For a personal perspective on its legacy, see David Elliott Bell, 'Looking Back at the Bell-LaPadula Model', Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, AZ, 5-9 December 2005, 337-351.

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'.[9]

Cuts in defence expenditure after the end of the Cold War contributed to this problem of computer security without obvious boundaries, as cheaper 'commercial off-the-shelf' solutions were sought for defence systems, with research and development costs borne by industry rather than the taxpayer.[10] The requirement that such 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 mean that, effectively, 'there is no such thing as a forced entry in cyberspace'.[11] There will always be a gap into which an attacker can insinuate code or through which data, in the jargon, can be 'exfiltrated'.[12]

This is the environment in which 'cyber exercises' and their ilk operate. No longer designed merely 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. They operate as forms of anticipatory security practices 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 such 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

[9] Mackenzie and Pottinger, 'Mathematics', 56.
[10] Ibid.
[11] Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare (New York: Cambridge University Press, 2007), 35.
[12] In military jargon, 'exfiltration' is the 'removal of personnel or units from areas under enemy control by stealth, deception, surprise, or clandestine means'; Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2013, as amended through 15 April 2013. In information security, the object of 'friendly' exfiltration has changed from 'people that belong to us' to 'data that belong to them'.

and other managerial and cultural aspects of institutional life. As one analyst argues, most organisations' knowledge of their own cyber security issues is so limited as to be 'alarming'.[13]

Simulations and exercises are considered necessary, above and beyond the requirements of organisational audit and training, because, particularly as one moves towards the military end of the 'attack spectrum', there is a limited set of 'real world' case studies from which to draw information and lessons, let alone ones particular to the institution in question, be it in the private or public sector. In the military case, there has been no conflict between two state militaries in which 'cyber' operations have played the dominant part and from which we could learn how such a conflict evolves and what its effects might be on non-military sectors of society. Again, in the military example, planners often need to simulate cyber attacks and stress-test defensive cyber security without 'threatening the integrity of operational networks', although many are undertaken in non-laboratory situations with appropriate safeguards.[14]

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, as summarised by Claudia Aradau and Rens van Munster:

> Increasingly, security professionals, high-level officials, civil servants, emergency responders as well as ordinary citizens are required by law to take part in exercises and simulations or become the eyes and ears of security experts. As such, we suggest, they are increasingly regimented within the sensorial regime of future catastrophic events. Although this may take place at different sites—from public spaces and artistic expressions to preparedness exercises—surprise and novelty require subjects to

[13] Kenneth Geers, 'Live Fire Exercise: Preparing for Cyber War', Journal of Homeland Security & Emergency Management 7, no. 1 (2010), article 74: 1.
[14] Ibid.

> inhabit the future …. 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.[15]

This chapter explores the ways in which cyber security futures are 'inhabited'. Rather than peer helplessly at the uncertain future or merely 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. 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. As suggested above, 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 such rehearsals of future attacks 'bind future decisions to decisions in the present'.[16] 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'.[17]

Aradau and van Munster argue that in order to achieve such ends, an aesthetic 'sensorium of anticipation' is developed with respect to catastrophic security futures.[18] Crucially, this is not

---

[15] Claudia Aradau and Rens van Munster, Politics of Catastrophe: Genealogies of the Unknown (London: Routledge, 2011), 95, emphasis added.
[16] Ibid., 86.
[17] Philip Sabin, Simulating War: Studying Conflict Through Simulation Games (London: Continuum, 2012), 56.
[18] Aradau and van Munster, Politics of Catastrophe, 85.

merely 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'.[19] The authors 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'.[20] Whereas crises develop and escalate over time, catastrophes simply happen and are unexpected and unpredictable events that disrupt ordinary social conduct.[21] 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 emphasis is often on the latter.[22]

This chapter extends Aradau and van Munster's conceptual framework of 'inhabiting the future' beyond their study of catastrophe to the field of future cyber security events in general. It also develops the concept of inhabitation in a further important 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

[19] Ibid., 86.
[20] Ibid., 28-29.
[21] Birkland suggests that 'crises tend to build over time, whereas disasters strike suddenly'; Thomas A. Birkland, Lessons of Disaster: Policy Change After Catastrophic Events (Washington, DC: Georgetown University Press, 2006), 5. Catastrophes are 'more profound' forms of disaster, on account of their scale and impact.
[22] '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'; Arjen Boin, 'Lessons from Crisis Research', International Studies Review 6, no. 1 (2004): 166.

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.[23] By doing so, we might more fully account for the role of the corporeal political subject in the anticipatory practices of cyber security.

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, in which attempts are made to 'materialise the virtual', such as by demonstrating what physical effects cyber attacks have 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 aim to render invisible threats visible. This shift towards the

[23] Aradau and van Munster, Politics of Catastrophe, 10.

public mediation of cyber security exercises includes the televised Cyber ShockWave exercise (2010), which suggested strongly 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 attentions 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.

## 6.2 Exercise and Simulation

In June 1997, the US government undertook one of the earliest and best-known formal large-scale cyber security exercises, couched in terms of the then-fashionable 'information warfare' (IW). '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 and—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.[24]

[24] Bill Gertz, 'Computer Hackers Could Disable Military', The Washington Times, 16 April 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 subsequent scepticism.[25] More significant than the plausibility of the exercise scenario is how Eligible Receiver quickly became the standard by which other exercises were judged. Chapter Four noted that Eligible Receiver is often interpreted as a 'sign' of 'cyber apocalypse' and 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'[26]—has become almost the default 'lesson' of subsequent US exercises, a lesson apparently corroborated by subsequent real cyber attacks. The year after Eligible Receiver, for instance, a series of cyber attacks dubbed 'Solar Sunrise' was perpetrated against US Department of Defense assets, with Iraq initially suspected due to ongoing US military operations there at the time. Two Californian high school students and a teenaged Israeli hacker were subsequently identified as the intruders but the episode, as a report to Congress concluded, 'confirmed the findings of Eligible Receiver: US information systems are vulnerable'.[27] A US government training video later circulated on the Internet captured this dynamic: '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'.[28]

George Smith, an outspoken critic of US government IW rhetoric in the late 1990s, described what he felt, in the case of Eligible Receiver, was a 'jump from alarming scenario to done deal'.[29] Smith held that the continued classification of information pertaining to such exercises disbarred external, objective evaluation of the claims made for the vulnerability or otherwise

[25] For example, George Smith, 'An Electronic Pearl Harbor? Not Likely', Issues in Science & Technology 15, no. 1 (1998): 68-73.
[26] Gertz, 'Computer Hackers'.
[27] Steven A. Hildreth, Cyberwarfare (Washington, DC: Congressional Research Service, June 2001), 5.
[28] National Infrastructure Protection Center, National Counterintelligence Center and Federal Bureau of Investigation, Solar Sunrise: Dawn of a New Threat, training video, 1999.
[29] Smith, 'Electronic Pearl Harbor'.

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'.[30] The 'done deal' to which Smith referred is the logical conclusion to which the public is drawn in the absence of credible, verifiable information: such 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 such exercises facilitate.

Writing in 2008, Myriam Dunn Cavelty also noted how Eligible Receiver and other early exercises confirmed existing fears about the vulnerability of US information infrastructures to attack. Of a US government-sponsored IW exercise conducted by RAND in early 1995, she concluded:

> the study naturally demonstrated that because the US economy, society, and military relied increasingly on a high-performance networked information infrastructure, this infrastructure presented a set of attractive strategic targets for opponents possessing IW capabilities. The fears everybody had were thus substantiated by this exercise.[31]

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

[30] Ibid.
[31] Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008), 82.

exist'.[32] 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 merely 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.

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.[33] Nevertheless, the singular and destructive event is still the benchmark against which the mettle of these institutions is tested, be they 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.[34] Cyber exercises are also conducted in preparation for large-scale, 'non-cyber' events that definitively will happen, such as the Olympic Games and other public spectacles.[35]

Like counterterrorism exercises contingent upon a terrorist 'event', what these cyber exercises demand from those involved in them is 'not so much that they are able to imagine plausible futures in order to help prevent them from becoming real but rather urges them to inhabit, rehearse and exercise the event in order to devise adequate responses should the event ever materialize'.[36] This requires that there be a 'world' for participants to inhabit and cyber

[32] John Arquilla, 'Information Wars', in Globalization and Security: An Encyclopedia, vol. 1, Social and Cultural Aspects, eds. G. Honor Fagan and Ronaldo Munck (Westport, CT: Praeger Security International, 2009), 212.
[33] Reports on Cyber Storm I (2006), II (2008) and III (2010) are available from http://www.dhs.gov/cyber-storm-securing-cyber-space.
[34] For a survey of 85 cyber exercises (2002-2012), see ENISA, On National and International Cyber Security Exercises: Survey, Analysis and Recommendations (Heraklion: ENISA, 2012).
[35] For a review of IT security for London 2012, see Institute of Engineering and Technology, Delivering London 2012: ICT Implementation and Operations (Stevenage: The IET, 2013).
[36] Aradau and van Munster, Politics of Catastrophe, 22.

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 coordinated cyber attack'.[37] 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.[38] London 2012's technical partner, ATOS, described its approach to simulating future cyber attacks:

> Security testing on the system will be carried out in a specially isolated version of the Olympic network, using an in-house team of pretend hackers. 'We simulate past competitions and we have a shadow team of about 100 people coming and creating problems—injecting viruses, disconnecting PC servers …. We are using a simulation system so it doesn't really matter if we corrupt the data. We simulate the effect and see how people react.'[39]

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 likely to be 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.[40] The responses to this inevitable shortcoming are either to run more simulations, or to increase the computing power of the simulation. In the former

[37] National Cyber Security Division, Cyber Storm: Exercise Report (Washington, DC: Department of Homeland Security, 2006), 14.
[38] Geers, 'Live Fire Exercise', 6.
[39] BBC News, 'Cyber-Attack Tests for Olympic Computer Systems', 10 October 2011.
[40] Geers, 'Live Fire Exercise', 4.

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', and organisers also ran repeated simulations for months prior to the Games.[41]

In the second category, there have been notable attempts to build truly impressive simulation environments, such as the US Department of Defense's National Cyber Range (NCR), development of which began in 2008.[42] 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.[43] Secretary of Homeland Security Michael Chertoff informed a security conference of the historical significance of the Comprehensive National Cybersecurity Initiative (CNCI) of which the NCR would be part:[44]

> This is, I don't want to overdo the analogy, but it would almost be like a Manhattan project to defend our cyber networks in the same way that we've undertaken previous efforts in the past to deal with emerging threats.[45]

One 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

---

[41] Institute of Engineering and Technology, Delivering London 2012: ICT Enabling the Games (Stevenage: The IET, 2011), 23.

[42] The UK launched its own cyber range in October 2010; 'Defence Minister Opens UK Cyber Security Test Range', Gov.uk, 26 October 2010, https://www.gov.uk/government/news/defence-minister-opens-uk-cyber-security-test-range.

[43] DARPA, 'National Cyber Range Proposers' Day Workshop', Special Notice DARPA-SN08-33, 29 April 2008.

[44] Details of the Bush, and later Obama, administrations' CNCI can be found at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[45] Michael Chertoff, 'Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference', San Francisco, CA, 8 April 2008. Since 1996, there have been many calls for a 'cyber' Manhattan Project and at least one public-private initiative has taken that name. Recently, one prominent legal scholar has written: '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'; Jonathan Zittrain, The Future of the Internet—And How To Stop It (London: Penguin, 2008), 173.

launch of which led directly to the founding of DARPA's forerunner in 1958.[46] The historical import of the NCR is for future minds to discern, particularly as it only went 'live' in 2012, when the operational responsibility for the $130 million project was transferred from DARPA to the testing and evaluation arm of the Department of Defense.[47] The DARPA press release announcing the handover noted the 'key benefits' of the NCR:

> the speed with which the range can be re-configured, the diversity of the networks that can be emulated, and the flexibility to handle multiple activities simultaneously at different classification levels. Given the dynamic nature of real-world cyber threats, providing fast-turnaround time for experimentation and analysis is vital.[48]

The NCR is able not only to simulate the behaviour of complex assemblages of code and machines ('nodes') but of people ('users') too, designated in the original design proposals as 'basic human replicants',[49] 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 this popular culture intertexuality, the UK's The Register declaring, 'DARPA Wants Matrix-Style Virtual World for Cybergeddon'.[50]

In contrast to the replicants of Blade Runner—genetically engineered creatures which impersonate human form and behaviour and who live amongst them, albeit illegally—and the simulated corporeality of the inhabitants of the Matrix, whose physical bodies are held in laboratory stasis elsewhere, the NCR replicants are non-sentient, non-corporeal informational

---

[46] Sharon Weinberger, 'Cyberwarfare: DARPA's New "Space Race"', Danger Room, 1 May 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'; David E. Sanger, John Markoff and Thom Shanker, 'US Plans Attack and Defense in Web Warfare', The New York Times, 28 April 2009.

[47] Ultimately, the NCR will be transferred to US Cyber Command (USCYBERCOM), itself only operational since 2010.

[48] DARPA, 'National Cyber Range Rapidly Emulates Complex Networks', press release, 13 November 2012.

[49] DARPA, 'National Cyber Range', Broad Agency Announcement DARPA-BAA-08-43, 5 May 2008.

[50] Lewis Page, 'DARPA Wants Matrix-Style Virtual World for Cybergeddon', The Register, 7 May 2008. The reference is to The Matrix (dirs. Lana Wachowski and Andy Wachowski, 1999).

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 solely in order to be killed. In these simulations the environment is merely a 'kill-box' where body counts matter and 'kinetic exchanges' are the 'order of the day'.[51]

For the real human participants, these 'virtual' environments are still experienced physically. James Der Derian's description of 'playing' a version of the 'first-person shooter' computer game Doom created by the US Marine Corps underscores further that physical affect persists even in such environments:

> The high quality graphics, sounds of gunfire and heavy breathing, and the sight of rounds kicking up in your face, as well as the constant patter of the lieutenant …. gave the 'game' a pretty high dose of realism, especially if accelerated heartbeat is any measure.[52]

In the case of cyber simulations and exercises such as those at the NCR, we can assume a similarly 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 such activities but from

[51] Christopher Coker, Warrior Geeks: How 21st Century Technology is Changing the Way We Fight and Think About War (London: Hurst & Company, 2013), 128.
[52] James Der Derian, Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network, 2nd. edn. (New York: Routledge, 2009), 90. Also, Roger Smith, 'The Long History of Gaming in Military Training', Simulation & Gaming 41, no. 1 (2010): 6-19.

other sources we can develop a basic picture of the environment.[53] 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.[54] This is a sensory assemblage far removed from the adrenalinized physicality of the traditional theatre of war but it is still one experienced sensorily, physiologically and emotionally by its human participants.

Such conditions will probably be encountered in the majority of cyber exercises, where informational rather than physical terrain is the resource over which control must be established. Whether military or civilian, or a combination of private and public sectors, the environments in which simulations are run 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 untutored 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.

---

[53] Some details are provided in a Lockheed Martin presentation (2012) available at http://www.ndia.org/Resources/OnlineProceedings/Documents/21M0/MODSIM/03-Defense-Pridmore.pdf.

[54] See, 'Locked Shields 2012', http://vimeo.com/42610977, and 'CDX Locked Shields 2013', http://vimeo.com/65305608.

These abstracted battlespaces represent the informational environments in which future cyber conflicts will be played out but they are not the only way in which the future is imagined and rehearsed. Due to the epistemological uncertainty which makes 'lessons learned' difficult to communicate to the public and the inherent difficulties identified in previous chapters with 'materialising the virtual' there are attempts to overcome or at least mitigate these problems by resorting to aesthetic modalities of a more established nature than is suggested by 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, including by the public.

## 6.3 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 4th March 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.[55] 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'.[56] The experiment was widely considered the first proof that hackers could enter a sophisticated

[55] The video is no longer available from CNN but is accessible at http://www.youtube.com/watch?v=fJyWngDco3g, accessed 4 May 2013.
[56] David A. Fulghum, 'No Fingerprints: Culprits in the Cyberattack on Iran are Still Unknown', Aviation Week & Space Technology 172, no. 36 (4 October 2010): 29.

industrial control system and cause a physical device to self-destruct.[57] This, suggested experts, showed that 'large electrical systems are vulnerable in ways not previously demonstrated'.[58] From this premise, a narrative of ever-greater threat was developed. Of the experiment, CNN reported:

> Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power. Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.[59]

For a specific investment—'about $5 million and between three to five years of preparation', according to one expert—an adversary could mount a plausible 'strategic attack' against the US which, if successful, could cost the country hundreds of billions of dollars.[60] 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'.[61]

Although some of the reporting may have been hyperbolic and some of the expert scenarios a little fanciful or exaggerated, much of the commentary by public officials was quite circumspect, identifying and accepting a vulnerability, giving assurances that it was being addressed, and stressing that the destruction imagined by some was possible, if highly unlikely. Later still, another simulation at Idaho National Laboratory, this time attended by journalists,

---

[57] Although, see the Maroochy Shire sewage system incident (2000), described in Thomas Rid and Peter McBurney, 'Cyber-Weapons', The RUSI Journal 157, no. 1 (2012): 10. There are also earlier press reports of INL tests resulting in physical destruction of infrastructure components; Justin Blum, 'Hackers Target US Power Grid', The Washington Post, 11 March 2005.
[58] Jeanne Meserve, 'Mouse Click Could Plunge City Into Darkness, Experts Say', CNN.com, 26 September 2007, http://edition.cnn.com/2007/US/09/26/power.at.risk/.
[59] Ibid.
[60] Ibid.
[61] Ibid.

showed how a red team could access a chemical plant mock-up and take control of the water-pumping system.[62] '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'.[63] 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. As journalists and analysts later found, however, it took substantial investment of time and resources to bring about these results.[64]

If industrial plant might seem quite obscure to the average observer, subsequent simulations would attempt 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 defense sector:

> SANS [Institute] today announced NetWars CyberCity, a small-scale city located close by the New Jersey turnpike complete with a bank, hospital, water tower, train system, electric power grid, and a coffee shop. NetWars CyberCity was developed to teach cyber warriors from the US military how online actions can have kinetic effects. SANS has defined various missions within CyberCity to help train cyber warriors to defend against online attacks and teach them how to secure a city's vital physical infrastructure[65]

---

[62] Mike M. Ahlers, 'Inside a Government Computer Attack Exercise', CNN.com, 17 October 2011, http://edition.cnn.com/2011/10/17/tech/innovation/cyberattack-exercise-idaho.
[63] Tom Gjelten, 'Stuxnet Raises "Blowback" Risk in Cyberwar', NPR.org, 2 November 2011, http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar.
[64] David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown Publishers, 2012), 188-209. Whether Stuxnet achieved its strategic aims is debatable; Ivanka Barzashka, 'Are Cyber-Weapons Effective?', The RUSI Journal 158, no. 2 (2013): 48-56.
[65] SANS Institute, 'SANS Launches NetWars CyberCity to Train Cyber Warriors for Defense', press release, 27 November 2012.

At the time, over 18 missions had been devised, lasting from a few hours to a few days.[66] The online magazine that broke the story described some of these missions:

> students must figure out how to simultaneously turn all of the traffic lights in town red, to halt the escape of terrorists fleeing the city. In others, they must derail a train barreling toward town with radiological weapons, or reprogram a rocket launcher on the military base that's been aimed at the hospital.[67]

The rationale for creating an urban mock-up was to stress the linkages and interdependencies of the 'cyber' and the physical.

> [It's] the simplest way to illustrate how dominoes fall in the real world. 'If you were to do the entire thing simulated, it would be less meaningful to most of the [military] leadership. They want to see physical things. They want to see the battle space, and what's happening there …. That's our whole goal here: to show you can cause physical damage or change in a city environment entirely using computers'.[68]

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',[69] and 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.

---

[66] BBC News, 'US Military Train in Cyber-City to Prepare Hack Defence', 28 November 2012.
[67] Emily Badger, 'A Tiny City Built to Be Destroyed by Cyber Terrorists, So Real Cities Know What's Coming', Co.Exist, n.d., http://www.fastcoexist.com/1681033/a-tiny-city-built-to-be-destroyed-by-cyber-terrorists-so-real-cities-know-whats-coming#1.
[68] Ibid.
[69] Seymour E. Goodman, Jessica C. Kirk and Megan H. Kirk, 'Cyberspace as a Medium for Terrorists', Technological Forecasting & Social Change 74, no. 2 (2007): 196-197.

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'.[70] From the Wiltshire villages first hollowed out by national need during World War II 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.[71] What is remarkable about CyberCity is that the entire 'city' 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:

> This isn't a working model of a town; it's just a model of a town. There's a whiff of security theater to all this—theater rendered in adorably modeled miniature. The game is, compared to its interactive counterparts, low-budget and low-tech—comically and terrifyingly so on each count. But that's part of the point. There's a psychic effect to the modeling here, a reminder of the kinetic effects of cyberwar …. As it is, CyberCity, with its scaled-down and model-focused layout, emphasizes the connections between the cloud-connected world and the quotidian; in its way, it exposes the many vulnerabilities in the places we take most for granted.[72]

[70] BBC News, 'US Military Train in Cyber-City'. On the history of one of these Wiltshire villages, see Rex Sawyer, Little Imber on the Down: Salisbury Plain's Ghost Village (East Knoyle: The Hobnob Press, 2001).
[71] For a description of 'Mojave Viper' at Twentynine Palms, CA, see Der Derian, Virtuous War, 274ff. This was later expanded at the cost of $170 million into a 'mock city' the 'size of downtown San Diego'; Julie Watson, 'Mock City Rises at Marine Base for Urban Training', Associated Press, 25 January 2011.
[72] Megan Garber, 'The Future of Cybersecurity Could Be Sitting in an Office in New Jersey', The Atlantic, 4 January 2013.

As SANS Institute director Eric Bessel asserted, when 'you lose control of cyberspace, you lose control of the physical world'.[73] Through illustrations of this argument, these simulations serve to raise awareness and concern, whilst 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 real-ness 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'.[74] 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'.[75] 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 defense exercise intended to assess how a 'typical' US

[73] BBC News, 'US Military Train in Cyber-City'.
[74] Der Derian, Virtuous War, 125.
[75] Ibid.

community—'rendered down to the last detail of consumer desire'—would fare after a 29-kiloton nuclear blast:

> An entire town was built on the test site [in Nevada], consisting of a fire station, a school, a radio station, a library, and a dozen homes in the current building styles. These buildings were carefully constructed, furnished with the latest consumer items—appliances, furniture, televisions, carpets, and linens—and stocked with food that had been specially flown in from Chicago and San Francisco. Residences were populated with mannequins dressed in brand new clothing and posed with domestic theatricality—at the dinner table, cowering in the basement, or watching television.[76]

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.[77] The reported damage 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'.[78]

> The formal message of Operation Cue was that the postnuclear environment would be only as chaotic as citizens allowed, that resources (food, shelter, and medical) would still be present, and that society—if not the nation-state—would continue. Nuclear war was ultimately presented as a state of mind that could be incorporated into ones [sic] normative reality—it was simply a matter of emotional preparation and mental discipline.[79]

---

[76] Joseph Masco, 'Nuclear Technoaesthetics: Sensory Politics from Trinity to the Virtual Bomb in Los Alamos', American Ethnologist 31, no. 3 (2004): 353-354. Also, Federal Civil Defense Administration, Cue For Survival: Operation Cue (Washington, DC: US Government Printing Office, 1955).
[77] Federal Civil Defense Administration, 'Operation Cue', 1955.
[78] Masco, 'Nuclear Technoaesthetics', 354.
[79] Joseph Masco, '"Survival is Your Business": Engineering Ruins and Affect in Nuclear America', Cultural Anthropology 23, no. 2 (2008): 375-376.

