Apocalyptic Visions: Cyber War and the Politics of Time

Tim Stevens, King’s College London (unpublished essay, 2013)

Abstract

This article contributes to the literature on representations of ‘cyber war’, specifically cyber war as a potential form of inter-state war or strategic terrorism. It argues that cyber war can be examined from a chronopolitical perspective; that is, with a concern for how collective understandings of time and temporality influence political behaviours. This article argues that discourses of strategic cyber war are contingent upon an apocalyptic temporality that is itself an expression of postmodernity. Recent speculation on the likelihood of strategic cyber war constructs it as both imminent and unavoidable, an existential catastrophe which forecloses temporal horizons and brings the future forward as a key driver of politics in the present. Cyber war discourses are interrogated here as forms of ‘catastrophic apocalypticism’, in which cyber war as apocalypse is permanently in abeyance, which facilitates a range of opportunities for the politics of security and the expansion of the national security apparatus.

Keywords
catastrophe; chronopolitics; cyber security; cyber war; international security; postmodernity.
Introduction

In a now notorious op-ed for *The Washington Post*, Mike McConnell, formerly director of both the National Security Agency and of US National Intelligence, told readers: ‘The United States is fighting a cyber-war today, and we are losing. It’s that simple’ (McConnell, 2010). His widely-reported comments were notable both for the hostility they attracted and for their timely re-injection of the ‘cyber war’ concept into the heart of cyber security discourse. As historical studies of cyber security show (Cavelty, 2008; Warner, 2012), war and the military have always been at the core of the dynamic relationship between information technologies and security, not least as modern computers were reared, if not born, in the global emergency of World War II (Ceruzzi, 2003). In the post-war period, the intensive interplay between computers and security became increasingly apparent but the terrorist attacks of 11 September 2001 took these concerns to ‘a new, more complex and heightened level’ (Buzan and Hansen, 2009: 248). McConnell’s comments coincided with a period during which publics worldwide were being re-sensitised to the national security implications of information technologies with substantial media interest in issues previously the preserve of security professionals and computer ‘geeks’ (Guitton, 2013).

Competing concepts of ‘cyber war’ have been around for at least two decades but it was perhaps inevitable, in the sometimes febrile atmosphere of speculation about cyber security events and their societal impacts, that recent evocations of future ‘cyber war’—both dangerous and glamorous—would attract widespread attention. This article contributes to a maturing academic engagement with the nature and character of this phenomenon. It argues that cyber war can be examined from a chronopolitical perspective; that is, with a concern for how collective understandings of time and temporality influence political behaviours (Maier, 1987; Hutchings, 2008; Klinke, 2013). This constructivist perspective holds that our conceptions of time and space shape the stories we tell about reality (Bakhtin, 1981). This article argues that discourses of strategic cyber war are contingent upon an apocalyptic temporality that is itself an expression of postmodernity. Recent speculation on
strategic cyber war constructs it as both imminent and unavoidable, an existential catastrophe which forecloses temporal horizons and brings the future forward as a key driver of politics in the present. In this article, I propose that cyber war discourses represent a form of ‘catastrophic apocalypticism’, in which cyber war as apocalypse is permanently in abeyance, thereby facilitating multiple opportunities for the politics of security and the expansion of the national security apparatus.

Apocalyptic Cyber War

Contemporary discourses of cyber war are notable in the diversity of the conceptualisation and deployment of this term. There has been a widening definition and use of ‘war’ with respect to ‘cyberspace’ in recent years (Cavelty, 2010; Lawson, 2012) and the meaning of war in this context risks degenerating into ‘a mere metaphor’ (Rid, 2012: 7). For present purposes, we can identify at least three principal meanings attributed to and derived from the term, ‘cyber war’.¹ One, an operational mode characterised by state militaries’ tactical use of information and networked information technologies, originally formulated as ‘cyberwar’ by RAND analysts John Arquilla and David Ronfeldt in the early 1990s (Arquilla and Ronfeldt, 1993), although best described as cyber warfare. Two, a generalised notion of societal warfare waged by state and non-state actors through information-technological means. This is war in its metaphorical register, a state of permanent ‘cyber conflict’ (Karatzogianni, 2009) between criminals, ‘black hat’ hackers, protest networks, citizens, hacktivists, terrorists, insurgents and the forces of government and business arrayed against them. This form of ‘cyber war’ is portrayed as a Hobbesian bellum omnium contra omnes, a constant low-level conflict or perpetuall cyber warre of all against all (see also, Arquilla, 2011: 40).

The third category of cyber war is strategic, in which ‘cyber war’ is war like any other war, as understood in international law and convention. This category of cyber war is central to our subsequent discussion: ‘cyber war proper’ is driven by political desires, and information-

¹ For a detailed review of ‘cyberwar’ terminology and typology, see Cavelty (2010). See also: cyberwar as the simulation and virtualisation of war (Virilio, 2005; Der Derian, 2009) and cyberwar as global information deterrence (Virilio, 2000).
technological means are used to force the capitulation of adversaries to one’s will. This category is here taken to include acts of strategic cyber terrorism, should such acts ever come to pass, on the basis that, first, large-scale terrorism may be considered strategic (Neumann and Smith, 2005) and, second, that since 9/11, cyberterrorism on this scale would likely be framed as an act of war eliciting a militarised response. The question of whether any ‘cyber attack’—state or non-state—actually satisfies the criteria of an ‘act of war’ is at the heart of an unresolved debate over the likelihood of cyber war in the academic literature on strategic theory (Rid, 2012, 2013a, b; Stone, 2013).

It is also questionable whether cyber war could constitute the totality of an inter-state war. Cyber operations would probably be part of a military campaign also involving other elements of national military power (Betz and Stevens, 2011; Betz, 2012). Taken together, these issues call into question whether there can exist a pure inter-state cyber war; if it isn’t conducted solely through information-technological—‘cyber’—means, is it not just ‘war’? The alleged Russian military cyber attacks on Georgian information assets in 2008 illustrate this well (Deibert et al, 2012). There was no strategic ‘cyber war’ between Russia and Georgia as commonly claimed but tactical/operational cyber warfare used in conjunction with other Russian military capabilities: in other words, cyber warfare as part of war.

Discourses of cyber security—of which ‘cyber war’ is a distinct subset—are heavily reliant on the articulation of catastrophic ‘cyber doom’ scenarios to mobilise political resources (Cavelty, 2008; Lawson, 2013). Strategic cyber war is also framed in ways prioritising the catastrophic nature of these scenarios, although their nature and character remain poorly understood. In the absence of historical events or processes definitively identified as strategic cyber war, cyber war can only be imagined rather than remembered. Moreover, rather than portraying cyber war as a protracted and heterogeneous process analogous to the unfolding of ‘real’ wars, cyber war is often reduced to a single image or identity, a textual cipher standing in for a more complex phenomenon. One of the
principal ways in which cyber war is imagined is as a cataclysmic and transformative event, which can be understood through the lens of apocalypse. The details of cyber war are described once this initial identity has been established, not before. This deductive rationale identifies cyber war as ‘catastrophic’ or ‘apocalyptic’, with its character inferred from this initial assertion of its nature. This is not to suggest those who promote apocalyptic interpretations of cyber war reached their conclusions in similar fashion—in most cases, the opposite is likely to