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.[80] By 1983, when the television movie The Day After (dir. Nicholas Meyer, 1983) was viewed by an audience of 100m Americans—roughly the same as watched the Operation Cue broadcast—President Reagan's Strategic Defense Initiative was threatening to destabilise the hard-won nuclear standoff, and movies had moved into a significantly more pessimistic register that questioned the illusion of survivability.[81] 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.[82] 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.[83]

Studies of the public reception of movies like The Day After are divided as to their emotional and political effect but these imagined futures doubtless serve at some minimum level to raise awareness of the nuclear issues presented.[84] 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

[80] Lawrence Freedman, The Evolution of Nuclear Strategy (Houndmills: Macmillan Press, 1981).
[81] For an account of Reagan's response to the movie, see Simon Braund, 'How Ronald Reagan Learned to Start Worrying and Stop Loving the Bomb', Empire 257 (2010): 134-140.
[82] Daniel Cordle, '"That's Going to Happen to Us. It Is": Threads and the Imagination of Nuclear Disaster on 1980s Television', Journal of British Cinema & Television 10, no. 1 (2013): 71-92.
[83] Daniel Cordle, 'Protect/Protest: British Nuclear Fiction of the 1980s', The British Journal for the History of Science 45, no. 4 (2012): 653-669.
[84] Stanley Feldman and Lee Sigelman, 'The Political Impact of Prime-Time Television: "The Day After"', The Journal of Politics 47, no. 2 (1985): 556-578; Janet W. Schofield and Mark A. Pavelchak, '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 (1989): 433-448.

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 videotaped and presumed leaked to CNN; by 2011, journalists were embedded in the simulation environment from the start. 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 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.[85]

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 US was insufficiently prepared for cyber attacks and that more administrative powers were required to control national communications networks in times of emergency.[86] 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.

[85] CNN, 'We Were Warned: Cyber Shockwave', first broadcast, 20 February 2010. A transcript is available at http://transcripts.cnn.com/TRANSCRIPTS/1002/20/se.01.html. Also, Bipartisan Policy Center, 'Cyber ShockWave', http://bipartisanpolicy.org/events/cyber2010.

[86] Bipartisan Policy Center, 'Cyber ShockWave Shows US Unprepared for Cyber Threats', press release, 17 February 2010.

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 can be excavated from this exercise, seems to have been an important aim.

> Former Clinton press secretary Joe Lockhart, who played a presidential adviser during the simulation, said it was immaterial whether the attack was an act of war; it had 'the effect' of an act of war …. Lockhart said that people would be scared by the simulation but that 'that's a good thing'. Only then, he said, would Congress act.[87]

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]'.[88] The public were assisted in this by the production itself, a mainstream approximation of what a 'hi-tech' situation room might look like, one not too dissimilar from the cyber exercise environments discussed previously, albeit with added futuristic graphics, dramatic overlays, non-stop portentous music and the presence of a real news anchor-man '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. Mediated events like 'Cyber ShockWave' show how audiences are enveloped in a sensory world created by the confluence of information technology, media, politics and

[87] Ellen Nakashima, 'War Game Reveals US Lacks Cyber-Crisis Skills', The Washington Post, 17 February 2010.
[88] Ibid.

security. That the real and the irreal, the actual and the virtual, might no longer be separated with certainty is illustrated by CNN keeping the word 'SIMULATION' permanently on overlay throughout the Cyber ShockWave broadcast.[89] In the absence of research calibrated to doing so, it is difficult to assess the effects of such activities on the public imagination and in political terms but such 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.

## 6.4 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'.[90] 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.[91] A year later, speaking at Cyber Security Summit 2012, Cabinet Office minister Chloe Smith stated even more clearly why these activities were

[89] Perhaps mindful of The War of the Worlds radio drama controversy (1938), in which millions of Americans were duped into believing they were under alien attack, CNN was probably wise to do so.
[90] Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (London: Cabinet Office, November 2011), 29. Pertinently, government had no idea how many people were working in government cyber security at this point; House of Commons Committee of Public Accounts, Information and Communications Technology in Government: Report, Together with Formal Minutes, Oral and Written Evidence, HC 1050 (London: The Stationery Office, July 2011), 10.
[91] Cabinet Office, Cyber Security Strategy. Also, Office of Cyber Security and Information Assurance, 'Cyber Security Skill Shortages', ITNOW 54, no. 2 (2012): 32-34.

necessary: '[o]ur ability to defend ourselves in cyberspace depends upon a strong skills and knowledge base'.[92] In the first comprehensive government review of UK cyber security, the National Audit Office (NAO) 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.[93] These and many other statements make a direct link between the national security of the UK and skills shortages in technical cyber security and allied fields, a situation one government cyber security official described as 'wholly inadequate'.[94]

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.[95] 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'.[96] The Pentagon's Cyber Command, which became operational in 2010, with responsibility for protecting national and Department of Defense 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, a task it confirmed would be difficult because of the recruitment situation.[97] The Pentagon recognised that defence budget cuts would compound these problems, not only

[92] Chloe Smith, speech to Cyber Security Summit, London, 6 November 2012.
[93] National Audit Office, The UK Cyber Security Strategy: Landscape Review, HC 890 (Norwich, The Stationery Office, February 2013), 26.
[94] Raphael Satter, 'Amateurs Battle Malware, Hackers in UK Cybergames', Associated Press, 11 March 2012.
[95] Eric Beidel and Stew Magnuson, 'Government, Military Face Severe Shortage of Cybersecurity Experts', National Defense, August 2011.
[96] Mark Weatherford, quoted in InfoSecurity, 'RSA 2013: As Cybersecurity Receives More Attention, DHS Becomes a Critical Player', 26 February 2013. Weatherford subsequently left for the private sector, to a consultancy run by ex-DHS secretary, Michael Chertoff.
[97] Elisabeth Bumiller, 'Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks', The New York Times, 28 January 2013; Ellen Nakashima, 'Pentagon to Build Up Its Cybersecurity Force', The Washington Post, 28 January 2013.

in making new appointments but also in retaining existing staff, whether soldiers or civilians. In the short term, head of Cyber Command General Keith Alexander admitted before Congress, he would find it difficult to staff the 40 support and operational 'cyber' teams he was committed to providing across the US military by autumn 2015.[98] Given that 13 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.

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: 'business conditions' demanding greater attention to information security across enterprise and the public sector; insufficient executive-level understanding of information security needs; and a lack of appropriately skilled and educated information security professionals.[99] 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 with the private sector for skilled personnel and also with one another.[100]

---

[98] Ellen Nakashima, 'Pentagon Plans to Add 13 Offensive Teams to Combat Online Threat', The Washington Post, 13 March 2013.

[99] Frost and Sullivan, The 2013 $(ISC)^2$ Global Information Security Workforce Study (Mountain View, CA: Frost and Sullivan, 2013), 12-14.

[100] In 2012, GCHQ told Parliament that these considerations meant it was 'losing critical staff with high end cyber technology skills at up to three times the rate of the corporate average'; Intelligence and Security Committee, Annual Report 2011-2012, Cm. 8403 (Norwich: The Stationery Office, July 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.[101] 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 although it was not unusual for technicians to have problems 'adjusting to more modern ideas as they grow older', it was new to find that 'the revolution which computers have forced on us is placing considerable intellectual strain on the whole mature generation of managers whose task is to evaluate and control, and whose education gave them no hint of what the future held for them'.[102] The Committee was concerned that the basic intellectual foundations of some fields were not even taught when the current cohort of professionals was in education, such was the pace of scientific and technological change. Although 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, 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 person potentially amenable to careers in cyber security: respectively, existing professionals, 'hackers', and the young.

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,

[101] It is a common lament that there are insufficient graduates in science, technology, engineering and mathematics (STEM). See, for example, House of Lords Select Committee on Science and Technology, Higher Education in Science, Technology, Engineering and Mathematics (STEM) Subjects: Report, HL Paper 37 (London: The Stationery Office, July 2012). On the US situation, see Microsoft, A National Talent Strategy: Ideas for Securing US Competitiveness and Economic Growth (Redmond, WA: Microsoft Corporation, September 2012).

[102] Committee on Manpower Resources for Science and Technology, The Flow Into Employment of Scientists, Engineers and Technologists. Report of the Working Group on Manpower for Scientific Growth, Cmnd. 3760 (London: HMSO, September 1968), 101.

training and development, risk analysis, policy and business'.[103] This recruitment drive is supported by new certification schemes aimed at providing 'cyber professionals' with a clear sense of personal progress along their chosen career paths.[104] Open competitions such as 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, whilst providing training, bursaries, work placements and, sometimes, job offers to those who win the various classes and categories of competitions held each year.[105] These public-private partnerships present a strong sense of civic responsibility and engagement. The CSCUK, for example, intends to satisfy the national demand for 'a larger and more dynamic cyber security workforce' underpinning 'the social, political and financial fabric of modern society'.[106] 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'.[107]

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'.[108] This reflected a common perception of hackers as 'anti-social, possibly dangerous individuals …. the new enemy of the Information Age'.[109] Ten years later, UK security minister Lord West articulated a

[103] OCSIA, 'Cyber Security', 33.
[104] GCHQ, 'New Certification Scheme Announced for IA Professionals', press release, 24 October 2012.
[105] As of March 2013, only 40 of the approximately 7000 participants across four iterations of CSCUK had been offered employment in cyber security. CSCUK stresses its role in raising awareness of cyber security issues and careers, as much as their impact on direct recruitment; Sooraj Shah, 'Cyber Security Challenge "Is Not Only About Recruiting Talent", Claims CEO', Computing, 13 March 2013.
[106] Cyber Security Challenge UK, 'Why We Need It', https://cybersecuritychallenge.org.uk/why-we-need-it.php, accessed 14 May 2013.
[107] US Cyber Challenge, 'Our Mission', http://www.uscyberchallenge.org/our-mission/, accessed 14 May 2013.
[108] National Infrastructure Protection Center et al, Solar Sunrise.
[109] Helen Nissenbaum, 'Hackers and the Contested Ontology of Cyberspace', New Media & Society 6, no. 2 (2004): 197-217. Also, Debora Halbert, 'Discourses of Danger and the Computer Hacker', The Information Society 13, no. 4 (1997): 361-374.

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.[110] Although West suggested that government would not recruit any 'ultra, ultra criminals', 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'.[111]

We might perhaps expect such 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.[112] 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.[113] Hackers may have 'potentially useful knowledge', writes Athina Karatzogianni, 'but such knowledge often does not sit comfortably with the academic and commercial worlds' preference for ethically unproblematic and rigorously researched knowledge'.[114] This has not prevented governments from attempting to recruit 'hackers' and Lord West's suggestion is consistent with other governmental efforts in this regard.

---

[110] Duncan Gardham, 'Hackers Hired to Halt Attacks on Britain by Cyber Terrorists', The Daily Telegraph, 26 June 2009.
[111] Siobhan Chapman, 'Government Criticised for Plan to Hire "Naughty Boys"', ComputerWorld UK, 30 June 2009.
[112] Paul A. Taylor, Hackers: Crime in the Digital Sublime (London: Routledge, 1999). Importantly, Taylor notes media and computer security industry roles in narrowing hacking to 'computer-based activities' alone, a conceptual straitening at odds with its original coinage as 'the imaginative and unorthodox use of any artefact' (ibid., viii).
[113] Ibid., 137.
[114] Athina Karatzogianni, The Politics of Cyberconflict (Abingdon: Routledge, 2006), 98.

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.[115] 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.[116] '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.

The game is still played but has lost some of its piquancy, particularly since DEFCON 7 in 1999, which hosted a 'Meet the Fed' panel for the first time.[117] 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.[118] 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. Although we cannot yet determine the success of this initiative, we might 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

[115] Thomas J. Holt, 'Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures', Deviant Behavior 28, no. 2 (2007): 193-194. These contests have been part of other conventions since the early 1990s; Alexander Urbelis, 'Toward a More Equitable Prosecution of Cybercrime: Concerning Hackers, Criminals, and the National Security', Vermont Law Review 29, no. 4 (2005): 976.

[116] Ed Pilkington, 'Fear: The Old Technology that Turned Hackers Into Informers', The Guardian, 7 June 2011.

[117] DEFCON 7, Las Vegas, NV, 9-11 July 1999, https://www.defcon.org/html/links/dc-archives/dc-7-archive.html. The more corporate Black Hat conference which precedes DEFCON had a 'Meet the Feds' panel in 1998; The Black Hat Briefings, Las Vegas, NV, 29-30 July 1998, https://www.blackhat.com/html/bh-usa-98/nss-schedule.html.

[118] The author attended one such panel in 2009, which included speakers from the Defense Computer Forensics Laboratory, Department of Defense, Department of Homeland Security, NASA, National Security Agency, Treasury, US Postal Service, and many others; DEFCON 17, Las Vegas, NV, 30 July-2 August 2009, https://www.defcon.org/html/links/dc-archives/dc-17-archive.html. Also, Gerry Smith, 'Feds Turn to Hackers to Defend Nation in Cyberspace', Huffington Post, 10 August 2011.

Security Agency and US Cyber Command, General Keith Alexander.[119] 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.[120]

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.[121] It is even possible to obtain professional certification as a 'Certified Ethical Hacker',[122] although one leading computer security specialist dismissed this nomenclature as a 'contradiction in terms' equivalent to 'ethical rapist'.[123] In June 2013, the US held its first National Day of Civic Hacking, organised by 'Code for America' and supported by a range of public- and private-sector organisations.[124] This event encouraged people

> to collaboratively create, build, and invent new solutions using publicly-released data, code and technology to solve challenges relevant to our neighborhoods, our cities, our states and our country [and] will provide citizens an opportunity to do what is most quintessentially American: roll up our sleeves, get involved and work together to improve our society.[125]

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

---

[119] Marcus Colon, 'Spies Recruiting Hackers: Gen. Keith Alexander at DefCon', SC Magazine, September 2012.
[120] Kevin D. Mitnick and William L. Simon, Ghost in the Wire: My Adventures as the World's Most Wanted Hacker (New York: Little, Brown and Company, 2011). Early examples of this confessional genre are discussed in Andrew Ross, Strange Weather: Culture, Science and, Technology in the Age of Limits (New York: Verso, 1991), 83-84.
[121] Cabinet Office, UK Cyber Security Strategy, 29.
[122] International Council of e-Commerce Consultants (EC-Council), 'Certified Ethical Hacker', http://www.eccouncil.org/courses/certified_ethical_hacker.aspx, accessed 16 May 2013.
[123] Marcus Ranum, quoted in Alberto D'Ottavi, 'Firewall Pioneer: Security Needs Integration', Zone-H, 4 February 2003.
[124] http://hackforchange.org/, accessed 15 May 2013.
[125] http://hackforchange.org/page/about, accessed 15 May 2013.

brainpower and ingenuity to create, enhance or fix something'.[126] This is broadly in agreement with long-established self-perceptions of hacking by hackers themselves 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.

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 the young as a valuable career path and 'life skill'. In May 2012, the UK government's special representative to business for cyber security told delegates to an IT security conference, '[t]here are far too many people over 40 working in this area and not nearly enough in their twenties'.[127] Echoing the concerns of the Committee on Manpower Resources for Science and Technology some 45 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'.[128] This emphasis on educating children and young adults in cyber security has been a distinct feature of cyber security policy in the UK and provides not only a framework and a future for cyber security careers but a framework for the future of cyber security itself.

---

[126] Ibid.

[127] Quoted in Anh Nguyen, 'UK Cybersecurity Professionals are "Too Old", Says Baroness Neville-Jones', ComputerWorld UK, 24 May 2012. Survey data supports this view, with only 7% of UK cyber security professionals aged 20-29; e-skills UK, Career Analysis into Cyber Security: New and Evolving Occupations (London: e-skills UK, 2013), 13.

[128] Nguyen, 'UK Cybersecurity Professionals'.

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.[129] 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 eight Academic Centres of Excellence in Cyber Security Research at British universities, and new training programmes in cyber security at major universities.[130] 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 amongst young women. A pilot program starting in autumn 2013 would target 2000 secondary schools, before expanding it across England and Wales in 2014. 'There will be regional trials, a bit like football', said CSCUK's chief executive, 'and then we will have a grand final in February or March next year [2014]. The winners will go on a cybercamp'.[131] Adult versions of intensive 'camps' lasting several days were trialled in the UK in 2012 for adult participants and borrow from similar schemes in the United States; on both sides of the Atlantic they are also referred to in the militarised language of 'boot camps'. As described by the BBC, the scenarios encountered by these youthful participants 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.[132]

---

[129] CSCUK, 'Education', https://cybersecuritychallenge.org.uk/education.php, accessed 14 May 2013.
[130] GCHQ, 'UK Universities Awarded Academic Centre of Excellence Status in Cyber Security Research', press release, April 2012; Sean Coughlan, '£7.5m University Fund to Train Cybersecurity Experts', BBC News, 9 May 2013.
[131] Nick Hopkins, '"Cyber Jedi" Schools Contest a New Hope for Britain's IT Empire to Strike Back', The Guardian, 28 April 2013.
[132] Natalie Ostroff and Jim Taylor, 'First Boot Camp Gets Young People Into Cybersecurity', BBC Newsbeat, 7 September 2012.

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.[133] In September 2014, the existing national ICT curriculum will be 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.[134]

Moving away from a teaching model centred on office software packages, the reinvigorated ICT program emphasises the desirability of online training programmes, a more interactive pedagogical environment and the need and opportunities for programming and application development.[135] 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.[136] 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' suggests that it may yet become formally integrated into ICT education.[137] There are, however, indications that cyber security is already being taught, or at least addressed, at both secondary and primary levels of education.

---

[133] Jonathan Watson, 'Getting Serious About Security', Business Technology, April 2012, 9.
[134] Department of Education, '"Harmful" ICT Curriculum Set to Be Dropped to Make Way for Rigorous Computer Science', press release, 11 January 2012. The term 'ICT' will be discarded, as it 'carries negative connotations of a dated and unchallenging curriculum that does not serve the needs and ambitions of pupils'; Department for Education, 'Consultation on Computing and Disapplication of the Current National Curriculum', 3 May 2013.
[135] The Raspberry Pi Foundation is a good example of encouraging children to program computers, rather than use prepared software packages, http://www.raspberrypi.org/.
[136] Rosalie Marshall, 'Ofsted, Microsoft and Teachers Voice Concerns with Draft DfE Computing Curriculum', V3.co.uk, 1 March 2013.
[137] Cabinet Office, UK Cyber Security Strategy, 31.

A report by the Information Assurance Advisory Council in conjunction with the Cabinet Office records that police 'are now in schools talking to year 3 [seven- and eight-year-olds] about cyber security', although no details are provided that corroborate this claim.[138] The same report suggests that information security should be built into teacher training qualifications, informed by the need to 'spread security metaphors without making people scared'.[139] The analogy is drawn between cyber security and road safety: 'Appropriate education at all levels is like a kerb drill for cyber security'.[140] The government-sponsored body charged with developing technology skills for business, e-skills UK, has developed 'Behind the Screen', a project preliminary to the development of a general secondary certificate in computing.[141] Cyber security is one of the topics directed at 14-16 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![142]

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

---

[138] Information Assurance Advisory Council, Record of a Joint IAAC/Cabinet Office Seminar—UK Cyber Security Strategy (Swindon: IAAC, January 2012), 8.
[139] Ibid., 9.
[140] Ibid., 10.
[141] http://www.behindthescreen.org.uk/.
[142] e-skills UK, 'Cyber Security in Schools', n.d., http://az290931.vo.msecnd.net/www.infosec.co.uk/__novadocuments/28345x$query$xvx$eq$x635018761162070000, accessed 15 May 2013.

time.[143] 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.[144] Least these be thought excluded from the purview of cyber security, all three are mentioned in the 2011 UK Cyber Security Strategy as models of progressive child online safety and protection and categorised as an aspect of cyber security concerned with personal internet safety.[145]

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 suggest 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.[146] 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. Although 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, the emphasis on security raises worrying questions about who exactly is being asked

[143] Department of Education, 'Child Internet Safety', 1 May 2013, http://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety, accessed 15 May 2013.
[144] Government public information campaigns to raise awareness of cyber security issues, including 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.
[145] Cabinet Office, UK Cyber Security Strategy.
[146] Antony Savvas, 'IT Students Aim for the Security Services', ComputerWorld UK, 17 May 2012.

to be an agent of state and commercial security and what their responsibilities might be.[147] 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.[148]

## 6.5 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, 'qualified security staff' being adjudged almost twice as important as 'hardware solutions'.[149] This underscores both the sociotechnical 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 IT networks. These people are not merely 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 whilst preparing personnel

[147] On 'homeland security education' in the US, in which a 'cyber' component is not uncommon, see Daniel Silander, Craig McLean and Don Wallace, 'The Challenges of Information and Communication Technologies for Transnational Efforts at Homeland Security Education', Journal of Applied Security Research 8, no. 1 (2013): 80-97.
[148] David Chandler, 'Resilience and the Autotelic Subject: Toward a Critique of the Societalization of Security', International Political Sociology 7, no. 2 (2013): 210-226.
[149] Frost and Sullivan, Global Information Security, 10.

for future eventualities, catastrophic or otherwise. They serve important institutional functions in training professionals to respond efficiently and effectively whilst 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 such 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 commonplace and to common sense. The media have become an integral part of this process, invited to attend demonstrations of the physical effects of cyber attacks and acting as the principle conduit through which exercises like Cyber ShockWave are communicated widely. Although these operations are also simulations, they engage the public through televisual media that deliberately blur the boundaries between the real and the imagined, so that they are presented not only as 'believable' but also even, 'likely'. Under such conditions, cyber security may be more readily identified as the 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, this is 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. Although we might make a similar argument of existing cyber security personnel in that they too will act in the future, 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.

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. As Walter Benjamin observes of education:

> who 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?[150]

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, we attempt to 'master' our relations with children, rather than the children

[150] Walter Benjamin, 'One-Way Street', One-Way Street and Other Writings (London: NLB, 1979), 104. The term 'generation' is also problematic politically; see, Jonathan White, 'Thinking Generations', British Journal of Sociology 64, no. 2 (2013): 216-247.

themselves. The Guardian traced the line from the present to the future in reporting on James Millican, a first-year university student crowned the UK'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.[151]

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 stating: 'We cannot afford to wait until further generations of graduates are trained and ready to take up employment'.[152] For this reason, we seek to recruit from our own generations but only as a stopgap while the young are trained and developed.

In conclusion, in common with all fields of security, cyber security enacts 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 has suggested 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 through recruitment and education. Although we cannot tell what events and insecurities will emerge, these modes of inhabiting and populating

[151] Nick Hopkins, 'Militarisation of Cyberspace: Why the West Fears the Threat from China's "Cyber Jedis"', The Guardian, 17 April 2012.
[152] OCSIA, 'Cyber Security', 33.

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 we can exert some limited agency, if only through devolving responsibility to a future generation we cannot control but whose potentialities we can attempt to constrain through practices that accord with our own imagination as to what the future holds and requires.

# 7 CYBER SECURITY AND THE POLITICS OF TIME

It had never had a past, nor could it ever have a future.

But it was full of happenings.[1]

## 7.1 Introduction: Logics and Chronopolitics

Chapter Two 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, as encountered in the posited community of cyber security practice. Chronotypes are the 'models or patterns' expressed by such communities 'through which time assumes practical or conceptual significance'.[2] Previous chapters have dealt with the diverse chronotypes of cyber security, the ways in which past, present, future and other aspects of temporality such as speed, acceleration and history are imagined 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, a sociotemporality that, as our framework of emergent temporality suggests, emerges in human cognition and includes the temporalities of nonhumans, of matter, energy and information. As narrative strands, however, these are principally stories that cyber security communities tell about themselves and their worlds. Although the discussion of each has explored the political implications of each chronotypical imagining, one more analytical step is necessary to look in greater detail at the chronopolitical logics of cyber security.

[1] Mervyn Peake, Titus Alone (London: Vintage Books, 2011/1959), LXVI.
[2] John Bender and David E. Wellbery, 'Introduction', in Chronotypes: The Construction of Time, eds. John Bender and David E. Wellbery (Stanford, CA: Stanford University Press, 1991), 4

For Richard Grusin, the concept of 'logics' does not imply 'universal or a priori principles that govern practice', or which are 'unchallengeable and unchangeable'.[3] Logics refer instead to 'tendencies that emerge from and within particular historical practices and assemblages', and from which 'competing or contradictory logics or illogics' can also be recovered.[4] Ben Anderson is more explicit still about the temporality of logics, each of which is 'a programmatic way of formalizing, justifying and deploying action in the here and now' and which 'involve action that aims to prevent, mitigate, adapt to, prepare for or pre-empt specific futures'.[5] These sets of (il)logics are organising principles through which cyber security assemblages coalesce and persist and that together shape the chronopolitics of cyber security. That is, they are proposed and presented as the principal modes in which time and temporality are expressed in and through cyber security, through which the politics of cyber security are informed and influenced and the practices of cyber security enabled. 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 the chronopolitical manifold or assemblage of cyber security. The chapter concludes with a discussion of the importance of recognising the heterogeneous nature of the chronopolitics of security.

[3] Richard Grusin, Premediation: Affect and Mediality After 9/11 (Basingstoke: Palgrave Macmillan, 2010), 5.
[4] Ibid.
[5] Ben Anderson, 'Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies', Progress in Human Geography 34, no. 6 (2010): 779.

## 7.2 The Logic of Assemblage

Cyber security is an 'assemblage', a dynamic web of human and nonhuman entities, in which 'the elements put together are not fixed in shape, do not belong to a larger pre-given list but are constructed in part as they are entangled together'.[6] Temporal tendencies emerge from the logic of assemblage itself, which 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'—or, in Spenser, 'assemblaunce'—whose active inflections better represent the nature of the object it described. 'Assemblage' was reintroduced into English from French social theory in the late 20th century, as a ready translation of agencement but, again, many of the active connotations of the root verb, agencer, 'to arrange, to fit up, to combine, to order', were not carried across.[7]

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'.[8] 'Assemblage' is more than its standard usage in English implies and its 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

[6] John Law, After Method: Mess in Social Science Research (London: Routledge, 2004), 42.
[7] Ibid., 41. Also, John Phillips, 'Agencement/Assemblage', Theory, Culture & Society 23, nos. 2-3 (2006): 108-109.
[8] Gilles Deleuze and Félix Guattari, Capitalism and Schizophrenia, vol. 2, A Thousand Plateaus (London: Continuum, 2004/1980), 99.

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, for example, is to reflect upon the caricatures of his original—admittedly often gnomic—philosophy of flux. As Plato reported Heraclitus, 'you cannot step into the same river twice'.[9] 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 proposed a deeper truth: that change and permanence co-exist—you and the river are both different and the same at each temporal remove.[10] No object retains all its characteristics and properties from one moment to the next but many of its aspects persist across time, including—as vexed the ancient philosophers greatly—human identity.

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 continued violence of thermonuclear fusion.[11] For Heraclitus, writes Nicholas Rescher, 'reality is at bottom not a constellation of

[9] Francesco Ademollo, The Cratylus of Plato: A Commentary (Cambridge: Cambridge University Press, 2011), 203.

[10] Hegel, with whom this dialectic approach is closely identified in modern thought, praised this unity of apparent contradiction: 'With Heraclitus, we see land; there is no proposition of Heraclitus which I have not adopted in my Logic'; Georg Wilhelm Friedrich Hegel, Lectures on the History of Philosophy, vol. 1 (London: Kegan Paul, Trench, Trübner & Co., 1892), 279, originally quoted in Justus Hartnack, An Introduction to Hegel's Logic (Indianapolis, IN: Hackett Publishing Company, 1988), 17.

[11] This perspective informs the 'Red Queen' hypothesis of evolutionary biology, which stresses constant adaptation as a means of species survival. Its name derives from the Red Queen's comment to Alice: 'Now, here, you see, it takes all the running you can do, to keep in the same place'; Lewis Carroll, Through the Looking-Glass and What Alice Found There (London: Bloomsbury, 2001/1871), 42-43.

things at all but one of processes'.[12] 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'.[13] 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'.[14] An assemblage exists in a temporality expectant of change and contingent upon change, which serves to maintain and to modify its character.

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. As Latour points out, 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.[15] 'Power' is only effective anyway through endless 'complicities, connivances, compromises and mixtures', none of which is explained by power itself.[16] For Latour, the logic of assemblage—or, in his formulation, the 'actor-network'—is how it extends its scale through the addition of more actors—human and

[12] Nicholas Rescher, Process Metaphysics: An Introduction to Process Philosophy (Albany, NY: State University of New York Press, 1996), 10, original emphasis.
[13] Manuel DeLanda, A New Philosophy of Society: Assemblage Theory and Social Complexity (London: Continuum, 2006), 12.
[14] Jane Bennett, Vibrant Matter: A Political Ecology of Things (Durham, NC: Duke University Press, 2010), 23-24.
[15] Bruno Latour, 'Drawing Things Together', in Representation in Scientific Practice, eds. Michael Lynch and Steve Woolgar (Cambridge, MA: MIT Press, 1990), 56.
[16] Bruno Latour, The Pasteurization of France (Cambridge, MA: Harvard University Press, 1988), 175.

nonhuman—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 more information infrastructure is created, 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. Although cyber security may lay claim to this global environment of 'cyberspace' as its field of responsibility, 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'.[17] Cyber security actors cannot rest whilst 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'.[18] 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 render threats emanating from anywhere in the world as national security issues due to their possible effects on domestic assets or populations. 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 but there are multiple methods through which this is

[17] Vivienne Jabri, 'War, Security and the Liberal State', Security Dialogue 37, no. 1 (2006): 57.
[18] Ibid., 59.

attempted.[19] 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 Six, which are responses to the problems of increasing cyber insecurity caused both by the changing information-technological landscape and the activities facilitated by it—war, crime, terrorism, espionage. In sociological terms, people are 'recruited', 'mobilized' and 'enrolled' into the cyber security assemblage.[20]

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'.[21] 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

[19] For a critique of 'cyber' as 'domain', see Tim Stevens, 'Information Warfare: A Response to Taddeo', Philosophy & Technology 26, no. 2 (2013): 223.
[20] Bruno Latour, Reassembling the Social: An Introduction to Actor-Network Theory (Oxford: Oxford University Press, 2005), 218; Michel Callon, '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, 1986), 196-233.
[21] DeLanda, New Philosophy, 22.

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 not to do so is to allow one's motives to be called into question. 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'.[22] 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 unproductiveness 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. Whilst 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.[23] The standardization 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 suggests, that the discipline of human affairs 'can proceed only via the manipulation of time and of space'.[24] The logic of the assemblage and the logic of capital coincide in their reproductive aspects, especially as cyber security is promoted

[22] Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge, 2008), 137.
[23] Henry J. Rutz, 'Introduction: The Idea of a Politics of Time', in The Politics of Time, ed. Henry J. Rutz (Arlington, VA: American Anthropological Association, 1992), 7.
[24] Anthony Giddens, The Constitution of Society: Outline of a Theory of Structuration (Berkeley, CA: University of California Press, 1984), 145.

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 establish a pipeline of talented people to help Britain succeed in the global race'.[25] 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.[26] 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', through which the future will be shaped.[27] 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.[28] 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.

## 7.3 The Logic of Real Time

Cyber security actors make several claims about the temporality of the contemporary world. They stress the uniqueness of the present time in world-historical terms: it marks the early

[25] Cabinet Minister Chloe Smith, video, https://cybersecuritychallenge.org.uk/education.php, accessed 7 June 2013.
[26] Marc Prensky, 'Digital Natives, Digital Immigrants Part 1', On the Horizon 9. no. 5 (2001): 1, 3-6. This highly-influential caricature is robustly challenged on empirical grounds by Sue Bennett, Karl Maton and Lisa Kervin, 'The "Digital Natives" Debate: A Critical Review of the Evidence', British Journal of Educational Technology 39, no. 5 (2008): 775-786.
[27] Michael Chertoff, 'The Cybersecurity Challenge', Regulation & Governance 2, no. 4 (2008): 482.
[28] Vera King, 'The Generational Rivalry for Time', Time & Society 19, no. 1 (2010): 54-71.

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 18th and 19th centuries. Cyber security identifies speed as the ontology of revolutionary postmodernity, a source of socioeconomic opportunity and political advantage—and hence the object of desire—and as a globalised vector of risk and threat, to be feared and countered. These opportunities and problems are intensified further by the acceleration of the rate of technological change, which causes 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. As the near-future comes to dictate all political actions, 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 the unregulable, an 'extended present' in which the future beyond the now is increasingly unimaginable and unrealisable.[29] 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'.[30] Neither the technical practices of cyber security nor the politics that govern it are yet so in thrall to speed and acceleration that there remains no space for the exercise of ethical judgement and democratic politics,

[29] Helga Nowotny, Time: The Modern and Postmodern Experience (Cambridge: Polity Press, 1994).
[30] Paul Virilio, Polar Inertia (London: Sage, 2000/1990), 76.

understood not necessarily as Western liberal democracy but as a political system 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, suggest that the logic of real time can be detected in the ongoing political development of cyber security.

The logic of real time is not something that necessarily reflects empirical reality but is 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 to the recruitment and education activities discussed above, which are still at an early stage of becoming institutionalised, the temporalities of machines are not only appropriated by cyber security but 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. Although there is great variation in the deterministic arguments deployed within the broad field of International Relations, they all, as Daniel McCarthy observes, resolve to a fundamental argument that posits that ‘technology develops according to a single linear

rationale which causes outcomes of social development'.[31] 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 and, importantly, the promotion of a worldview that subscribes to this interpretation of history forecloses, as already suggested, the possibilities of democratic politics. Although cyber security discourses often stress the variety and heterogeneity of 'cyberspace' or 'the Internet', 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.[32] The canonical example of this genre is often held—by advocates and critics alike—to be historian E.P. Thompson's 1967 article, 'Time, Work-Discipline and Industrial Capitalism', describing the replacement in the 18th 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.[33] In 1884, the International Meridian Conference formalised Greenwich as the prime meridian and divided the globe into 24 time zones, effectively institutionalising the first unified public global time.[34] Almost exactly

[31] Daniel McCarthy, 'Technology and "the International" or: How I Learned to Stop Worrying and Love Determinism', Millennium: Journal of International Studies 41, no. 3 (2013): 470-490.
[32] Andrew R. Hom, 'Hegemonic Metronome: The Ascendancy of Western Standard Time', Review of International Studies 36, no. 4 (2010): 1145-1170.
[33] E.P. Thompson, 'Time, Work-Discipline and Industrial Capitalism', Past & Present 38 (1967): 56-97.
[34] Allen W. Palmer, 'Negotiation and Resistance in Global Networks: The 1884 International Meridian Conference', Mass Communication & Society 5, no. 1 (2002): 7-24.

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).[35] In these developments, we may see the emergence of technological time as the global chronos, the always-synchronised time of life and societies and of world history.

Real time is the apotheosis of this 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'.[36] 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. There are premonitions of cyber security in the characterisation of real time as 'a temporality so focused on the intensity or presence of the instant that it elides the richness of lived temporality, with its retentions of past sensations and its purposeful yet uncertain anticipations of future possibility'.[37]

These narratives see 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'.[38] 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, an horizon beyond which other temporalities are obscured, if not totally ignored.

---

[35] David L. Mills, Computer Network Time Synchronization: The Network Time Protocol (Boca Raton, FL: CRC Press, 2006).
[36] Paul Virilio, Open Sky (London: Verso, 1997/1995), 69.
[37] Ian James, Paul Virilio (London: Routledge, 2007), 61.
[38] Paul Glennie and Nigel Thrift, Shaping the Day: A History of Timekeeping in England and Wales 1300-1800 (Oxford: Oxford University Press, 2009), 50.

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'.[39] 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.[40] Ulrich Beck and Daniel Levy argue 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.[41] 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'.[42] This perspective refuses totalising narratives of the temporal present propounded by mainstream political actors and critical voices alike.

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 such narratives are beholden to a peculiar paradox. Why would anyone promote a perspective on the world that diminishes the possibilities of politics whilst also pursuing

[39] Ibid., 66.
[40] Susan Leong, Teodor Mitew, Marta Celletti and Erika Pearson, 'The Question Concerning (Internet) Time', New Media & Society 11, no. 8 (2009): 1267-1285; also, Heejin Lee and Jonathan Liebenau, 'Time and the Internet at the Turn of Millennium', Time & Society 9, no. 1 (2000): 43-56.
[41] Ulrich Beck and Daniel Levy, 'Cosmopolitanized Nations: Re-Imagining Collectivity in World Risk Society', Theory, Culture & Society 30, no. 2 (2013): 9.
[42] Kimberly Hutchings, Time and World Politics: Thinking the Present (Manchester: Manchester University Press, 2008), 176.

politics to regulate that world? The answer lies in the fallacy of real time itself. As Robert Hassan points out, 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:

> Real time [is] the final goal of machine/human interaction, the very end of the temporal continuum that would stretch from 'no time' to the speed of light. To be able to achieve true real-time response would mean the ultimate surrender of human agency to digital technology, where latencies have been driven out and where lags no longer occur. This would constitute the militarist dream of the achievement of absolute power through absolute speed and the capitalist Nirvana where production and circulation function 'at the speed of thought'. Both dreams are destined, however, to be unrealizable because imperfect humans constantly get in the way of perfect systems.[43]

To exist as a 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. It is also to return metaphysics to the technological, as Heidegger reminds us we must.[44] 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.[45] 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

[43] Robert Hassan, 'Network Time', in 24/7: Time and Temporality in the Network Society, eds. Robert Hassan and Ronald E. Purser (Stanford, CA: Stanford Business Books, 2007), 51.
[44] Martin Heidegger, 'The Question Concerning Technology', in The Question Concerning Technology and Other Essays (New York: Harper, 1977), 3-35.
[45] William E. Connolly, 'Speed, Concentric Cultures, and Cosmopolitanism', Political Theory 28, no. 5 (2000): 596-618; David McIvor, 'The Politics of Speed: Connolly, Wolin, and the Prospects for Democratic Citizenship in an Accelerated Polity', Polity 43, no. 1 (2011): 58-83; Simon Glezos, The Politics of Speed: Capitalism, the State and War in an Accelerating World (London: Routledge, 2012).

will still be a human monopoly'.[46] 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.[47]

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.[48] This logic emerges from narratives contingent upon highly deterministic interpretations of reality and temporality consisting 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.

[46] Christopher Coker, Warrior Geeks: How 21st Century Technology is Changing the Way We Fight and Think About War (London: Hurst & Company, 2013), 149, emphasis added. Also, Kevin Cunningham and Robert R. Tomes, 'Space-Time Orientations and Contemporary Political-Military Thought', Armed Forces & Society 31, no. 1 (2004): 119-140.
[47] Doreen Massey, 'Politics and Space/Time', New Left Review 196 (1992): 65-84.
[48] See, for example, the political problems raised by the 'real-time' television news cycle; Nik Gowing, 'Skyful of Lies' and Black Swans: The New Tyranny of Shifting Information Power in Crises (Oxford: Reuters Institute for the Study of Journalism, 2009).

## 7.4 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'.[49] Many cyber security actors would seem to have adopted this as a mantra guiding their pronouncements and practices if we are to judge by their discursive reliance upon dystopian narratives of future cyber insecurity and its existential implications. 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.[50] 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 preceding chapters that these events, historical or speculative, and the narratives in which they are embedded, require mediation through news organisations and other platforms and institutions in order to reach and potentially persuade their audiences,

[49] John Cooper, The Queen's Agent: Frances Walsingham at the Court of Elizabeth I (London: Faber and Faber, 2011), 53.
[50] Marc R. Beissinger, Nationalist Mobilization and the Collapse of the Soviet State (Cambridge: Cambridge University Press, 2002).

and to anchor cyber security in a more stable and coherent past.[51] This much is established but the topic of present interest is why else is this considered necessary and politically expedient: what logics peculiar to the event operate in the chronopolitics of cyber security? In Virilio's real time, 'there is an expectation that the event will be calculated in advance, so that it can be packaged and sold to the viewer according to the commercial structures which underpin the whole business of news coverage …. [If] the event does not unfold as calculated, the entire time of transmission is wasted'.[52] I would argue that it is not wasted at all but to demonstrate this requires that we move away from understanding the event purely in and of itself—as a commodity to exchange or as a discrete temporal moment—but regard it also as an aesthetic form.

Reinhart Koselleck suggests that the 'prospect of the future, raising hopes and anxieties, making one precautionary or planful, is certainly reflected within consciousness'; in this respect, he argues, 'even expectation can be experienced'.[53] This experience of expectation is politicized through Aradau and van Munster's 'sensorium of anticipation', in which all the senses are enlisted to create an aesthetic of the future that facilitates security politics in the present.[54] As Kevin McSorley notes, scholars have argued that visual culture—which we might propose is a principal form of mediation in cyber security—should be analysed not only for the ideologies and politics it represents or communicates but also in terms of its 'affective logics'.[55] Carter and McCormack suggest that images do not necessarily transmit messages per se but contribute to political cultures in ways 'excessive' of 'representational and discursive logics …. as blocs of affective intensity with differential speeds, durations and capacities to affect other

[51] The practices discussed in Chapter 6 may actually be 'essential if we are to learn from the past and make sense of the present'; Jenny KItzinger, 'Media Templates: Patterns of Association and the (Re)construction of Meaning Over Time', Media, Culture & Society 22, no. 1 (2000): 78.
[52] James, Paul Virilio, 62.
[53] Reinhart Koselleck, Futures Past: On the Semantics of Historical Time (New York: Columbia University Press, 2004/1979), 261.
[54] Claudia Aradau and Rens van Munster, Politics of Catastrophe: Genealogies of the Unknown (London: Routledge, 2011), 85-86.
[55] Kevin McSorley, 'Helmetcams, Militarized Sensation and "Somatic War"', Journal of War & Culture Studies 5, no. 1 (2012): 55.

kinds of bodies'.[56] Although mediated cyber security narratives do convey specific messages, they also help to foster an affective aesthetic of the future cyber security event, through which to further political ends.

To illustrate this, consider the example of 'cyber war', understood provisionally as a societal conflict conducted through information technologies, in which public and private infrastructures and attendant functionalities are degraded by adversarial 'cyber attacks'. As described in Chapter Four, this form of conflict is a staple of the cyber security imaginary, whether or not it constitutes part of a broader strategic-level war or not. Numerous authors observe that in postmodernity the boundaries between actual and metaphorical 'war' are blurred. Christopher Coker argues that contemporary writers have difficulty in comprehending and representing the nature of war, so that our 'accounts of war today tend to be graphically visual, not textual'.[57] The 'image rather than the word renders war into an experience that can be shared' and it is 'the extremities of human experience that make war so vivid' for an observer.[58] Narratives of war—real or imagined—need to engage audiences through emotional stimulation and 'cyber war' is fought principally on such abstracted informational terrain that it can only become meaningful, in Coker's terms, first, through the 'materialisation' of the virtual and, second, through war's affective embodiment. 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.

[56] Sean Carter and Derek P. McCormack, 'Affectivity and Geopolitical Images', in Observant States: Geopolitics and Visual Culture, eds. Fraser McDonald, Rachel Hughes and Klaus Dodds (London: IB Tauris, 2010), 118, quoted in ibid.
[57] Coker, Warrior Geeks, 110.
[58] Ibid., 109, 110.

Whether it invokes clichés of planes tumbling from the sky and chemical plants exploding, or requires more immediate demonstrations of industrial plant malfunctioning to the point of destruction, or mock cities in defence contractors' office blocks, material effects express the 'virtual' threat and the familiar and mundane are transformed into objects of extraordinary subversion and sabotage. Although not exclusively visual, these events are at the very least made 'vivid' through this translation and 'bring home' to viewers and readers 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.[59] Although information infrastructures in toto are transnational and global, they are also local and predominantly urban, and their targeting in cyber war is similar to the urbicidal logics of other forms of war and may elicit similarly emotive responses to the destruction of assets with social and cultural value.[60]

The second dynamic is closely related but asks audiences and observers to become active participants in countering potential infrastructural degradation under conditions of 'cyber war'. As McSorley, Coker and others point out, even with the increased 'technicization' of war through the widespread adoption of information technologies and 'remote' methods of killing, war is not becoming as disembodied as many critics maintain. Soldiers controlling drones from outposts in the American Southwest are not wholly detached from their targets in Afghanistan or Yemen but are 'embodied in the network' of modern war.[61] McSorley theorises the emergence of 'somatic war' that 'foregrounds sensory immersion and real feeling, vital living

[59] Martin Coward, Urbicide: The Politics of Urban Destruction (Abingdon: Routledge, 2009). Also, Robert Bevan, The Destruction of Memory: Architecture at War (London: Reaktion Books, 2006).
[60] J. Peter Burgess, 'Social Values and Material Threat: The European Programme for Critical Infrastructure Protection', International Journal of Critical Infrastructures 3, nos. 3-4 (2007): 471-487.
[61] Coker, Warrior Geeks, 98.

and bodily vulnerability'.[62] In similar language, Coker notes that even in the case of a 'virtual' technology like a flight simulator, it does not merely 'replicate' reality but 'sucks you in; it immerses you'.[63] This technology does not seek to represent reality but to create it or at least 'to propose itself as proxy for the real'.[64]

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. 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. Coker notes that the US military's 'Warrior Ethos' document of 2005 reminded even ancillary staff that 'to find oneself under fire required that everyone should subscribe to the principles of the warrior ethos'.[65] 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. Although 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.[66] Perhaps, if the 're-enchantment' of war relies on 'putting us back in touch

[62] McSorley, 'Helmetcams'.
[63] Christopher Coker, The Future of War: The Re-Enchantment of War in the Twenty-First Century (Malden, MA: Blackwell Publishing, 2004), 72; also, Coker, Warrior Geeks, 129-131.
[64] Sherry Turkle, Simulation and Its Discontents (Cambridge, MA: MIT Press, 2009), 80.
[65] Coker, Warrior Geeks, 117.
[66] Alexander Klimburg, 'The Whole of Nation in Cyberpower', Georgetown Journal of International Affairs 11 (2010): 171-179; Alexander Klimburg, 'Mobilising Cyber Power', Survival 53, no. 1 (2011): 41-60.

with our humanity',[67] 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:

> Premediation is not about getting the future right, but about proliferating multiple remediations of the future both to maintain a low level of fear in the present and to prevent an occurrence of the kind of tremendous media shock that the United States and much of the networked world experienced on 9/11.[68]

Catastrophic futures are rehearsed before they irrupt into the present and help to inure publics to the shocks of future events, an outcome which can be read as increasing resilience to the future event.[69] If the 'unexpected has the power of surprise, and this surprise involves new experience',[70] 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'.[71] These processes are assisted further by 'remediating' past events—like Pearl Harbor and 9/11—and repurposing them 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, premediation of the future creates 'societal fragilities and resentment' by limiting the number of possible futures: 'the imagination of some scenarios

---

[67] Coker, Future of War, 44.
[68] Grusin, Premediation, 4.
[69] Also, Claudia Aradau and Rens van Munster, Politics of Catastrophe: Genealogies of the Unknown (London: Routledge, 2011), 46.
[70] Koselleck, Futures Past, 262.
[71] Grusin, Premediation, 46.

over others, the visualization of some futures and not others, entails profoundly political work that enables and constrains political decisionmaking in the present'.[72]

Cyber security, in its resilience mode, 'intervenes in these affective relations to construct an order of fear that re-orients life in relation to a potentially catastrophic future'.[73] In this respect, the evental logic of cyber security is again shown to be consistent with postmodernity but we should 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'.[74] This is probably correct but he also suggested the exercise might have 'some small effect on modulating individual and collective affect' and was, more importantly, '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'.[75] This is certainly the case and there are few 'news days' without a cyber security story of some description. 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'.[76] The efficacy of premediation attempts may be

[72] Marieke De Goede, 'Beyond Risk: Premediation and the Post-9/11 Security Imagination', Security Dialogue 39, nos. 2-3 (2008): 171.
[73] Kevin Grove, 'On Resilience Politics: From Transformation to Subversion', Resilience: International Policies, Practices and Discourses 1, no. 2 (2013): 146-153.
[74] Richard Grusin, 'Cyber Shock Wave—Fearmongering on CNN', Premediation, 25 February 2010.
[75] Ibid.
[76] Grusin, Premediation, 47.

disputed but their chronopolitical logic is apparent and invests in the interpretation of past and future events the ability to shape political behaviours in the present.

## 7.5 The Logic of Eschaton

At several points in this enquiry, most notably in Chapters Three and Four, 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 contingent on 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' 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 'new media ecology' of global postmodernity.[77]

[77] Andrew Hoskins and Ben O'Loughlin, War and Media: The Emergence of Diffused War (Cambridge: Polity, 2010).

Although 'the end' may never arrive, these narratives disclose a deep concern with finitude, in which apocalypse is but one 'species of the genus eschatology'.[78] As Bernard McGinn explains, apocalypticism is 'a particular kind of belief about the last things—the End of history and what lies beyond it', whereas eschatology 'sees history as a teleological process and believes that Scripture reveals truth about its End'.[79] Although this may seem a trivial distinction, it is the difference between 'viewing the events of one's own time in the light of the End of history [eschatology] and seeing them as the last events themselves [apocalypticism]'.[80] 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 political logics of eschatology as expressed in political theology. As Paul Fletcher argues, liberal modernity has distanced itself from the metaphysics of theology but its political authority derives from its theological heritage: 'If the underlying authority of political governance is theological it is not because of the manner in which scripture or dogma is espoused or reconfigured—the opposite is largely true of the liberal tradition—but because of the ways in which the mundane political order is dependent on a (now recurrently unavowed) transcendent order of things'.[81]

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 to the politics of security in general an eschatological ontology—'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).[82] Yet, as we have identified in apocalyptic cyber security narratives, the end is not the End but also a beginning—'the natality' and the 'advent of the

[78] Bernard McGinn, Visions of the End: Apocalyptic Traditions in the Middle Ages (New York: Columbia University Press, 1998/1979), 3.
[79] Ibid., 3-4.
[80] Ibid., 4.
[81] Paul Fletcher, 'The Political Theology of the Empire to Come', Cambridge Review of International Affairs 17, no. 1 (2004): 54.
[82] Michael Dillon, Politics of Security: Towards a Political Philosophy of Continental Thought (London: Routledge, 1996), 31.

political'.[83] However, there is still more temporal texture than this simple picture suggests. As both Fletcher and Dillon recognise, there is a gap between the historical present and the end of history (eschaton) that must be accounted for, as it has a distinctly chronopolitical character that helps to explain, for example, why the cyber apocalypse never arrives and what 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. 'In the present quest for infinite justice there can be no goal, no realizable telos and, if the terror (rather than any geopolitically specific antagonist) is the object of this endless war, there is no longer an enemy as such'.[84] The war on terror becomes 'a security project that finds its condition of possibility in omni-malevolence'.[85] In the absence of telos there remains only a 'zone of anomic indistinction' between present and future, a state of exception in which due legal process is suspended and all manner of 'emergency powers' can be enacted.[86] This would include the practices of executive centralisation discussed in Chapter Three, which were identified with the nascent yet unconsummated logic of real time. Again, Dillon expands upon this formulation through his identification of this 'zone' with the katechon, which in Christian eschatology is the 'impetus to resist, restrain, or otherwise defer' the messianic eschaton.[87] Where they differ is in Fletcher's insistence on the exceptionality of this temporality; Dillon treats it 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 'zone of anomic indistinction', 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

[83] Ibid.
[84] Fletcher, 'Political Theology', 56.
[85] Ibid., 57.
[86] Ibid., 59.
[87] Michael Dillon, 'Specters of Biopolitics: Finitude, Eschaton, and Katechon', The South Atlantic Quarterly 110, no. 3 (2011): 780-792.

apocalyptic transformation.[88] 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'.[89] Therefore, as Dillon notes, eschaton and katechon 'appear to be in continuous war with one another', particularly as maintenance of the katechon becomes its own form of 'messianic mission'.[90]

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 are contingent 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'.[91] Although the apocalypse is frequently portrayed as something desirable and necessary for political transformation in the name of cyber security, the apocalypse is not equal to the eschaton, which, as Dillon describes it, would be the 'catastrophic threat of the dissolution of the order of things'.[92] 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.

[88] Steven Ostovich, 'Carl Schmitt, Political Theology, and Eschatology', KronoScope 7, no. 1 (2007): 49-66.
[89] McGinn, Visions of the End, 30.
[90] Dillon, 'Specters', 784.
[91] David Barnard-Wills and Debi Ashenden, 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', Space & Culture 15, no. 2 (2012): 118.
[92] Dillon, 'Specters', 782.

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 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'.[93] 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'. [94] 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'.[95] 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.[96] As in other areas of life, those who incubate an apocalyptic aesthetic are usually the same as those who promise salvation,[97] and 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'.[98] The constant deferral of the end creates a gap in which the cyber

[93] Ibid., 789.
[94] Ibid., 783.
[95] Jonathan Marcus, 'Are We Really Facing Cyberwar?', BBC News, 5 March 2013.
[96] Barnard-Wills and Ashenden, 'Securing Virtual Space', 118.
[97] Erik Swyngedouw, 'Apocalypse Now! Fear and Doomsday Pleasures', Capitalism Nature Socialism 24, no. 1 (2013): 9-18.
[98] Ronald J. Deibert, 'The Growing Dark Side of Cyberspace (… And What To Do About It)', Penn State Journal of Law & International Affairs 1, no. 2 (2012): 270-271.

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'.[99] There seems little room in this schema for hope or optimism, both of which founder on the rocks of 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 at bay 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 exercised in pursuit of a better life on earth in the present.[100] '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.[101] Endeavours like eugenics, cryonics and even space exploration share the belief that science and technology can improve the future of the human species.[102] The posthumanist movement, in its concerns with a fast-approaching 'technological singularity'—

[99] Carl Schmitt, The Concept of the Political (Chicago: Chicago University Press, 1996/1932), 61, quoted in Ostovich, 'Carl Schmitt', 63.
[100] Jürgen Moltmann, Theology of Hope: On the Ground and the Implications of a Christian Eschatology (Minneapolis, MN: Fortress Press, 1993/1965).
[101] Catherine Wessinger, 'Millennialism With and Without the Mayhem', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements, eds. Thomas Robbins and Susan J. Palmer (New York: Routledge, 1997), 47-59.
[102] John M. Bozeman, 'Technological Millennialism in the United States', in Robbins and Palmer, Millennium, 139-158.

mischievously dubbed the 'Rapture of the Nerds'[103]—is infused with apocalypticism but emphasises the positive social benefits made possible through radical information-technological developments.[104] These are expressions of a long heritage of technoscientific thought that is secular rather than religious in its apocalypticism, although the two are closely related.[105]

Most cyber security narratives are in the catastrophic tradition but 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. These are not aspirations to be dismissed 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'.[106] 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'.[107] 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.

[103] Cory Doctorow and Charles Stross, The Rapture of the Nerds (New York: Tor Books, 2012).
[104] Michael W. DeLashmutt, 'A Better Life Through Information Technology? The Techno-Theological Eschatology of Posthuman Speculative Science', Zygon: Journal of Religion & Science 41, no. 2 (2006): 267-288.
[105] James J. Hughes, 'The Politics of Transhumanism and the Techno-Millennial Imagination, 1626-2030', Zygon: Journal of Religion and Science 47, no. 4 (2012): 757-776. For an excoriating review of contemporary technological utopianism, see David Rieff, 'The Singularity of Fools', Foreign Policy 200 (2013): 96.
[106] Antonio Gramsci, Letters from Prison (New York: Harper Row, 1973/1929), 175, quoted in Oliver Bennett, 'Cultures of Optimism', Cultural Sociology 5, no. 2 (2011): 302.
[107] Ken Booth, Theory of World Security (Cambridge: Cambridge University Press, 2007), 179.

## 7.6 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 the cyber security community 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 borne of the nature of reality itself, in which continuity and change are two sides of the same existential coin; each presupposes and is contingent upon 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 actors—and time—by appropriating their temporalities—or it will lose its identity and potency.

In this light, all other logics can be viewed as 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 'space' 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: assemblage is a way to conceptualise the world rather than an empirical theory; it is a 'philosophical wager' about reality, not a claim to reality.[108]

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'. 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' 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. As predicted by our original model of emergent sociotemporality and by the logic of assemblage, cyber security appropriates the time of machines but it is also seduced by the temporalities of nonhumans, 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, facilitating 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; the future is

[108] Patrick Thaddeus Jackson, The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics (London: Routledge, 2011), 32-40.

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 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.[109] This hiatus between now and the end is also the space opened up by the logic of real time,

[109] David J. Betz and Tim Stevens, Cyberspace and the State (London: Routledge for the IISS, 2011).

between the technologically supercharged speed of postmodernity and the cumbersome bureaucracies of modernity, in which the cyber security assemblage can be reworked and refashioned in any of 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 that inform and influence the politics of cyber security and which become embedded in practice. 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 and 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 but 'rather are squinting into the dark, telling themselves stories about what the world is like, and then acting on the basis of what they think is "out there", while competing with others who have different notions'.[110] These notions will 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 should not be treated as static or definitive, or as 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

[110] Lynn Eden, 'Learning and Forgetting: The Development of Organizational Knowledge About US Weapons Effects', paper presented at the American Political Science Association annual meeting, Chicago, 1992, quoted in Theo Farrell, 'Figuring Out Fighting Organisations: The New Organisational Analysis in Strategic Studies', Journal of Strategic Studies 19, no. 1 (1996): 130.

exercise in futurity. 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'.[111] For this reason, William Gibson, the science-fiction writer most frequently cited in discussions of cyber security, has said that when writing about the future he is just 'squinting at the present in a certain way'.[112] 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.[113] In such 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.[114]

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

[111] Frank Furedi, Culture of Fear Revisited: Risk-Taking and the Morality of Low Expectation, 4th. edn. (London: Continuum, 2006/1997), 68.
[112] David Hiltbrand, 'Squinting at the Present', The Philadelphia Inquirer, 17 February 2004, originally quoted in Coker, Warrior Geeks, xix.
[113] Furedi, Culture of Fear, 68.
[114] De Goede, 'Beyond Risk', 159.

the immediate moment'.[115] Most products of this 'neologorrhea'—like 'cyber security'—are destined to become 'painfully anachronistic clichés' rather quickly.[116] This may be so but it should not detract from the importance attributed to cyber security, whether it retains that moniker or not.[117] Cyber security is not just 'epiphenomenal, a consequence of the computer and Internet revolution', as some authors suggest.[118] It is, rather, a condition of that revolution itself, a transformation in which state, commercial and civil actors alike have 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 politicized. 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'.[119] 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.[120] 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

[115] Peter Lunenfeld, 'Theorizing in Real Time: Hyperaesthetics for the Technoculture', Afterimage 23, no. 4 (1996): 16-18.
[116] Ibid.
[117] Bennett notes that an assemblage 'not only has a distinctive history of formation but a finite life span'; Bennett, Vibrant Matter, 24.
[118] Richard J. Harknett and James A. Stever, 'The New Policy World of Cybersecurity', Public Administration Review 71, no. 3 (2011): 455.
[119] Fletcher, 'Political Theology', 59.
[120] Jennifer Mitzen, 'Ontological Security in World Politics', European Journal of International Relations 12, no. 3 (2006): 341-370; Brent J. Steele, Ontological Security In International Relations: Self-Identity and the IR State (Abingdon: Routledge, 2008).

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'.[1] In the same year, a British MP's 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.[2] Three decades later, it is inconceivable that either situation would be possible or tolerated, given enormous changes in the nature and distribution of computer networks and their relations with security and politics. It has been argued that the perceived risks and threats arising from the uses and abuses of information technologies constitute 'the central security policy concern today'.[3] 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.

As such, the rate of cyber security policy adoption, implementation and change is 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'.[4] The present enquiry is an attempt not to resist that tide, as such, but

[1] Rita Summers, 'An Overview of Computer Security', IBM Systems Journal 23, no. 4 (1984): 309-325.
[2] House of Commons Select Committee on House of Commons (Services), Computer Sub-Committee, Minutes of Evidence, 24 January 1984, HC 109-vi, 138.
[3] Myriam Dunn Cavelty and Victor Mauer, '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, eds. Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel (Aldershot: Ashgate, 2007), 152, original emphasis.
[4] Barry Buzan, People, States and Fear: The National Security Problem in International Relations (Chapel Hill, NC: University of North Carolina Press, 1983), 12.

at least 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 time and temporality are conceived and experienced by the community of cyber security practice. 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. Whilst this does not deny the existence of material reality, it does privilege human cognition of the world as a means through which the world is understood and through which knowledge of the world is generated in human communities. 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 thesis contributes to the literature on cyber security and its antecedent and related practices within IR and security studies, especially that corpus of constructivist 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.[5] The present enquiry has focused upon three aspects of the cyber security imaginary. First, that which pertains to an identifiable community of cyber security practice, 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 'elite' actors imagine their roles in the world and 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, derived from J.T. Fraser, 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.

[5] Joelien Pretorius, 'The Security Imaginary: Explaining Military Isomorphism', Security Dialogue 39, no. 1 (2008): 112.

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 gain 'practical or conceptual significance',[6] 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 have been described and examined within Chapter Three to Six. 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 as 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. It is apparent to this author that 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 such matters in International Relations.

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. They are here referred to as the logics of assemblage, real time, event and eschaton, and have potential application beyond cyber security, as they may perhaps be detected 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 such an aggregate entity to reproduce itself in time, as well as in space. Given the ontological pretensions of such a

[6] John Bender and David E. Wellbery, 'Introduction', in Chronotypes: The Construction of Time, eds. John Bender and David E. Wellbery (Stanford, CA: Stanford University Press, 1991), 4.

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 media studies work on the politics of news cycles, for instance, and the pressures of real-time connectivity and communications have 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 also 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 a 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 events—past and future—are invested with political significance by cyber security communities. With respect to future events—crises, disasters, catastrophes—it has long been recognised, as by Arnold Wolfers, that such events 'must always remain a matter of subjective evaluation and speculation'.[7] In cyber security, these future events are substantially premediated and rehearsed to mitigate uncertainty and prepare state and public entities alike for their possible occurrence. The forms of premediation, affective engagement, 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

[7] Arnold Wolfers, 'National Security as Ambiguous Symbol', Political Science Quarterly 67, no. 4 (1952): 485.

security scenarios that are often, as much of this thesis illustrates, rife with pessimism and truly dark visions of futurity.

Despite the potential contributions of the thesis to the potential 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 an historical one and I make no apologies for being selective in source material or in the orientation towards the Anglophone cyber security communities of the UK and US. However, this does raise 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 is justifiable because of the author's predilections but it does not allow us to generalise our findings beyond the Western context, although that was not an original aim of this enquiry. The thesis intended 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 and 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 thesis 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' lines, and the resistance of the US, in particular, to greater multilateralism in the global governance of the Internet reflects American insistence on policy that favours American interests above all others.[8] Accusations of American colonisation of the Internet and networked imperialism are a

[8] Ryan David Kiggins, 'Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era', International Studies Perspectives (forthcoming); also, Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', Contemporary Security Policy 33, no. 1 (2012): 148-170.

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', exploring Western politics of security through non-Western theoretical frameworks, including philosophies of history and time.[9]

An additional charge of exclusion might also be brought. The thesis 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, voters, 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 these? 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 elites and to their views and opinions. We might venture that these elites 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. This might reveal how conceptions of time differ between elites, both vertically in terms of communities but also horizontally between nations.

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.[10] Elite political conflicts tend to arise over pace and scale of implementation rather than 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

[9] See, Dipesh Chakrabarty, Provincializing Europe: Postcolonial Thought and Historical Difference (Princeton, NJ: Princeton University Press, 200), 29.
[10] Corey Robin, 'The Language of Fear: National Security in Modern Politics', in Fear: Across the Disciplines, eds. Jan Plamper and Benjamin Lazier (Pittsburgh, PA: University of Pittsburgh Press, 2012), 118-131.

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 elite and civil—for want of a better dichotomy—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 thesis.

In closing, the principal contribution of this thesis has been the development of chronopolitics 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. Friedrich Schlegel wrote that 'No time has ever been so strongly, so closely, so exclusively, and so generally bound up with the future than that of our present'.[11] That he wrote this in 1828 should remind us that, despite the urgencies thrust upon us by looming existential crises, there is always time to reflect upon courses of future action. We may be, as Schlegel supposed, at a critical moment of importance in human affairs, stood upon the cusp of 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'.[12] This intuition has guided the present enquiry and similar impulses will hopefully guide future investigations into politics and security, the need for which could not be more timely or, indeed, timeless.

[11] Friedrich Schlegel, Kritische Friedrich Schlegel Ausgabe, vol. 9, Philosophie der Geschichte (1828), 417, quoted in Koselleck, Futures Past, 242.
[12] Barbara Adam, Timewatch: The Social Analysis of Time (Cambridge: Polity Press, 1995), 6.

# REFERENCE LIST

## A. PRIMARY SOURCES

### A1. Official Documents

#### *European Union*

ENISA (2012), On National and International Cyber Security Exercises: Survey, Analysis and Recommendations (Heraklion: ENISA).

#### *United Kingdom*

Annual Report of the Chief of Inspector of Factories for the Year 1954, Cmd. 9605 (London: HMSO), November 1955.

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

Central Office of Information (1998), Our Information Age: The Government's Vision, INDY J98-2429, URN 98/677 4/98 (London: Central Office of Information).

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, Cmnd. 3760 (London: HMSO), September 1968.

Department for Education (2013), 'Consultation on Computing and Disapplication of the Current National Curriculum', 3 May, https://www.education.gov.uk/schools/teachingandlearning/curriculum/nationalcurriculum2014/a00224578/consultation, accessed 15 May 2013.

Freedom of Information Act (2000).

HM Government (2000), A New Future for Communications, Cm. 5010 (London: HMSO), December 2000.

HM Government (2009), Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, Cm. 7642 (Norwich: The Stationery Office), June 2009.

HM Government (2009), Digital Britain: Final Report, Cm. 7650 (Norwich: The Stationery Office), June 2009.

HM Government (2010), Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, Cm. 7948 (Norwich: The Stationery Office), October 2010.

HM Government (2010), Britain's Superfast Broadband Future (London: Department for Business, Innovation and Skills), December 2010.

HM Government (2013), The Coalition: Together in the National Interest (London: Cabinet Office), January 2013.

Home Office (2010), Cyber Crime Strategy, Cm. 7842 (Norwich: The Stationery Office), March 2010.

House of Commons Committee of Public Accounts (2011), Information and Communications Technology in Government: Report, Together with Formal Minutes, Oral and Written Evidence, HC 1050 (London: The Stationery Office), July 2011.

House of Commons Defence Committee (2013), Defence and Cyber-Security, vol. 1, HC 106 (London: The Stationery Office), January 2013.

House of Commons Select Committee on House of Commons (Services), Computer Sub-Committee (1984), Minutes of Evidence, 24 January 1984, HC 109-vi.

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, HL Paper 37 (London: The Stationery Office), July 2012.

Intelligence and Security Committee (2012), Annual Report 2011-2012, Cm. 8403 (Norwich: The Stationery Office), July 2012.

Ministry of Defence (2010), Global Strategic Trends: Out to 2040, 4th. edn., Development, Concepts and Doctrine Centre Strategic Trends Programme, January 2010.

National Audit Office (2013), The UK Cyber Security Strategy: Landscape Review, HC 890 (Norwich, The Stationery Office).

Public Records Act (1958), amended 1967.

***United States***

Defense Advanced Research Projects Agency (2008), 'National Cyber Range Proposers' Day Workshop', Special Notice DARPA-SN08-33, 29 April, https://www.fbo.gov/index?s=opportunity&mode=form&id=250832bfd8f71f0340ce65767397fb25&tab=core&_cview=0.

Defense Advanced Research Projects Agency (2008), 'National Cyber Range', Broad Agency Announcement DARPA-BAA-08-43, 5 May, https://www.fbo.gov/download/c33/c330660f00c9820d05c9f4c54422024b/080505_BAA_National_Cyber_Range_Final.doc.

Defense Science Board (2013), Task Force Report: Resilient Military Systems and the Advanced Cyber Threat (Washington, DC: Department of Defense, January 2013).

Department of Defense (2013), Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010, as amended through 15 April 2013, http://www.dtic.mil/doctrine/dod_dictionary/.

Federal Civil Defense Administration (1955), Cue For Survival: Operation Cue (Washington, DC: US Government Printing Office).

Hildreth, Steven A. (2001), Cyberwarfare (Washington, DC: Congressional Research Service), June 2001.

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, http://www.nhc.noaa.gov/pdf/TCR-AL122005_Katrina.pdf.

National Cyber Security Division (2006), Cyber Storm: Exercise Report (Washington, DC: Department of Homeland Security).

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), December 2010.

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, September 2010).

White House (2003), The National Strategy to Secure Cyberspace (Washington, DC: White House), February 2003.

White House (2009), Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, DC: White House), May 2009.

White House (2011), International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: White House), May 2011.

White House (2013), Improving Critical Infrastructure Cybersecurity, Executive Order 13636, 12 February 2013.

White House (2013), Critical Infrastructure Security and Resilience, Presidential Policy Directive 21, 12 February 2013.

Wilson, Clay (2005), Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (Washington, DC: Congressional Research Service, April 2005).

**A2. Speeches**

Cameron, David (2012), speech to Conservative Party Conference, Birmingham, 10 October, http://www.conservatives.com/News/Speeches/2012/10/David_Cameron_Conference_2012.aspx.

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

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

Hayden, Michael V. (2011), Aspen Security Forum, Aspen, CO, 29 July, http://www.youtube.com/watch?v=yoWkAVXmSs0.

Napolitano, Janet (2013), 'From Cyber to Immigration, Terrorism to Disasters: Securing America in the Next Administration', Wilson Center, Washington, DC, 24 January, http://www.wilsoncenter.org/event/cyber-to-immigration-terrorism-to-disasters-securing-america-the-next-administration.

Obama, Barack (2010), 'Remarks by the President on the Economy', Winston-Salem, NC, 6 December, http://www.whitehouse.gov/the-press-office/2010/12/06/remarks-president-economy-winston-salem-north-carolina.

Panetta, Leon (2012), 'Remarks by Secretary Panetta on Cybersecurity', speech to Business Executives for National Security, New York, 11 October, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Panetta, Leon (2013), 'Remarks by Secretary Panetta', speech at Georgetown University, Washington, DC, 6 February, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5189.

Smith, Chloe (2012), speech to Cyber Security Summit, London, 6 November, https://www.gov.uk/government/speeches/chloe-smith-speaks-at-cyber-security-summit.

**A3. Media**

*All news and comment disseminated through broadcast, print and online media, including blogs, magazines and press releases from industry and government.*

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.

Arquilla, John (2012), 'Panetta's Wrong About a Cyber "Pearl Harbor"', Foreign Policy, 19 November, http://www.foreignpolicy.com/articles/2012/11/19/panettas_wrong_about_a_cyber_pearl_harbor.

Badger, Emily (n.d.), 'A Tiny City Built to Be Destroyed by Cyber Terrorists, So Real Cities Know What's Coming', Co.Exist, http://www.fastcoexist.com/1681033/a-tiny-city-built-to-be-destroyed-by-cyber-terrorists-so-real-cities-know-whats-coming#1.

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

BBC (2013), 'Newsnight', 29 April.

BBC News (2011), 'Cyber-Attack Tests for Olympic Computer Systems', 10 October, http://www.bbc.co.uk/news/technology-15244808.

BBC News (2012), 'David Cameron: We Must Push in "Global Trade Race"', 12 November, http://www.bbc.co.uk/news/uk-politics-20304800.

BBC News (2012), 'US Military Train in Cyber-City to Prepare Hack Defence', 28 November, http://www.bbc.co.uk/news/technology-20525545.

BBC News (2013), 'Asteroid 2012 DA14 in Record-Breaking Earth Pass', 15 February, http://www.bbc.co.uk/news/science-environment-21442863.

BBC News (2013), 'King Richard III Burial Row Heads to High Court', 1 May, http://www.bbc.co.uk/news/uk-england-york-north-yorkshire-22371814.

BBC News (2013), 'China's Tianhe-2 Retakes Fastest Supercomputer Crown', 17 June, http://www.bbc.co.uk/news/technology-22936989.

Beidel, Eric and Stew Magnuson (2011), 'Government, Military Face Severe Shortage of Cybersecurity Experts', National Defense, August, http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx.

Berinato, Scott (2003), 'The Future of Security', CIO 17, no. 6: 71-76, available at http://www.cio.com/article/32033/2010_The_Future_of_Security.

Bharara, Preet (2012), 'Asleep at the Laptop', The New York Times, 4 June.

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.

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.

Braund, Simon (2010), 'How Ronald Reagan Learned to Start Worrying and Stop Loving the Bomb', Empire 257: 134-140.

Bruno, Greg (2008), 'Backgrounder: The Evolution of Cyber Warfare', The New York Times, 27 February, http://www.nytimes.com/cfr/world/slot1_20080227.html.

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.

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

Cant, Sue (2003), '"Cyber 9/11 Risk Warning', Sydney Morning Herald, 22 April.

CERN (2013), 'New Results Indicate That New Particle is a Higgs Boson', press release, 14 March, http://home.web.cern.ch/about/updates/2013/03/new-results-indicate-new-particle-higgs-boson.

Chapman, Siobhan (2009), 'Government Criticised for Plan to Hire "Naughty Boys"', ComputerWorld UK, 30 June, http://www.computerworlduk.com/news/security/15467/government-criticised-for-plan-to-hire-naughty-boys/.

Clayton, Mark (2012), 'Senate Cybersecurity Bill Fails, So Obama Could Take Charge', The Christian Science Monitor, 16 November.

Clayton, Mark (2012), '"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.

Cohen, Tova and Maayan Lubell (2012), 'Nations Must Talk to Halt "Cyber Terrorism"—Kaspersky', Reuters, 6 June.

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

Coughlan, Sean (2013), '£7.5m University Fund to Train Cybersecurity Experts', BBC News, 9 May, http://www.bbc.co.uk/news/education-22450544.

Daily Telegraph (2013), 'Russian Meteor Exploded with Force of 30 Hiroshima Bombs', 16 February.

Daniel, Lisa (2011), 'Panetta: Intelligence Community Needs to Predict Uprisings', American Forces Press Service, 11 February, http://www.defense.gov/news/newsarticle.aspx?id=62790.

Davis, Joshua (2007), 'Hackers Take Down the Most Wired Country in Europe', Wired 15, no. 9, http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

Defense Advanced Research Projects Agency (2012), 'National Cyber Range Rapidly Emulates Complex Networks', press release, 13 November, http://www.darpa.mil/NewsEvents/Releases/2012/11/13.aspx.

Deibert, Ronald J. and Rafal Rohozinski (2011), 'The New Cyber Military Industrial Complex', The Globe & Mail, 28 March, http://www.theglobeandmail.com/commentary/the-new-cyber-military-industrial-complex/article573990/.

Department of Education (2012), '"Harmful" ICT Curriculum Set to Be Dropped to Make Way for Rigorous Computer Science', press release, 11 January, https://www.gov.uk/government/news/harmful-ict-curriculum-set-to-be-dropped-to-make-way-for-rigorous-computer-science.

D'Ottavi, Alberto (2003), 'Firewall Pioneer: Security Needs Integration', Zone-H, 4 February, http://www.zone-h.org/news/id/2058.

Dyer, Geoff (2012), 'Panetta Warns US of "Cyber Pearl Harbor"', FT.com, 12 October, http://www.ft.com/cms/s/0/6c06b03a-1423-11e2-9ac6-00144feabdc0.html#axzz2PsqYDZXx.

Epstein, Keith (2009), 'Fearing "Cyber Katrina", Obama Candidate for Cyber Czar Urges a "FEMA for the Internet"', Bloomberg Businessweek, 18 February, http://www.businessweek.com/the_thread/techbeat/archives/2009/02/fearing_cyber_k.html.

Folger, Tim (2007), 'Newsflash: Time May Not Exist', Discover Magazine, June, http://discovermagazine.com/2007/jun/in-no-time.

Fulghum, David A. (2010), 'No Fingerprints: Culprits in the Cyberattack on Iran are Still Unknown', Aviation Week & Space Technology 172, no. 36 (4 October): 29-30.

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, http://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.

GCHQ (2012), 'UK Universities Awarded Academic Centre of Excellence Status in Cyber Security Research', press release, April, http://www.gchq.gov.uk/press/pages/cyber-security-research-centres-of-excellence.aspx.

GCHQ (2012), 'New Certification Scheme Announced for IA Professionals', press release, 24 October, http://www.gchq.gov.uk/Press/Pages/New-IA-Certification-pages.aspx.

Gertz, Bill (1998), 'Computer Hackers Could Disable Military', The Washington Times, 16 April.

Gjelten, Tom (2011), 'Stuxnet Raises "Blowback" Risk in Cyberwar', NPR.org, 2 November, http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar.

Glenny, Misha (2011), 'Virtual Warfare in Race to Avoid "Doomsday"', The Guardian, 17 May.

Goldsmith, Jack and Melissa Hathaway (2010), 'The Cybersecurity Changes We Need', Washington Post, 29 May.

Gov.uk (2010), Defence Minister Opens UK Cyber Security Test Range', 26 October, https://www.gov.uk/government/news/defence-minister-opens-uk-cyber-security-test-range.

Gray, John (2012), 'The Violent Visions of Slavoj Žižek', New York Review of Books, 12 July, http://www.nybooks.com/articles/archives/2012/jul/12/violent-visions-slavoj-zizek/.

Gray, John (2013), 'Ignore at Our Peril', The Guardian, 2 February.

Greenwald, Glenn (2013), 'Pentagon's New Massive Expansion of "Cyber-Security" Unit is About Everything Except Defense', The Guardian, 28 January, http://www.guardian.co.uk/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet.

Gross, Michael Joseph (2011), 'A Declaration of Cyber-War', Vanity Fair, April, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

Grusin, Richard (2010), 'Cyber Shock Wave—Fearmongering on CNN', Premediation, 25 February, http://premediation.blogspot.co.uk/2010/02/cyber-shock-wave-fearmongering-on-cnn.html.

Guthrie, Charles (2009), 'Dumbed-Down Defenders of Their Own Turf', The Times, 27 August.

Haring, Bruce (1995), 'Hackers Rampant in Cyberspace', USA Today 28 March.

Harris, Paul (2011), 'Living with 9/11: The Anti-Terror Chief', The Guardian, 6 September.

Healey, Jason (2012), 'Hazard, Outrage and Panetta's Cyber Speech', New Atlanticist, 23 October, http://www.acus.org/new_atlanticist/hazard-outrage-and-panettas-cyber-speech.

Hiltbrand, David (2004), 'Squinting at the Present', The Philadelphia Inquirer, 17 February.

Hoekstra, Peter and Brian Finch (2013), 'The Looming Certainty of a Cyber Pearl Harbor', Politico, 19 February, http://www.politico.com/story/2013/02/the-looming-certainty-of-a-cyber-pearl-harbor-87806.html.

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, http://www.guardian.co.uk/technology/2013/apr/28/cyber-jedi-contest-britain-empire.

InfoSecurity (2013), 'RSA 2013: As Cybersecurity Receives More Attention, DHS Becomes a Critical Player', 26 February, http://www.infosecurity-magazine.com/view/30907/rsa-2013-as-cybersecurity-receives-more-attention-dhs-becomes-a-critical-player/.

Jennings, Paul (1948), 'Report on Resistentialism', The Spectator 180, no. 6252: 491.

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.

Kane, Margaret (2002), 'US Vulnerable to Data Sneak Attack', CNet News, 13 August, http://news.cnet.com/2100-1017-949605.html.

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, http://www.guardian.co.uk/commentisfree/2013/feb/15/meaning-of-meteors.

Kleinman, Zoe (2013), 'Why Air Traffic Control Still Needs the Human Touch', BBC News, 5 February, http://www.bbc.co.uk/news/technology-21195765.

Klimburg, Alexander (2013), 'Commentary: The Internet Yalta', Center for a New American Security', 5 February, http://www.cnas.org/theinternetyalta.

Lawson, Sean (2012), 'DHS Secretary Napolitano Uses Hurricane Sandy to Hype Cyber Threat', Forbes, 1 November, http://www.forbes.com/sites/seanlawson/2012/11/01/dhs-secretary-napolitano-uses-hurricane-sandy-to-hype-cyber-threat/.

Levin, Adam (2012), 'How the SEC Almost Shut Down Wall Street' Huffington Post, 15 November, http://www.huffingtonpost.com/adam-levin/did-you-know-the-sec-almo_b_2133962.html.

Lieberman, Joseph I. and Susan Collins (2012), 'At Dawn We Sleep', The New York Times, 7 December.

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.

McConnell, Mike (2010), 'To Win the Cyber-War, Look to the Cold War', The Washington Post, 28 February.

Marcus, Jonathan (2013), 'Are We Really Facing Cyberwar?', BBC News, 5 March, http://www.bbc.co.uk/news/technology-21653361.

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, http://www.v3.co.uk/v3-uk/news/2251555/ofsted-microsoft-and-teachers-worried-dfe-computing-curriculum-not-up-to-scratch.

Meserve, Jeanne (2007), 'Mouse Click Could Plunge City Into Darkness, Experts Say', CNN.com, 26 September, http://edition.cnn.com/2007/US/09/26/power.at.risk/.

Mulrine, Anna (2011), 'CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack', The Christian Science Monitor, 9 June.

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.

National Public Radio, 'Assessing the Threat of Cyberterrorism: Interview with James Lewis', Fresh Air, 10 February 2010, http://www.npr.org/templates/story/story.php?storyId=123531188.

Nguyen, Anh (2012), 'UK Cybersecurity Professionals are "Too Old", Says Baroness Neville-Jones', ComputerWorld UK, 24 May, http://www.computerworlduk.com/news/careers/3359837/uk-cybersecurity-professionals-are-too-old-says-baroness-neville-jones/.

Office of Cyber Security and Information Assurance (2012), 'Cyber Security Skill Shortages', ITNOW 54, no. 2: 32-34.

Ostroff, Natalie and Jim Taylor (2012), 'First Boot Camp Gets Young People Into Cybersecurity', BBC Newsbeat, 7 September, http://www.bbc.co.uk/newsbeat/19515213.

Page, Lewis (2008), 'DARPA Wants Matrix-Style Virtual World for Cybergeddon', The Register, 7 May, http://www.theregister.co.uk/2008/05/07/darpa_cyber_range_rfp/.

Partridge, Chris (1997), 'How to Conquer the World … And Never Leave the Barracks', The Times, 27 August.

Pilkington, Ed (2011), 'Fear: The Old Technology that Turned Hackers Into Informers', The Guardian, 7 June.

Poole, Steven (2012), 'Invasion of the Cyber Hustlers', New Statesman, 6 December, http://www.newstatesman.com/sci-tech/internet/2012/12/jeff-jarvis-clay-shirky-jay-rosen-invasion-cyber-hustlers.

Reichhardt, Tony (2005), 'Harder Than Rocket Science', Nature 435, no. 7045: 1024-1025.

Rid, Thomas (2013), 'Cyber Fail', New Republic, 4 February, http://www.newrepublic.com/article/112314/obama-administrations-lousy-record-cyber-security.

Rieff, David (2013), 'The Singularity of Fools', Foreign Policy 200: 96.

RT (2013), 'Panetta Back at It with "Cyber Pearl Harbor" Fear Mongering', 7 February, http://rt.com/usa/panetta-cyber-pearl-harbor-611/.

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, https://www.sans.org/press/netwars-cybercity.php.

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, http://www.computerworlduk.com/news/careers/3358292/it-students-aim-for-security-services/.

Schneier, Bruce (2013), 'Our Security Models Will Never Work—No Matter What We Do', Wired, 14 March, http://www.wired.com/opinion/2013/03/security-when-the-bad-guys-have-technology-too-how-do-we-survive/.

Schwartau, Winn (1991), 'Fighting Terminal Terrorism', Computerworld, 28 January 1991, 23.

Shah, Sooraj (2013), 'Cyber Security Challenge "Is Not Only About Recruiting Talent", Claims CEO', Computing, 13 March, http://www.computing.co.uk/ctg/news/2254243/cyber-security-challenge-is-not-only-about-recruiting-talent-claims-ceo.

Sky News (2013), bulletin, 8 January.

Smith, Gerry (2011), 'Feds Turn to Hackers to Defend Nation in Cyberspace', Huffington Post, 10 August, http://www.huffingtonpost.com/2011/08/08/government-recruits-hackers-cyber-shortage_n_920795.html.

Taylor, Paul (2012), 'Former US Spy Chief Warns on Cybersecurity', Financial Times, 2 December.

Thibodeau, Patrick (2013), 'Fear of Thinking War Machines May Push US to Exascale', ComputerWorld, 20 June, http://www.computerworld.com/s/article/9240230/Fear_of_thinking_war_machines_may_push_U.S._to_exascale.

The Economist (2012), 'Hype and Fear', 8 December, 62.

The Times, 'Dreadful Accident to Mr. Huskisson', 17 September 1830.

The Times, 'Death of Mr. Huskisson', 18 September 1830.

Virilio, Paul, Gérard Courtois and Michel Guerrin, 'Le Krach Actuel Représente l'Accident Intégral par Excellence', Le Monde, 18 October 2008.

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.

Weinberger, Sharon (2008), 'Cyberwarfare: DARPA's New "Space Race"', Danger Room, 1 May 2008, http://www.wired.com/dangerroom/2008/05/the-pentagon-wa-2/.

**A4. Films**

2012 (2009), dir. Roland Emmerich (Columbia Pictures), 158 mins.

Blade Runner (1982), dir. Ridley Scott (Warner Bros.), 116 mins.

Federal Civil Defense Administration (1955), 'Operation Cue', 15 mins., available at http://archive.org/details/Operatio1955.

National Infrastructure Protection Center, National Counterintelligence Center and Federal Bureau of Investigation (1999), Solar Sunrise: Dawn of a New Threat, training video, 18 mins., available at http://www.wired.com/threatlevel/2008/09/video-solar-sun/.

The Day After (1983), dir. Nicholas Meyer (ABC Circle Films), 126 mins.

The Matrix (1999), dirs. Lana Wachowski and Andy Wachowski (Warner Bros.), 136 mins.

Threads (1984), dir. Mick Jackson (BBC), 112 mins.

**B. SECONDARY SOURCES**

**B1. Books and Monographs**

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

Abou-Bakr, Ami J. (2013), Managing Disasters through Public-Private Partnerships (Washington, DC: Georgetown University Press, 2013).

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

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

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

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

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

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

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).

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

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

Aristotle (1996), Physics, tr. Robin Waterfield (Oxford: Oxford University Press).

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

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

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: Oxford University Press).

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

Aymé, Marcel (2012) [1943], The Man Who Walked Through Walls, tr. Sophie Lewis (London: Pushkin Press).

Badiou, Alain (2005), Infinite Thought: Truth and the Return to Philosophy, eds. and trs. Oliver Feltham and Justin Clemens (London: Continuum).

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

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).

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).

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

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

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

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

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

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

Bergson, Henri (2001) [1913], Time and Free Will: An Essay on the Immediate Data of Consciousness, 3rd. edn., tr. F.L. Pogson (Mineola, NY: Dover Publications).

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

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

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

Beveridge, W.I.B. (1957) [1950], The Art of Scientific Investigation, rev. edn. (New York: W.W. Norton and Company, Inc.).

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

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

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

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

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

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

Bousquet, Antoine (2009), The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity (London: Hurst & Company).

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

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

Broad, C.D. (1938), An Examination of McTaggart's Philosophy, vol. 2, part 1 (Cambridge: Cambridge University Press).

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

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

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).

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: Cambridge University Press).

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

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

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

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

Carroll, Lewis (2001) [1871], Through the Looking-Glass and What Alice Found There (London: Bloomsbury).

Castells, Manuel (2010) [1996], The Information Age: Economy, Society, and Culture, vol. 1: The Rise of the Network Society, 2nd. edn. (Chichester: Wiley-Blackwell).

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

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

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 (Chicago, IL: University of Chicago Press).

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).

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

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).

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

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

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

Dainton, Barry (2010) [2001], Time and Space, 2nd. edn. (Durham: Acumen).

D'Amico, Robert (1989), Historicism and Knowledge (New York: Routledge).

Davis, Mike (1999), Ecology of Fear: Los Angeles and the Imagination of Disaster (New York: Vintage Books).

Dawkins, Richard (1998), Unweaving the Rainbow: Science, Delusion and the Appetite for Wonder (London: Penguin Books).

Deibert, Ronald J. (1997), Parchment, Printing, and Hypermedia: Communication in World Order Transformation (New York: Columbia University Press).

DeLanda, Manuel (2006), A New Philosophy of Society: Assemblage Theory and Social Complexity (London: Continuum).

De Leeuw, Karl and Jan Bergstra, eds. (2007), The History of Information Security: A Comprehensive Handbook (Amsterdam: Elsevier).

Deleuze, Gilles and Félix Guattari (2004) [1980], Capitalism and Schizophrenia, vol. 2, A Thousand Plateaus, tr. Brian Massumi (London: Continuum).

Dennett, Daniel C. (1984), Elbow Room: The Varieties of Free Will Worth Wanting (Oxford: Oxford University Press).

Der Derian, James (1992), Antidiplomacy: Spies, Terror, Speed and War (Oxford: Blackwell).

Der Derian, James (2009) [2001], Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network, 2nd. edn. (New York: Routledge).

Dienstag, Joshua Foa (2006), Pessimism: Philosophy, Ethic, Spirit (Princeton, NJ: Princeton University Press).

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).

Doctorow, Cory and Charles Stross (2012), The Rapture of the Nerds (New York: Tor Books).

Dover, Robert and Michael S. Goodman, eds. (2011), Learning from the Secret Past: Cases in British Intelligence History (Washington, DC: Georgetown University Press).

Dunn Cavelty, Myriam (2008), Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (London: Routledge).

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], Four Quartets (San Diego, CA: Harvest).

English, Richard (2009), Terrorism: How to Respond (Oxford: Oxford University Press, 2009).

Erikson, Kai (1994), A New Species of Trouble: The Human Experience of Modern Disasters (New York: W.W. Norton & Company).

Fabian, Johannes (2002) [1983], Time and the Other: How Anthropology Makes Its Object (New York: Columbia University Press).

Feyerabend, Paul (1993) [1975], Against Method: Outline of an Anarchistic Theory of Knowledge, 3rd. edn. (London: Verso).

Forsee, Aylesa (1963), Albert Einstein: Theoretical Physicist (New York: Macmillan).

Foucault, Michel (2002) [1966], The Order of Things: An Archaeology of the Human Sciences (London: Routledge).

Frank, Adam (2011), About Time (Oxford: Oneworld).

Fraser, J.T. (1999), Time, Conflict, and Human Values (Urbana, IL: University of Illinois Press).

Freedman, Lawrence (1981), The Evolution of Nuclear Strategy (Houndmills: Macmillan Press).

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).

Galison, Peter (2003), Einstein's Clocks, Poincaré's Maps: Empires of Time (New York: W.W. Norton & Company).

Galison, Peter and Bruce Hevly, eds. (1992), Big Science: The Growth of Large-Scale Research (Stanford, CA: Stanford University Press).

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).

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).

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: Oxford University Press).

Glezos, Simon (2012), The Politics of Speed: Capitalism, the State and War in an Accelerating World (London: Routledge).

Goldman, Alvin I. (1999), Knowledge in a Social World (Oxford: Oxford University Press).

Goodman, Michael S. (forthcoming), The Anvil of Discussion: The Official History of the Joint Intelligence Committee (Routledge).

Gould, Stephen Jay (1987), Time's Arrow, Time's Cycle: Myth and Metaphor in the Discovery of Geological Time (Cambridge, MA: Harvard University Press).

Gowing, Nik (2009), 'Skyful of Lies' and Black Swans: The New Tyranny of Shifting Information Power in Crises (Oxford: Reuters Institute for the Study of Journalism).

Graham, Stephen and Simon Marvin (2001), Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition (London: Routledge).

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).

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).

Grusin, Richard (2010), Premediation: Affect and Mediality After 9/11 (Basingstoke: Palgrave Macmillan).

Guins, Raiford (2009), Edited Clean Version: Technology and the Culture of Control (Minneapolis, MN: University of Minnesota Press).

Guthrie, W.K.C. (1978), A History of Greek Philosophy, vol. 5: The Later Plato and the Academy (Cambridge: Cambridge University Press).

Hacking, Ian (1999), The Social Construction of What? (Cambridge, MA: Harvard University Press).

Hall, Wayne M. (2003), Stray Voltage: War in the Information Age (Annapolis, MD: Naval Institute Press).

Haraway, Donna (1997), Modest Witness@Second_Millennium: Female_Man©_Meets Oncomouse™: Feminism and Technoscience (New York: Routledge).

Harris, Jose (1993), Private Lives, Public Spirit: Britain 1870-1914 (London: Penguin Books).

Hartnack, Justus (1988), An Introduction to Hegel's Logic (Indianapolis, IN: Hackett Publishing Company).

Harvey, David (1990), The Condition of Postmodernity: An Enquiry Into the Origins of Cultural Change (Cambridge, MA: Blackwell).

Hassan, Robert (2009), Empires of Speed: Time and the Acceleration of Politics and Society (Leiden: Brill).

Hassan, Robert and Ronald E. Purser, eds. (2007) 24/7: Time and Temporality in the Network Society (Stanford, CA: Stanford Business Books).

Healey, Jason, ed. (2013), A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Washington, DC: Atlantic Council).

Hegel, Georg Wilhelm Friedrich (1892), Lectures on the History of Philosophy, vol. 1 (London: Kegan Paul, Trench, Trübner & Co.).

Heidegger, Martin (1977), The Question Concerning Technology and Other Essays, tr. William Lovitt (New York: Harper).

Heidegger, Martin (1995) [1929-1930], The Fundamental Concepts of Metaphysics: World, Finitude, Solitude, tr. 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).

Heywood, Andrew (2000), Key Concepts in Politics (Basingstoke: Palgrave Macmillan).

Hitler, Adolf (1965), Reden und Proklamationen 1932-1945 (Munich: Süddeutscher Verlag).

Hobbes, Thomas (1996) [1651], Leviathan, ed. Richard Tuck, rev. edn. (Cambridge: Cambridge University Press).

Hobbes, Thomas (1998) [1642], On the Citizen, eds. Richard Tuck and Michael Silverthorne (Cambridge: Cambridge University Press).

Hobsbawm, Eric (1994) [1987], The Age of Empire, 1875-1914 (London: Abacus).

Hodder, Ian (2012), Entangled: An Archaeology of the Relationships between Humans and Things (Chichester: Wiley-Blackwell).

Hoofd, Ingrid M. (2012), Ambiguities of Activism: Alter-Globalism and the Imperatives of Speed (New York: Routledge).

Hoskins, Andrew and Ben O'Loughlin (2010), War and Media: The Emergence of Diffused War (Cambridge: Polity).

Husserl, Edmund (1964) [1928], The Phenomenology of Internal Time-Consciousness, ed. Martin Heidegger, tr. James S. Churchill (The Hague: Martinus Nijhoff).

Hutchings, Kimberly (2008), Time and World Politics: Thinking the Present (Manchester: Manchester University Press).

Huyssen, Andreas (2003), Present Pasts: Urban Palimpsests and the Politics of Memory (Stanford, CA: Stanford University Press).

Innes, Michael, ed. (2007), Denial of Sanctuary: Understanding Terrorist Safe Havens (Westport, CT: Praeger Security International).

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: Manchester University Press).

James, Ian (2007), Paul Virilio (London: Routledge).

Jeffery, Keith (2010), MI6: The History of the Secret Intelligence Service (London: Bloomsbury Publishing).

Jungk, Robert (1958) [1956], 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.

Kaldor, Mary (2006) [1999], New and Old Wars: Organized Violence in a Global Era, 2nd. edn. (Cambridge: Polity Press).

Kant, Immanuel (1998) [1781/1787], Critique of Pure Reason (Cambridge: Cambridge University Press).

Karatzogianni, Athina (2006), The Politics of Cyberconflict (Abingdon: Routledge).

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).

Khong, Yuen Foong (1992), Analogies at War: Korea, Munich, Dien Bhen Phu, and the Vietnam Decisions of 1965 (Princeton, NJ: Princeton University Press).

Kierkegaard, Søren (1980) [1844], The Concept of Anxiety, ed. and tr. Reidar Thomte with Albert B. Anderson (Princeton, NJ: Princeton University Press).

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).

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: Oxford University Press).

Lakoff, George and Mark Johnson (1980), Metaphors We Live By (Chicago, IL: University of Chicago Press).

Kundera, Milan (1997), Slowness: A Novel, tr. Linda Asher (New York: HarperCollins).

Landes, Richard (1998), Whilst God Tarried: Disappointed Millennialism and the Genealogy of the Modern West (New York: Basic Books).

Latour, Bruno (1988), The Pasteurization of France, trs. Alan Sheridan and John Law (Cambridge, MA: Harvard University Press).

Latour, Bruno (1993) [1991], We Have Never Been Modern, tr. Catherine Porter (Cambridge, MA: Harvard University Press).

Latour, Bruno (2005), Reassembling the Social: An Introduction to Actor-Network Theory (Oxford: Oxford University Press).

Law, John (2004), After Method: Mess in Social Science Research (London: Routledge).

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).

Lidwell, William, Kritina Holden and Jill Butler (2010) [2003], Universal Principles of Design, rev. edn. (Gloucester, MA: Rockport Publishers).

Lucas, Gavin (2005), The Archaeology of Time (London: Routledge).

McGinn, Bernard (1998) [1979], Visions of the End: Apocalyptic Traditions in the Middle Ages (New York: Columbia University Press).

Mackenzie, Adrian (2002), Transductions: Bodies and Machines at Speed (London: Continuum).

McLuhan, Marshall (2002) [1951], The Mechanical Bride: Folklore of Industrial Man (Corte Madera, CA: Ginkgo Press).

McManners, John (1981), Death and the Enlightenment: Changing Attitudes to Death Among Christians and Unbelievers in Eighteenth-Century France (Oxford: Oxford University Press).

Miéville, China (2012), London's Overthrow (London: Westbourne Press).

Mills, David L. (2006), Computer Network Time Synchronization: The Network Time Protocol (Boca Raton, FL: CRC Press).

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).

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, CA: Stanford University Press).

Mueller, John (1995), Quiet Cataclysm: Reflections on the Recent Transformation of World Politics (New York: HarperCollins).

Mumford, Lewis (1934), Technics and Civilization (New York: Harcourt, Brace and Company).

Münkler, Herfried (2005), The New Wars (Cambridge, Polity Press).

Naughtie, James (2005), The Accidental American: Tony Blair and the Presidency, rev. edn. (London: Macmillan).

Needham, Joseph (1959), Science and Civilization in China, vol. III: Mathematics and the Sciences of the Heavens and Earth (Cambridge: Cambridge University Press).

Neocleous, Mark (2008), Critique of Security (Edinburgh: 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).

Newton, Isaac (1729), The Mathematic Principles of Natural Philosophy, vol. 1, tr. Andrew Motte (London: Benjamin Motte).

Nietzsche, Friedrich (1911) [1888], Ecce Homo, tr. Anthony M. Lupovici (New York: Macmillan).

Nowotny, Helga (1994), Time: The Modern and Postmodern Experience (Cambridge: Polity Press).

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).

Orwell, George (1965) [1949], Nineteen Eighty-Four (London: Heinemann).

Osborne, Peter (1995), The Politics of Time: Modernity and Avant-Garde (London: Verso).

Overy, Richard (2009), The Morbid Age: Britain Between the Wars (London: Allen Lane).

Ovid (1916), Metamorphoses, vol. 2, tr. Frank Justus Miller (London: William Heinemann, Ltd.).

Parker Pearson, Mike (1999), The Archaeology of Death and Burial (Stroud: Sutton Publishing).

Parsons, Talcott (1949) [1937], The Structure of Social Action, 2nd. edn. (Glencoe, IL: The Free Press).

Peake, Mervyn (2011) [1959], Titus Alone (London: Vintage Books).

Penrose, Roger (1989), The Emperor's New Mind: Concerning Computers, Minds and the Laws of Physics (Oxford: Oxford University Press).

Perrow, Charles(1999) [1984], Normal Accidents: Living with High-Risk Technologies, 2nd. edn. (Princeton, NJ: Princeton University Press).

Peters, F.E. (1967), Greek Philosophical Terms: A Historical Lexicon (New York: New York University Press).

Pick, Daniel (1993), War Machine: The Rationalisation of Slaughter in the Modern Age (New Haven, CT: Yale University Press).

Pike, Luke Owen (1894), A Constitutional History of the House of Lords (London: Macmillan and Co.)

Plotinus (1992), The Enneads, tr. Stephen MacKenna (Burdett, NY: Larson Publications).

Ramo, Joshua Cooper (2009), The Age of the Unthinkable: Why the New World Order Constantly Surprises Us and What We Can Do About It (New York: Little, Brown and Company).

Reichenbach, Hans and Maria Reichenbach (1956), The Direction of Time (Berkeley, CA: University of California Press).

Rescher, Nicholas (1996), Process Metaphysics: An Introduction to Process Philosophy (Albany, NY: State University of New York Press).

Rid, Thomas (2013), Cyber War Will Not Take Place (London: Hurst & Company).

Rifkin, Jeremy (1987), Time Wars: The Primary Conflict in Human History (New York: Henry Holt and Company).

Romm, Joseph J. (1993), Defining National Security: The Nonmilitary Aspects (New York: Council on Foreign Relations Press).

Rosa, Hartmut and William E. Scheuerman, eds. (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).

Rosenzweig, Paul (2013), Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World (Santa Barbara, CA: ABC-CLIO).

Ross, Andrew (1991), Strange Weather: Culture, Science and, Technology in the Age of Limits (New York: Verso).

Sabin, Philip (2012), Simulating War: Studying Conflict Through Simulation Games (London: Continuum).

Sanders, James (2001), Celluloid Skyline: New York and the Movies (New York: Alfred A. Knopf).

Sanger, David E. (2012), Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown Publishers).

Sawyer, Rex (2001), Little Imber on the Down: Salisbury Plain's Ghost Village (East Knoyle: The Hobnob Press).

Schell, Bernadette and Clemens Martin (2006), Webster's New World Hacker Dictionary (Indianapolis, IN: Wiley Publishing, Inc.).

Scheuerman, William E. (2004), Liberal Democracy and the Social Acceleration of Time (Baltimore, MD: Johns Hopkins University Press).

Schivelbusch, Wolfgang (1986) [1977], The Railway Journey: The Industrialization of Time and Space in the 19th Century (Berkeley, CA: University of California Press).

Schegel, Friedrich (1828), Kritische Friedrich Schlegel Ausgabe, vol. 9, Philosophie der Geschichte (1828).

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: Chicago University Press).

Schwartau, Winn (1991), Terminal Compromise—Computer Terrorism: When Privacy and Freedom are the Victims (Seminole, FL: Interpact Press).

Schwartau, Winn (1993) [1991], Terminal Compromise—Computer Terrorism: When Privacy and Freedom are the Victims (Seminole, FL: Interpact Press).

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).

Shakespeare, William (1988), The Complete Works, eds. Stanley Wells and Gary Taylor (Oxford: Clarendon Press).

Smart, Barry (1992), Postmodernity (London: Routledge).

Spellman, Frank R. and Melissa L. Stoudt (2011), Nuclear Infrastructure Protection and Homeland Security (Lanham, MD: Government Institutes).

Staudenmeier, John M. (1985), Technology's Storytellers: Reweaving the Human Fabric (Cambridge, MA: MIT Press).

Steele, Brent J. (2008), Ontological Security In International Relations: Self-Identity and the IR State (Abingdon: Routledge).

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', The Virtual Battlefield: Perspectives on Cyber Warfare, eds. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press), 118-131.

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 A. (1999), Hackers: Crime in the Digital Sublime (London: Routledge).

Tennyson, Alfred (1971), Poems and Plays, ed. T. Herbert Warren (Oxford: Oxford University Press).

Thrift, Nigel (2008), Non-Representational Theory: Space, Politics, Affect (London: Routledge).

Thoreau, Henry David (1888) [1854], Walden (London: Walter Scott).

Toulmin, Stephen and June Goodfield (1965), The Discovery of Time (London: Hutchinson).

Trigger, Bruce G. (1989), A History of Archaeological Thought (Cambridge: Cambridge University Press).

Tsouras, Peter G., ed. (2000), The Greenhill Dictionary of Military Quotations (London: Greenhill Books).

Turkle, Sherry (2009), Simulation and Its Discontents (Cambridge, MA: MIT Press).

Verbeek, Peter-Paul (2004), What Things Do: Philosophical Reflections on Technology, Agency, and Design (University Park, PA: Pennsylvania State University Press).

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 (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 Philippe Petit (1999) [1996], Politics of the Very Worst: An Interview by Philippe Petit, tr. Michael Cavaliere, ed. Sylvère Lotringer (New York: Semiotext(e)).

Walker, R.B.J. (1993), Inside/Outside: International Relations as Political Theory (Cambridge: Cambridge University Press).

Ward, Koral (2008), Augenblick: The Concept of the 'Decisive Moment' in 19th- and 20th-Century Philosophy (Aldershot: Ashgate Publishing).

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).

Weinberg, Gerhard L. (1994), A World at Arms: A Global History of World War II (Cambridge: Cambridge University Press).

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).

Whitehead, Alfred North (1920), The Concept of Nature (Cambridge: Cambridge University Press).

Wojcik, Daniel (1997), The End of the World as We Know It: Faith, Fatalism, and Apocalypse in America (New York: New York University Press).

Woodward, Bob (2002), Bush at War (New York: Simon & Schuster).

Yeats, William Butler (2008), The Collected Poems of W.B. Yeats (Ware: Wordsworth Editions).

Young-Bruehl, Elisabeth (1984), Hannah Arendt: For Love of the World (London: Yale University Press).

Zittrain, Jonathan (2008), The Future of the Internet—And How to Stop It (London: Penguin).

**B2. Book Chapters**

Adler, Emanuel (2012), 'Constructivism in International Relations: Sources, Contributions, and Debates', in Handbook of International Relations, eds. Walter Carlsnaes, Thomas Risse and Beth A. Simmons, 2nd. edn. (Thousand Oaks, CA: Sage), 112-144.

Agnew, John (2011), 'Space and Place', in Handbook of Geographical Knowledge, eds. John Agnew and David N. Livingstone (London: Sage), 316-330.

Aho, James A. (1997), 'The Apocalypse of Modernity', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements, eds. Thomas Robbins and Susan J. Palmer (New York: Routledge), 61-72.

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, eds. Louise Amoore and Marieke de Goede (London: Routledge), 23-40.

Aron, Raymond (1984) [1978], 'The Dawn of Universal History', Politics and History, ed. and tr. Miriam Bernheim Conant (New Brunswick, NJ: Transaction Publishers), 212-233.

Arquilla, John (2009), 'Information Wars', in Globalization and Security: An Encyclopedia, vol. 1, Social and Cultural Aspects, eds. G. Honor Fagan and Ronaldo Munck (Westport, CT: Praeger Security International), 206-220.

Bakhtin, Mikhail (1981) [1937-1938], 'Forms of Time and of the Chronotope in the Novel: Notes Towards an Historical Poetics', in 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.

Barkun, Michael (1997), 'Millenarians and Violence: The Case of the Christian Identity Movement', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements, eds. Thomas Robbins and Susan J. Palmer (New York: Routledge), 247-260.

Baudelaire, Charles (1981), 'The Painter of Modern Life', Selected Writings on Art and Artists, tr. P.E. Charvet (Cambridge: Cambridge University Press), 390-435.

Bender, John and David E. Wellbery (1991), 'Introduction', in Chronotypes: The Construction of Time, eds. John Bender and David E. Wellbery (Stanford, CA: Stanford University Press), 1-15.

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, eds. Johan Eriksson and Giampiero Giacomello (London: Routledge), 57-82.

Benjamin, Walter (1979), 'One-Way Street', One-Way Street and Other Writings, trs. Edmund Jephcott and Kingsley Shorter (London: NLB), 45-104.

Bennett, Jane (2010), 'A Vitalist Stopover on the Way to a New Materialism', in New Materialisms: Ontology, Agency, and Politics, eds. Diana Coole and Samantha Frost (Durham, NC: Duke University Press), 47-69.

Bigo, Didier (2001), 'The Möbius Ribbon of Internal and External Security(ies)', in Identities, Borders, Orders: Rethinking International Relations Theory, eds. Mathias Albert, David Jacobson and Yosef Lapid (Minneapolis, MN: University of Minnesota Press), 91-136.

Bozeman, John M. (1997), 'Technological Millennialism in the United States', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements, eds. Thomas Robbins and Susan J. Palmer (New York: Routledge), 139-158.

Bromley, David G. (1997), Constructing Apocalypticism: Social and Cultural Elements of Radical Organization', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements, eds. Thomas Robbins and Susan J. Palmer (New York: Routledge), 32-45.

Bryant, Levi, Nick Srnicek and Graham Harman (2011), 'Towards a Speculative Philosophy', in The Speculative Turn: Continental Materialism and Realism, eds. Levi Bryant, Nick Srnicek and Graham Harman (Melbourne: re.press), 1-18.

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.

Carnap, Rudolf (1963), 'Intellectual Autobiography', in The Philosophy of Rudolf Carnap, ed. Paul Arthur Schilpp (La Salle, IL: Open Court), 3-84.

Caroll, Brian (2002), 'Seeing Cyberspace: The Electrical Infrastructure as Architecture', in The Cities of Everyday Life, eds. Ravi Vasudevan, Ravi Sundaram, Jeebesh Bagchi, Monica Narula, Geert Lovink and Shuddhabrata Sengupta (Delhi: Centre for the Study of Developing Societies), 249-267.

Carter, Sean and Derek P. McCormack (2010), 'Affectivity and Geopolitical Images', in Observant States: Geopolitics and Visual Culture, eds. Fraser McDonald, Rachel Hughes and Klaus Dodds (London: IB Tauris), 103-122.

Castoriadis, Cornelius (1991), 'Time and Creation', in Chronotypes: The Construction of Time, eds. John Bender and David E. Wellbery (Stanford, CA: Stanford University Press), 38-64.

Collier, Stephen J. and Aihwa Ong (2005), 'Global Assemblages, Anthropological Problems', in Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems, eds. Aihwa Ong and Stephen J. Collier (Malden, MA: Blackwell), 3-21.

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, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge), 109-129.

Cook, Martin L. (2004), 'Christian Apocalypticism and Weapons of Mass Destruction', in Ethics and Weapons of Mass Destruction: Religious and Secular Perspectives, eds. Sohail H. Hashmi and Steven P. Lee (Cambridge: Cambridge University Press), 200-210.

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), 177-199.

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), 137-162.

Dellamora, Richard (1995), 'Introduction', in Postmodern Apocalypse: Theory and Cultural Practice at the End, ed. Richard Dellamora (Philadelphia, PA: University of Pennsylvania Press), 1-14.

Dennett, Daniel (2000), 'Making Tools for Thinking', in Metarepresentations: A Multidisciplinary Perspective, ed. Dan Sperber (New York: Oxford University Press, 2000), 17-29.

Der Derian, James (2009), 'Paul Virilio', in Critical Theorists and International Relations, eds. Jenny Edkins and Nick Vaughan-Williams (Abingdon: Routledge), 330-340.

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, eds. Paul Graves-Brown, Siân Jones and Clive Gamble (London: Routledge), 48-61.

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), 159-185.

Duncan, James (1993), 'Sites of Representation: Place, Time and the Discourse of the Other', in Place/Culture/Representation, eds. 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, eds. 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. 2: Analyzing Issues, Challenges, and Prospects, eds. Myriam Dunn and Victor Mauer (Zurich: Swiss Federal Institute of Technology), 189-206.

Dunn Cavelty, Myriam and Jennifer Giroux (forthcoming), '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).

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, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge), 1-14.

Dunn Cavelty, 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, eds. Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel (Aldershot: Ashgate), 151-162.

Dunn Cavelty, Myriam and Manuel Suter (2012), 'The Art of CIIP Strategy: Taking Stock of Content and Processes', in Critical Information Infrastructure Protection, eds. Javier Lopez, Robert Setola and Stephen D. Wolthusen (Berlin: Springer-Verlag), 15-38.

Eriksson, Johan and Giampiero Giacomello (2007a), 'Introduction: Closing the Gap between International Relations Theory and Studies of Digital-Age Security', in International Relations and Security in the Digital Age, eds. Johan Eriksson and Giampiero Giacomello (London: Routledge), 1-28.

Foucault, Michel (1984), 'What is Enlightenment?', in The Foucault Reader, ed. Paul Rabinow (New York: Pantheon Books), 32-50.

Goscilo, Helena (2013), 'Putin's Performance of Masculinity: The Action Hero and Macho Sex-Object', in Putin as Celebrity and Cultural Icon, ed. Helena Goscilo (New York: Routledge), 180-205.

Gusterson, Hugh (1999), 'Missing the End of the Cold War in International Security', in Cultures of Insecurity: States, Communities, and the Production of Danger, eds. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall (Minneapolis, MN: University of Minnesota Press), 319-345.

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), 149-181.

Hassan, Robert (2007), 'Network Time', in 24/7: Time and Temporality in the Network Society, eds. Robert Hassan and Ronald E. Purser (Stanford, CA: Stanford Business Books), 37-61.

Hobsbawm, Eric (2013), 'The American Cowboy: An International Myth?', Fractured Times: Culture and Society in the 20th Century (London: Little, Brown), 272-289.

Holquist, Michael (2010), 'The Fugue of Chronotope', in Bakhtin's Theory of the Literary Chronotope: Reflections, Applications, Perspectives, eds. Nele Bemong, Pieter Borghart, Michel de Dobbeleer, Kristoffel Demoen, Koen de Temmerman and Bart Keunen (Ghent: Ginkgo Academia Press), 19-33.

Huysmans, Jef (1997), 'James Der Derian: The Unbearable Lightness of Theory', in The Future of International Relations: Masters in the Making?, eds. Iver B. Neumann and Ole Wæver (London: Routledge), 361-383.

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.

Jessop, Bob (2009), 'The Spatiotemporal Dynamics of Globalizing Capital and Their Impact on State Power and Democracy', in High Speed: Social Acceleration, Power, and Modernity, eds. Hartmut Rosa and William E. Scheuerman (University Park, PA: Pennsylvania State University Press), 135-158.

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), 262-274.

Kohl, Philip L. and Clare Fawcett (1995), 'Archaeology in the Service of the State: Theoretical Considerations', in Nationalism, Politics, and the Practice of Archaeology, eds. Philip L. Kohl and Clare Fawcett (Cambridge: Cambridge University Press), 3-18.

Krüger, Jörg, Bertram Nickolay and Sandro Gaycken (2013), 'Preface', in The Secure Information Society: Ethical, Legal and Political Challenges, eds. Jörg Krüger, Bertram Nickolay and Sandro Gaycken (London: Springer-Verlag), v-vi.

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.

Latour, Bruno (1990), 'Drawing Things Together', in Representation in Scientific Practice, eds. 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, eds. Wiebe E. Bijker and John Law (Cambridge, MA: MIT Press), 225-258.

Lawson, Sean (2013), '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, eds. Christopher Laing, Atta Badii and Paul Vickers (Hershey, PA: IGI Global), 168-188.

Leccardi, Carmen (2007), 'New Temporal Perspectives in the "High-Speed Society"', in 24/7: Time and Temporality in the Network Society, eds. Robert Hassan and Robert E. Purser (Stanford, CA: Stanford Business Books), 25-36.

Lyotard, Jean-François (1987), 'The Sign of History', in Post-Structuralism and the Question of History, eds. Derek Attridge, Geoff Bennington and Robert Young (Cambridge: Cambridge University Press), 162-180.

Macaulay, Thomas Babington (1903), 'Southey's Colloquies on Society (Jan. 1830)', Critical and Historical Essays Contributed to the Edinburgh Review, vol. 1 (London: Longman, Green, and Co.), 215-266.

MacKenzie, Donald (1996), 'Nuclear Weapons Laboratories and the Development of Supercomputing', Knowing Machines: Essays on Technical Change (Cambridge, MA: MIT Press), 99-129.

McLuhan, Marshall (2006) [2001], 'The Medium is the Message', in Media and Cultural Studies: KeyWorks, rev. edn., eds. Meenakshi Gigi Durham and Douglas M. Kellner (Malden, MA: Blackwell Publishing), 107-116, originally published as Marshall McLuhan, 'The Medium is the Message', Understanding Media: The Extensions of Man (New York: Signet, 1964), 23-35, 63-67.

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: Cambridge University Press), 151-175.

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.

May, Jon and Nigel Thrift (2001), 'Introduction', in Timespace: Geographies of Temporality, eds. Jon May and Nigel Thrift (London: Routledge), 1-46.

Mellor, D.H. (1993), 'The Unreality of Tense', in The Philosophy of Time, eds. Robin Le Poidevin and Murray MacBeath (Oxford: Oxford University Press), 47-59.

Minkowski, Hermann (2010), 'Space and Time', tr. Dennis Lehmkuhl, in Minkowski Spacetime: A Hundred Years Later, ed. Vesselin Petkov (New York: Springer), xiv-xli. Originally presented to the Eightieth Meeting of German Natural Scientists and Physicians, Köln, 21 September 1908, and published in 1909 as 'Raum und Zeit', Jahresberichte der Deutschen Mathematiker-Vereinigung, 1-14.

Molfino, Emily (2012), 'Viewpoint: Cyberterrorism: Cyber "Pearl Harbor" is Imminent', in Cyberspaces and Global Affairs, eds. Sean S. Costigan and Jake Perry (Farnham: Ashgate Publishing), 75-82.

Ong, Aihwa (2005), 'Ecologies of Expertise: Assembling Flows, Managing Citizenship', in Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems, eds. Aihwa Ong and Stephen J. Collier (Malden, MA: Blackwell Publishers), 337-353.

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, eds. Stef Aupers and Dick Houtman (Leiden: Brill), 239-259.

Paz, Octavio (1974) [1969], 'Order and Accident', Conjunctions and Disjunctions, tr. Helen R. Lane (New York: Viking Press,), 91-139.

Portnoy, Michael and Seymour Goodman (2009), 'A Brief History of Global Responses to Cyber Threats', in Global Initiatives to Secure Cyberspace: An Emerging Landscape, eds. Michael Portnoy and Seymour Goodman (New York: Springer), 5-10.

Prior, Arthur N. (1993), 'Changes in Events and Changes in Things', in The Philosophy of Time, eds. Robin Le Poidevin and Murray MacBeath (Oxford: Oxford University Press), 35-46.

Robbins, Thomas and Susan J. Palmer (1997), 'Patterns of Contemporary Apocalypticism in North America', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements, eds. Thomas Robbins and Susan J. Palmer (New York: Routledge, 1997), 1-27.

Robin, Corey (2012), 'The Language of Fear: National Security in Modern Politics', in Fear: Across the Disciplines, eds. Jan Plamper and Benjamin Lazier (Pittsburgh, PA: University of Pittsburgh Press), 118-131.

Rosa, Hartmut (2009), 'Social Acceleration: Ethical and Political Consequences of a Desynchronized High-Speed Society', in High-Speed Society: Social Acceleration, Power, and Modernity, eds. Hartmut Rosa and William E. Scheuerman (University Park, PA: Pennsylvania State University Press), 77-111.

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.

Saco, Diana (1999), 'Colonizing Cyberspace: "National Security" and the Internet', in Cultures of Insecurity: States, Communities, and the Production of Danger, eds. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall (Minneapolis, MN: University of Minnesota Press), 261-291.

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.

Schurz, Carl (1913), 'Manifest Destiny', Speeches, Correspondence and Political Papers, vol. 5, ed. Frederic Bancroft (New York: The Knickerbocker Press), 191-214.

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, NJ: Princeton University Press, 2010), 104-126.

Virilio, Paul (2004), 'The Last Vehicle', in The Paul Virilio Reader, ed. Steve Redhead (New York: Columbia University Press), 109-120.

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 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 Nicholas Zurbrugg (2001), 'Not Words But Visions! Interview with Nicholas Zurbrugg (1998)', in Virilio Live: Selected Interviews, ed. John Armitage (London: Sage), 154-163.

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, R.B.J. (1997), 'The Subject of Security', in Critical Security Studies: Concepts and Cases, eds. 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. 36, ed. W.S. Lewis (New Haven, CT: Yale University), 231-233.

Weithman, Paul (2001), 'Augustine's Political Philosophy', in The Cambridge Companion to Augustine, eds. Eleonore Stump and Norman Kretzmann (Cambridge: Cambridge University Press, 2001), 234-252.

Wessinger, Catherine (1997), 'Millennialism With and Without the Mayhem', in Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements , eds. 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), 307-318.

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), 209-243.

Woodcock, George (1977), 'The Tyranny of the Clock', in The Anarchist Reader, ed. George Woodcock (Hassocks: Harvester Press), 132-136.

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.

**B3. Journal Articles**

Abrahamsen, Rita and Michael C. Williams (2009), 'Security Beyond the State: Global Security Assemblages in International Politics', International Political Sociology 3, no. 1: 1-17.

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: 458-473.

Adams, James (2001), 'Virtual Defense', Foreign Affairs 80, no. 3: 98-112.

Adler, Emanuel (1997), 'Seizing the Middle Ground: Constructivism in World Politics', European Journal of International Relations 3, no. 3: 319-363.

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 and Peter M. Haas (1992), 'Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program', International Organization 46, no. 1: 367-390.

Adler, Emanuel and Vincent Pouliot (2011), 'International Practices', International Theory 3, no. 1: 1-36.

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 & Society 5, no. 1: 27-45.

Allan, Stuart (1994), '"When Discourse is Torn From Reality"': Bakhtin and the Principle of Chronotopicity', Time & Society 3, no. 2: 193-218.

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 (2010), 'Security and the Future: Anticipating the Event of Terror', Geoforum 41, no. 2: 227-235.

Anderson, Ben (2010), 'Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies', Progress in Human Geography 34, no. 6: 1-22.

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.

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 & Society 16, nos. 5-6: 25-55.

Barnard-Wills, David and Debi Ashenden (2012), 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', Space & Culture 15, no. 2: 110-123.

Barzashka, Ivanka (2013), 'Are Cyber-Weapons Effective?', The RUSI Journal 158, no. 2: 48-56.

Baudrillard, Jean (1997), 'The End of the Millennium or the Countdown', Economy & Society 26, no. 4: 447-455.

Bauer, Johannes M. and Michel J.G. van Eeten (2009), 'Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options', Telecommunications Policy 33, nos. 10-11: 706-719.

Beck, Ulrich and Daniel Levy, 'Cosmopolitanized Nations: Re-Imagining Collectivity in World Risk Society', Theory, Culture & Society 30, no. 2: 3-31.

Bendrath, Ralf (2001), 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', Information & Security 7: 80-103.

Bennett, Oliver (2011), 'Cultures of Optimism', Cultural Sociology 5, no. 2: 301-320.

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: 775-786.

Betz, David J. and Tim Stevens (2013), 'Analogical Reasoning and Cyber Security', Security Dialogue 44, no. 2: 147-164.

Bhaskar, Rahul (2006), 'State and Local Law Enforcement is Not Ready for a Cyber Katrina', Communications of the ACM 49, no. 2: 81-83.

Blank, Stephen (2008), 'Web War I: Is Europe's First Information War a New Kind of War?', Comparative Strategy 27, no. 3: 227-247.

Bobrow, Davis B. (1986), 'Complex Insecurity: Implications of a Sobering Metaphor', International Studies Quarterly 40, no. 4: 435-450.

Boin, Arjen (2004), 'Lessons from Crisis Research', International Studies Review 6, no. 1: 165-174.

Boin, Arjen and Allan McConnell (2007), 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience', Journal of Contingencies & Crisis Management 15, no. 1: 50-59.

Bolt, Neville (2009), 'Unsettling Networks', The RUSI Journal 154, no. 5: 34-39.

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: 739-764.

Bowker, Geoffrey (1993), 'How to Be Universal: Some Cybernetic Strategies, 1943-70', Social Studies of Science 23, no. 1: 107-127.

Boyle, Philip and Kevin D. Haggerty (2009), 'Spectacular Security: Mega-Events and the Security Complex', International Political Sociology 3, no. 3: 257-274.

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: 241-259.

Brandão, Luis Alberto (2006), 'Chronotope', Theory, Culture & Society 23, nos. 2-3: 133-134.

Brants, Kees (1989), 'The Social Construction of the Information Revolution', European Journal of Communication 4, no. 1 (1989): 79-97.

Brown, Chris (1994), '"Turtles All the Way Down": Anti-Foundationalism, Critical Theory and International Relations', Millennium: Journal of International Studies 23, no. 2: 213-236.

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: 235-255.

Bubandt, Nils (2005), 'Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds', Security Dialogue 36, no. 3: 275-296.

Budiansky, Stephen (2010), 'What's the Use of Cryptologic History?', Intelligence & National Security 25, no. 6: 767-777.

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: 471-487.

Büthe, Tim (2002), 'Taking Temporality Seriously: Modeling History and the Use of Narratives as Evidence', American Political Science Review 96, no. 3: 481-493.

Campbell, David (2002), 'Time is Broken: The Return of the Past in the Response to September 11', Theory & Event 5, no. 4: n.p., http://www.david-campbell.org/wp-content/documents/Time_is_broken.pdf.

Cannavò, Peter F. (2012), 'Ecological Citizenship, Time, and Corruption: Aldo Leopold's Green Republicanism', Environmental Politics 21, no. 6: 864-881.

Carr, Matt (2010), 'Slouching Towards Dystopia: The New Military Futurism', Race & 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: 579-593.

Castells, Manuel (2000), 'Urban Sustainability in the Information Age', City: Analysis of Urban Trends, Culture, Theory, Policy, Action 4, no. 1: 118-122.

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

Chandler, David (2012), 'Resilience and Human Security: The Post-Interventionist Paradigm', Security Dialogue 43, no. 3: 213-229.

Chandler, David (2013), 'Resilience and the Autotelic Subject: Toward a Critique of the Societalization of Security', International Political Sociology 7, no. 2: 210-226.

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.

Chertoff, Michael (2008), 'The Cybersecurity Challenge', Regulation & Governance 2, no. 4: 480-484.

Chesneaux, Jean (2000), 'Speed and Democracy: An Uneasy Dialogue', Social Science Information 39, no. 3: 407-420.

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.

Coaffee, Jon (2010) 'Protecting Vulnerable Cities: The UK's Resilience Response to Defending Everyday Urban Infrastructure', International Affairs 86, no. 4: 939-954.

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: 133-149.

Cohen, Julie E. (2007), 'Cyberspace As/And Space', Columbia Law Review 107, no. 1: 210-256.

Connolly, William E. (2000), 'Speed, Concentric Cultures, and Cosmopolitanism', Political Theory 28, no. 5: 596-618.

Conway, Maura (2011), 'Against Cyberterrorism', Communications of the ACM 54, no. 2: 26-28.

Copeland, Dale C. (2000), 'The Constructivist Challenge to Structural Realism: A Review Essay', International Security 25, no. 2: 187-212.

Cordle, Daniel (2012), 'Protect/Protest: British Nuclear Fiction of the 1980s', The British Journal for the History of Science 45, no. 4: 653-669.

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 & Television 10, no. 1: 71-92.

Cox, Robert W. (1981), 'Social Forces, States and World Orders: Beyond International Relations Theory', Millennium: Journal of International Studies 10, no. 2: 126-155.

Cunningham, Kevin and Robert R. Tomes (2004), 'Space-Time Orientations and Contemporary Political-Military Thought', Armed Forces & Society 31, no. 1: 119-140.

Davis Cross, Mai'a K. (2013), 'Rethinking Epistemic Communities Twenty Years Later', Review of International Studies 39, no. 1: 137-160.

Defty, Andrew (2008), 'Educating Parliamentarians about Intelligence: The Role of the British Intelligence and Security Committee', Parliamentary Affairs 61, no. 4: 621-641.

De Goede, Marieke (2008), 'Beyond Risk: Premediation and the Post-9/11 Security Imagination', Security Dialogue 39, nos. 2-3: 155-176.

Deibert, Ronald J. (1999), 'Harold Innis and the Empire of Speed', Review of International Studies 25, no. 2: 273-289.

Deibert, Ronald J. (2012), 'The Growing Dark Side of Cyberspace (… And What To Do About It)', Penn State Journal of Law & International Affairs 1, no. 2: 260-274.

DeLashmutt, Michael W. (2006), 'A Better Life Through Information Technology? The Techno-Theological Eschatology of Posthuman Speculative Science', Zygon 41, no. 2: 267-288.

De Mul, Jos (1999), 'The Informatization of the Worldview', Information, Communication & Society 2, no. 1: 69-94.

Denning, Peter J. (2001), 'Who Are We?', Communications of the ACM 44, no. 2: 15-19.

Denning, Peter J. and Dennis J. Frailey (2011), 'Who Are We—Now?', Communications of the ACM 54, no. 6: 25-27.

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 (1999), 'The Conceptual Cosmology of Paul Virilio', Theory, Culture & Society 16, nos. 5-6: 215-227.

Der Derian, James (2001), 'Global Events, National Security, and Virtual Theory', Millennium: Journal of International Studies 30, no. 3: 669-690.

Der Derian, James (2002), 'Virtuous War/Virtual Theory', International Affairs 76, no. 4: 771-788.

Der Derian, James (2003), 'The Question of Information Technology in International Relations', Millennium: Journal of International Studies 32, no. 3: 441-456.

Derrida, Jacques (1984), 'No Apocalypse, Not Now (Full Speed Ahead, Seven Missiles, Seven Missives)', diacritics 14, no. 2: 20-31.

Dillon, Michael (2011), 'Specters of Biopolitics: Finitude, Eschaton, and Katechon', South Atlantic Quarterly 110, no. 3: 780-792.

Dillon, Michael and Julian Reid (2001), 'Global Liberal Governance: Biopolitics, Security and War', Millennium: Journal of International Studies 30, no. 1: 41-66.

Dimitrov, Radoslav S. (2010), 'Inside Copenhagen: The State of Climate Governance', Global Environmental Politics 10, no. 2: 18-24.

Dunn Cavelty, Myriam (2007), 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Journal of Information Technology & Politics 4, no. 1: 19-36.

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: 105-122.

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.

Enloe, Cynthia (2011), 'The Mundane Matters', International Political Sociology 5, no. 4: 447-450.

Eriksson, Johan (2001), 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', Journal of Contingencies & Crisis Management 9, no. 4: 211-222.

Everett, Daniel L. (2005), 'Cultural Constraints on Grammar and Cognition in Pirahã', Current Anthropology 46, no. 4: 621-646.

Farrell, Theo (1996), 'Figuring Out Fighting Organisations: The New Organisational Analysis in Strategic Studies', Journal of Strategic Studies 19, no. 1: 122-135.

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 & Society 24, no. 2: 105-109.

Featherstone, Mark (2010), 'Virilio's Apocalypticism', CTheory, 16 September, http://www.ctheory.net/articles.aspx?id=662.

Feldman, Stanley and Lee Sigelman (1985), 'The Political Impact of Prime-Time Television: "The Day After"', The Journal of Politics 47, no. 2: 556-578.

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.

Formosa, Paul (2013), 'Is Kant a Moral Constructivist or a Moral Realist?', European Journal of Philosophy 21, no. 2: 170-196.

Foucault, Michel (1986), 'Of Other Spaces', diacritics 16, no. 1: 22-27.

Fox, Robin (2001), 'Time Out of Mind: Anthropological Reflections on Temporality', KronoScope 1, nos. 1-2: 129-137.

Fraser, J.T. (1992), 'Human Temporality in a Nowless Universe', Time & Society 1, no. 2: 159-173.

Fraser, J.T. (2001), 'The Extended Umwelt Principle: Uexküll and the Nature of Time', Semiotica 134, nos. 1-4: 263-273.

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: 151-175.

Friedman, Milton (1961), 'The Lag in Effect of Monetary Policy', Journal of Political Economy 69, no. 5: 447-466.

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.

Gane, Nicholas (2006), 'Speed Up or Slow Down? Social Theory in the Information Age', Information, Communication & 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.

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 & Emergency Management 7, no. 1, article 74.

Gerovitch, Slava (2008), 'InterNyet: Why the Soviet Union Did Not Build a Nationwide Computer Network', History & Technology 24, no. 4: 335-350.

Gill, Peter (2007), 'Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the "War on Terror"', Intelligence & National Security 22, no. 1: 14-37.

Gill, Stanley (1951), 'The Diagnosis of Mistakes in Programmes on the EDSAC', Proceedings of the Royal Society A 206, no. 1087: 538-554.

Glenny, Misha and Camino Kavanagh (2012), '800 Titles But No Policy—Thoughts on Cyber Warfare', American Foreign Policy Interests 34, no. 6: 287-294.

Golding, Peter (2000), 'Forthcoming Features: Information and Communications Technologies and the Sociology of the Future', Sociology 34, no. 1: 165-184.

Goodman, Seymour E., Jessica C. Kirk and Megan H. Kirk (2007), 'Cyberspace as a Medium for Terrorists', Technological Forecasting & Social Change 74, no. 2: 193-210.

Gordon, Uri (2009), 'Anarchism and the Politics of Technology', WorkingUSA: The Journal of Labor & Society 12, no. 3: 489-503.

Graham, Philip (2001), 'Space: Irrealis Objects in Technology Policy and Their Role in a New Political Economy', Discourse & Society 12, no. 6: 761-788.

Graham, Stephen and Nigel Thrift (2007), 'Out of Order: Understanding Repair and Maintenance', Theory, Culture & Society 24, no. 3: 1-25.

Gregory, Donna U. (1989), 'The Dictator's Furnace', Peace Review: A Journal of Social Justice 1, no. 1: 12-16.

Grove, Kevin (2013), 'On Resilience Politics: From Transformation to Subversion', Resilience: International Policies, Practices and Discourses 1, no. 2: 146-153.

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.

Grzymala-Busse, Anna (2011), 'Time Will Tell? Temporality and the Analysis of Causal Mechanisms and Processes', Comparative Political Studies 44, no. 9: 1267-1297.

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.

Guzzini, Stefano (2000), 'A Reconstruction of Constructivism in International Relations', European Journal of International Relations 6, no. 2: 147-182.

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.

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: 361-374.

Hancock, Peter (2007), 'On the Nature of Time in Conceptual and Computational Nervous Systems', KronoScope 7, 2: 185-196.

Hansen, Lene and Helen Nissenbaum (2009), 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly 53, no. 4: 1155-1175.

Harknett, Richard A. and James A. Stever (2011), 'The New Policy World of Cybersecurity', Public Administration Review 71, no. 3: 455-460.

Harman, Graham (2010), 'Technology, Objects and Things in Heidegger', Cambridge Journal of Economics 34, no. 1: 17-25.

Harman, Graham (2010), 'I Am Also of the Opinion that Materialism Must Be Destroyed', Environment and Planning D: Society and Space 28, no. 5: 772-790.

Harris, Paul A. (2012), 'Time and Emergence in the Evolutionary Epic, Naturalistic Theology, and J.T. Fraser's Hierarchical Theory of Time', KronoScope 12, no. 2: 147-158.

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: 411-434.

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.

Healey, Jason (2010), 'The Five Futures of Cyber Conflict and Cooperation', Georgetown Journal of International Affairs 11, no. 1: 110-117.

Hellström, Tomas (2003), 'Systemic Innovation and Risk: Technology Assessment and the Challenge of Responsible Innovation', Technology in Society 25, no. 3: 369-384.

Hellström, Tomas (2007), 'Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework', Safety Science 45, no. 3: 415-430.

Hindess, Barry (2007), 'The Past is Another Culture', International Political Sociology 1, no. 4: 325-338.

Hobson, John and George Lawson, 'What is History in International Relations?', Millennium: Journal of International Studies 37, no. 2: 415-435.

Holt, Thomas J. (2007), 'Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures', Deviant Behavior 28, no. 2: 171-198.

Hom, Andrew R. (2010), 'Hegemonic Metronome: The Ascendancy of Western Standard Time', Review of International Studies 36, no. 4: 1145-1170.

Hom, Andrew R. and Brent J. Steele (2010), 'Open Horizons: The Temporal Visions of Reflexive Realism', International Studies Review 12, no. 2: 271-300.

Hook, Glenn D (1984), 'The Nuclearization of Language: Nuclear Allergy as Political Metaphor', Journal of Peace Research 21, no. 3: 259-275.

Hosein, Ian (2004), 'The Sources of Laws: Policy Dynamics in a Digital and Terrorized World', The Information Society: An International Journal 20, no. 3: 187-199.

Hoskins, Andrew (2006), 'Temporality, Proximity and Security: Terror in a Media-Drenched Age', International Relations 20, no. 4: 453-466.

Hoskins, Andrew (2011), 'Media, Memory, Metaphor: Remembering and the Connective Turn', Parallax 17, no. 4: 19-31.

Hughes, James J. (2012), 'The Politics of Transhumanism and the Techno-Millennial Imagination, 1626-2030', Zygon: Journal of Religion and Science 47, no. 4: 757-776.

Hughes, Rex (2010), 'A Treaty for Cyberspace', International Affairs 86, no. 2: 523-541.

Hundley, Richard O. and Robert H. Anderson (1995), 'Emerging Challenge: Security and Safety in Cyberspace', IEEE Technology & 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.

Hutchings, Kimberly (2007), 'Happy Anniversary! Time and Critique in International Relations Theory', Review of International Studies 33, supplement S1: 71-89.

Huysmans, Jef (1996), 'Security! What Do You Mean? From Concept to Thick Signifier', European Journal of International Relations 4, no. 2: 226-255.

Huysmans, Jef and Claudia Aradau (forthcoming), 'Critical Methods in International Relations: The Politics of Techniques, Devices and Acts', European Journal of International Relations.

Hynek, Nik and David Chandler (2013), 'No Emancipatory Alternative, No Critical Security Studies', Critical Studies on Security 1, no. 1: 46-63.

Iskin, Ruth E. (2003), 'Father Time, Speed, and the Temporality of Posters Around 1900', KronoScope 3, no. 1: 28-50.

Jabri, Vivienne (2006), 'War, Security and the Liberal State', Security Dialogue 37, no. 1: 47-64.

Jarvis, Lee (2008), 'Times of Terror: Writing Temporality into the War on Terror', Critical Studies on Terrorism 1, no. 2: 245-262.

Jordan, Glenn (1995), 'Flight from Modernity: Time, the Other and the Discourse of Primitivism', Time & Society 4, no. 3: 281-303.

Kaika, Maria and Erik Swyngedouw (2000), 'Fetishizing the Modern City: The Phantasmagoria of Urban Technological Networks', International Journal of Urban & Regional Research 24, no. 1: 120-138.

Kamp, Poul-Henning (2011), 'The One-Second War', Communications of the ACM 54, no. 5: 44-48.

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: 660-668.

Kiggins, Ryan David (forthcoming), 'Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era', International Studies Perspectives.

Kincanon, Eric (2004), 'Misuses of Physical Models in Understanding Time', KronoScope 4, no. 1: 70-73.

King, Martin Luther, Jr. (1993), 'Letter from Birmingham Jail', University of California Davis Law Review 26, no. 4: 835-851.

King, Vera (2010), 'The Generational Rivalry for Time', Time & Society 19, no. 1: 54-71.

Kitzinger, Jenny (2000), 'Media Templates: Patterns of Association and the (Re)construction of Meaning Over Time', Media, Culture & Society 22, no. 1: 61-84.

Klein, Olivier (2004), 'Social Perception of Time, Distance and High-Speed Transportation', Time & Society 13, nos. 2-3: 245-263.

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: 171-179.

Klimburg, Alexander (2011), 'Mobilising Cyber Power', Survival 53, no. 1: 41-60.

Klinke, Ian (2013), 'Chronopolitics: A Conceptual Matrix', Progress in Human Geography 37, no. 5: 673-690.

Krahmann, Elke (2008), 'Security: Collective Good or Commodity?', European Journal of International Relations 14, no. 3: 379-404.

Krebs, Ronald R. and Aaron Rapport (2012), 'International Relations and the Psychology of Time Horizons', International Studies Quarterly 56, no. 3: 530-543.

Lake, David A. (2011), 'Why "Isms" are Evil: Theory, Epistemology, and Academic Sects as Impediments to Understanding and Progress', International Studies Quarterly 55, no. 2: 465-480.

Latour, Bruno (2002), 'Morality and Technology: The End of the Means', Theory, Culture & Society 19, nos. 5-6: 247-260.

Lawson, George (2012), 'The Eternal Divide? History and International Relations', European Journal of International Relations 18, no. 2: 203-226.

Lawson, Sean (2011), 'Articulation, Antagonism, and Intercalation in Western Military Imaginaries', Security Dialogue 42, no. 1: 39-56.

Lawson, Sean (2012), '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 (2013), 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats', Journal of Information Technology & Politics 10, no. 1: 86-103.

Lee, Heejin and Jonathan Liebenau (2000), 'Time and the Internet at the Turn of Millennium', Time & 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 & Society 11, no. 8: 1267-1285.

Lewis, James A. (2003), 'Cyber Terror: Missing in Action', Knowledge, Technology & 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: 821-830.

Lewis, James A. (2010), 'Sovereignty and the Role of Government in Cyberspace', Brown Journal of World Affairs 16, no. 2: 55-65.

Little, Richard G. (2002), 'Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures', Journal of Urban Technology 9, no. 1: 109-123.

Lule, Jack (1991), 'Roots of the Space Race: Sputnik and the Language of US News in 1957', Journalism & Mass Communication Quarterly 68, nos. 1-2: 76-86.

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.

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: 470-490.

McFarlane, Colin and Ben Anderson (2011), 'Thinking with Assemblage', Area 43, no. 2: 162-164.

McGoey, Linsey (2012), 'Strategic Unknowns: Towards a Sociology of Ignorance', Economy & Society 41, no. 1: 1-16.

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, 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.

McLaren, Peter (2002), 'George Bush, Apocalypse Sometime Soon, and the American Imperium', Cultural Studies—Critical Methodologies 2, no. 3: 327-333.

McLure, Helen (2000), 'The Wild, Wild Web: The Mythic American West and the Electronic Frontier', The Western Historical Quarterly 31, no. 4: 457-476.

McSorley, Kevin (2012), 'Helmetcams, Militarized Sensation and "Somatic War"', Journal of War & Culture Studies 5, no. 1: 47-58.

McTaggart, J.M.E. (1908), 'The Unreality of Time', Mind: A Quarterly Review of Psychology & Philosophy 17, no. 4: 457-474.

Magee, Clifford S. (2013), 'Awaiting Cyber 9/11', Joint Force Quarterly 70: 76-82.

Malphurs, Ryan (2008), 'The Media's Frontier Construction of President George W. Bush', The Journal of American Culture 31, no. 2: 185-201.

Marcus, George E. and Erkan Saka (2006), 'Assemblage', Theory, Culture & Society 23, nos. 2-3: 101-106.

Martin, Lauren and Stephanie Simon (2008), 'A Formula for Disaster: The Department of Homeland Security's Virtual Ontology', Space & Polity 12, no. 3: 281-296.

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: 349-373.

Masco, Joseph (2008), '"Survival is Your Business": Engineering Ruins and Affect in Nuclear America', Cultural Anthropology 23, no. 2: 361-398.

Massey, Doreen (1992), 'Politics and Space/Time', New Left Review 196: 65-84.

Miller, Donald F. (1993), 'Political Time: The Problem of Timing and Chance', Time & Society 2, no. 2: 179-187.

Mitzen, Jennifer (2006), 'Ontological Security in World Politics', European Journal of International Relations 12, no. 3: 341-370.

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 & Society 10, nos. 2-3: 329-348.

Mythen, Gabe and Sandra Walklate (2008), 'Terrorism, Risk and International Security: The Perils of Asking "What If?", Security Dialogue 39, nos. 2-3: 221-242.

Näf, Michael (2001), 'Ubiquitous Insecurity? How to "Hack" IT Systems', Information & Security 7: 104-118.

Newitz, Annalee and Simon Glezos (2010), 'Digital Inflections: Annalee Newitz in Conversation with Simon Glezos', CTheory, 30 November, http://www.ctheory.net/articles.aspx?id=673.

Nissenbaum, Helen (2004), 'Hackers and the Contested Ontology of Cyberspace', New Media & Society 6, no. 2: 195-217.

Nowotny, Helga (1992), 'Time and Social Theory: Towards a Social Theory of Time', Time & Society 1, no. 3: 421-454.

Onuf, Nicholas (1994), 'The Constitution of International Society', European Journal of International Law 5, no. 1: 1-19.

Ostovich, Steven (2007), 'Carl Schmitt, Political Theology, and Eschatology', KronoScope 7, no. 1: 49-66.

Palmer, Allen W. (2002), 'Negotiation and Resistance in Global Networks: The 1884 International Meridian Conference', Mass Communication & Society 5, no. 1: 7-24.

Parkins, Wendy (2004), 'Out of Time: Fast Subjects and Slow Living', Time & Society 13, nos. 2-3: 363-382.

Pepper, David (2010), 'The Business of SIGINT: The Role of Modern Management in the Transformation of GCHQ', Public Policy & Administration 25, no. 1: 85-97.

Perrow, Charles (1981), 'Normal Accident at Three Mile Island', Society 18, no. 5: 17-26.

Phillips, John (2006), 'Agencement/Assemblage', Theory, Culture & Society 23, nos. 2-3: 108-109.

Pieterse, Jan Nederveen (1993), 'Aesthetics of Power: Time and Body Politics', Third Text 7, no. 22: 33-42.

Pietz, William (1997), 'Death of the Deodand: Accursed Objects and the Money Value of Human Life', RES: Anthropology & Aesthetics 31: 97-108.

Pobojewska, Aldona (2001), 'New Biology—Jakob von Uexküll's Umweltlehre', Semiotica 134, nos. 1-4: 323-339.

Prensky, Marc (2001), 'Digital Natives, Digital Immigrants Part 1', On the Horizon 9. no. 5: 1, 3-6.

Pretorius, Joelien (2008), 'The Security Imaginary: Explaining Military Isomorphism', Security Dialogue 39, no. 1 (2008): 99-120.

Rämö, Hans (1999), 'An Aristotelian Human Time-Space Manifold: From Chronochora to Kairotopos', Time & Society 8, no. 2: 309-328.

Rapoport, David C. (1988), 'Messianic Sanctions for Terror', Comparative Politics 20, no. 2: 195-213.

Rid, Thomas (2012), 'Cyber War Will Not Take Place', Journal of Strategic Studies 35, no. 1: 5-32.

Rid, Thomas (2013), 'More Attacks, Less Violence', Journal of Strategic Studies 36, no. 1: 139-142.

Rid, Thomas and Peter McBurney (2012), 'Cyber-Weapons', The RUSI Journal 157, no. 1: 6-13.

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.

Roberts, Geoffrey (2006), 'History, Theory and the Narrative Turn in IR', Review of International Studies 32, no. 4: 703-714.

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 & Politics 7, nos. 2-3: 241-260.

Ronfeldt, David and John Arquilla (2000), 'From Cyberspace to the Noosphere: Emergence of the Global Mind', New Perspectives Quarterly 17, no. 1: 18-25.

Rosa, Hartmut (2005), 'The Speed of Global Flows and the Pace of Democratic Politics', New Political Science 27, no. 4: 445-459.

Rosenberg, Justin (1994), 'The International Imagination: IR Theory and "Classic Social Analysis"', Millennium: Journal of International Studies 23, no. 1: 85-108.

Ruggie, John Gerard (1975), 'International Responses to Technology: Concepts and Trends', International Organization 29, no. 3: 557-583.

Ruggie, John Gerard (1993), 'Territoriality and Beyond: Problematizing Modernity in International Relations', International Organization 47, no. 1: 139-174.

Saward, Michael (2011), 'Slow Theory: Taking Time Over Transnational Democratic Representation', Ethics & Global Politics 4, no. 1: 1-18.

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: 415-435.

Schaffer, Jonathan (2003), 'Is There a Fundamental Level?', Noûs 37, no. 3: 498-517.

Scherpe, Klaus R. (1986), 'Dramatization and De-dramatization of "the End": The Apocalyptic Consciousness of Modernity and Post-Modernity', tr. Brent O. Peterson, Cultural Critique 5: 95-129.

Schieber, Philip (1987), 'The Wit and Wisdom of Grace Hopper', The OCLC Newsletter 167, n.p., http://www.cs.yale.edu/homes/tap/Files/hopper-wit.html.

Schildkraut, Deborah J. (2002), 'The More Things Change … American Identity and Mass and Elite Responses to 9/11', Political Psychology 23, no. 3: 511-535.

Schneier, Bruce (2013), 'Our New Regimes of Trust', The SciTech Lawyer 9, nos. 3-4, reproduced at http://www.schneier.com/blog/archives/2013/02/our_new_regimes.html.

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: 433-448.

Schroeder, Paul W. (1997), 'History and International Relations Theory', International Security 22, no. 1: 64-74.

Schwaller, Caroline M. (1997), 'Year 2000. A Date with Destiny. Apocalypse as "The End" or as "Revelation"?', Space & Culture 1, no. 2: 37-49.

Sewell, William H., Jr. (1990), 'Collective Violence and Collective Loyalties in France: Why the French Revolution Made a Difference', Politics & Society 18, no. 4: 527-552.

Shameli-Sendi, Alireza, Naser Ezzati-jivan, Masoume Jabbarifar and Michael Dagenais (2012), 'Intrusion Response Systems: Survey and Taxonomy', International Journal of Computer Science & Network Security 12, no. 1: 1-14.

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.

Silander, Daniel, Craig McLean and Don Wallace (2013), 'The Challenges of Information and Communication Technologies for Transnational Efforts at Homeland Security Education', Journal of Applied Security Research 8, no. 1: 80-97.

Sinha, Chris, Vera da Silva Sinha, Jörg Zinken and Wany Sampaio (2011), 'When Time is Not Space: The Social and Linguistic Construction of Time Intervals and Temporal Event Relations in an Amazonian Culture', Language & Cognition 3, no. 1: 137-169.

Skinner, Quentin (1969), 'Meaning and Understanding in the History of Ideas', History & Theory 8, no. 1: 3-53.

Slack, Jennifer Daryl (1984), 'The Information Revolution as Ideology', Media, Culture & Society 6, no. 3: 247-256.

Smith, George (1998), 'An Electronic Pearl Harbor? Not Likely', Issues in Science & 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 & 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.

Stakhanova, Natalia, Samik Basu and Johnny Wong (2007), 'A Taxonomy of Intrusion Response Systems', International Journal of Information & Computer Security 1, nos. 1-2: 169-184.

Star, Susan Leigh (1999), 'The Ethnography of Infrastructure', American Behavioral Scientist 43, no. 3: 377-391.

Stephens, Carlene (1989), '"The Most Reliable Time": William Bond, the New England Railroads, and Time Awareness in 19th-Century America', Technology & Culture 30, no. 1: 1-24.

Stevens, Tim (2012), 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', Contemporary Security Policy 33, no. 1: 148-170.

Stevens, Tim (2013), 'Information Warfare: A Response to Taddeo', Philosophy & Technology 26, no. 2: 221-225.

Stockdale, Liam P.D. (2013), 'Imagined Futures and Exceptional Presents: A Conceptual Critique of "Pre-Emptive Security"', Global Change, Peace & Security 25, no. 2: 141-157.

Stone, Deborah A. (1989), 'Causal Stories and the Formation of Policy Agendas', Political Science Quarterly 104, no. 2: 281-300.

Stronach, Ian, John Clarke and Jo Frankham (forthcoming), 'Economic "Revelations" and the Metaphors of the Meltdown: An Educational Deconstruction', British Educational Research Journal.

Summers, Rita C. (1984), 'An Overview of Computer Security', IBM Systems Journal 23, no. 4: 309-325.

Swedberg, Richard (2011), 'Theorizing in Sociology and Social Science: Turning to the Context of Discovery', Theory & Society 41, no. 1: 1-40.

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 & Human Values 28, no. 4: 483-512.

Tegmark, Max and Nick Bostrom (2005), 'Is a Doomsday Catastrophe Likely?', Nature 438, no. 754: 754.

Teske, Roland J. (2000), 'William of Auvergne on Time and Eternity', Traditio 55: 125-141.

Thierer, Adam (2013), 'Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle', Minnesota Journal of Law, Science & Technology 14, no. 1: 309-386.

Thompson, E.P. (1967), 'Time, Work-Discipline and Industrial Capitalism', Past & Present 38: 56-97.

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 & 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: 140-164.

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 & Society 3, no. 2: 131-149.

Van Loon, Joost (2000), 'Imminent Immanence: The Time-Politics of Speed and the Management of Decline', Time & Society 9, nos. 2-3: 347-353.

Van Wassenhove, Virginie (2009), 'Minding Time in an Amodal Representational Space', Philosophical Transactions of the Royal Society B 364, no. 1525: 1815-1830.

Vaughan-Williams, Nick (2005), 'International Relations and the "Problem of History"', Millennium: Journal of International Studies 34, no. 1: 115-136;

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 & Theory 50, no. 3: 373-389.

Viereck, Peter (1949), 'The Poet in the Machine Age', Journal of the History of Ideas 10, no. 1: 88-103.

Virilio, Paul and John Armitage (1999), 'From Modernism to Hypermodernism and Beyond: An Interview with Paul Virilio', tr. Patrice Riemens, Theory, Culture & Society 16, nos. 5-6: 25-55.

Walker, R.B.J. (1989), 'History and Structure in the Theory of International Relations', Millennium: Journal of International Studies 18, no. 2: 163-183.

Walker, Jeremy and Melinda Cooper (2011), 'Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation', Security Dialogue 42, no. 2: 143-160.

Warner, Michael (2012), 'Cybersecurity: A Pre-History', Intelligence & National Security 27, no. 5: 781-799.

Waugh, Joanne B. (1991), 'Heraclitus: The Postmodern Presocratic?', The Monist 74, no. 4: 605-623.

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: 557-572.

White, Jonathan (2013), 'Thinking Generations', British Journal of Sociology 64, no. 2: 216-247.

Williams, Donald C. (1951), 'The Myth of Passage', The Journal of Philosophy 48, no. 15: 457-472.

Williams, Michael C. (2003), 'Words, Images, Enemies: Securitization and International Politics', International Studies Quarterly 47, no. 4: 511-531.

Williams, Michael C. (2012), 'The New Economy of Security', Global Crime 13, no. 4: 312-319.

Williams, Stewart (2012), 'Rendering the Untimely Event of Disaster Ever Present', Landscape Review 14, no. 2: 86-96.

Wilson, Eric (2012), 'Criminogenic Cyber-Capitalism: Paul Virilio, Simulation, and the Global Financial Crisis', Critical Criminology 20, no. 3: 249-274.

Winner, Langdon (2004), 'Trust and Terror: The Vulnerability of Complex Socio-Technical Systems', Science as Culture 13, no. 2: 155-172.

Wolfers, Arnold (1952), 'National Security as Ambiguous Symbol', Political Science Quarterly 67, no. 4: 481-502.

Wood, Charles Cresson (1987), 'The Human Immune System as an Information Systems Security Reference Model', Computers & Security 6, no. 6: 511-516.

Worth, Aaron (2010), 'Imperial Transmissions: H.G. Wells, 1897-1901', Victorian Studies 53, no. 1: 65-89.

Wright, Stuart A. (1999), 'Anatomy of a Government Massacre: Abuses of Hostage-Barricade Protocols during the Waco Standoff', Terrorism & Political Violence 11, no. 2: 39-68.

Wriston, Walter B. (1997), 'Bits, Bytes, and Diplomacy', Foreign Affairs 76, no. 5: 172-182.

Zerubavel, Eviatar (1987), 'The Language of Time: Toward a Semiotics of Temporality', The Sociological Quarterly 28, no. 3: 343-356.

Zimmerman, Rae (2001), 'Social Implications of Infrastructure Network Interactions', Journal of Urban Technology 8, no. 3: 97-119.

Zurbrugg, Nicholas (1999), 'Virilio, Stelarc and "Terminal" Technoculture', Theory, Culture & Society 16, nos. 5-6: 177-199.

**B4. Conference Papers and Proceedings**

Adam, Barbara (2008), 'Of Timescapes, Futurescapes and Timeprints', paper presented at Lüneberg University, 17 June.

Bell, David Elliott (2005), 'Looking Back at the Bell-LaPadula Model', Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, AZ, 5-9 December 2005, 337-351.

Clarke, Roger (2010), 'Cyborg Rights', 2010 IEEE International Symposium on Technology and Society (ISTAS), 9-22.

Eden, Lynn (1992), 'Learning and Forgetting: The Development of Organizational Knowledge About US Weapons Effects', paper presented at the 1992 American Political Science Association annual meeting, Chicago.

Haack, Jerome N., Glenn A. Fink, Wendy M. Maiden, A. David McKinnon, Steven J. Templeton and Errin W. Fulp (2011), 'Ant-Based Cyber Security', Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations (ITNG 2011), Las Vegas, NV, 11-13 April, 918-926.

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.

Kaminski, Ryan T. (2010), 'Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions', in Conference on Cyber Conflict Proceedings 2010, eds. Christian Czosseck and Karlis Podins (Tallinn: CCD COE Publications), 79-94.

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), 327-342.

Magaziner, Ira (1998), 'Democracy and Cyberspace: First Principles', Democracy and Digital Media Conference, Cambridge, MA, 8 May.

Office of Cyber Security and Information Assurance (2011), presentation, London Conference on Cyberspace, 2 November.

Peters, Bernard (1967), 'Security Considerations in a Multi-Programmed Computer System', Proceedings of the 1967 Spring Joint Computer Conference 30, 283-286.

Sterling, Bruce (2010), 'Atemporality for the Creative Artist', Transmediale 10, Berlin, 6 February, transcript available at http://www.wired.com/beyond_the_beyond/2010/02/atemporality-for-the-creative-artist/.

**B5. Research Reports**

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).

Colbaugh, Richard and Kristin Glass, eds. (2012), Proactive Defense for Evolving Cyber Threats, Sandia Report SAND2012-10177 (Albuquerque, NM: Sandia National Laboratories).

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

e-skills UK (2013), Career Analysis into Cyber Security: New and Evolving Occupations (London: e-skills UK).

Frost and Sullivan (2013), The 2013 $(ISC)^2$ Global Information Security Workforce Study (Mountain View, CA: Frost and Sullivan).

Information Assurance Advisory Council (2012), Record of a Joint IAAC/Cabinet Office Seminar—UK Cyber Security Strategy (Swindon: IAAC).

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).

Microsoft (2012), A National Talent Strategy: Ideas for Securing US Competitiveness and Economic Growth (Redmond, WA: Microsoft Corporation).

Pélissié du Rausas, Matthieu, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui and Rémi Said (2011), Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity (New York: McKinsey Global Institute).

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, eds. Abraham M. Denmark and James Mulvenon (Washington, DC: Center for a New American Security), 139-172.

Vatis, Michael (2002), 'Cyber Attacks: Protecting America's Security Against Digital Threats', ESDP Discussion Paper ESDP-2002-04 (Cambridge, MA: John F. Kennedy School of Government, Harvard University).

**B6. PhD Thesis**

Lévy, Anne Shullenberger (1995), 'America Discovered a Second Time: French Perceptions of American Notions of Time from Tocqueville to Laboulaye', PhD thesis, Yale University.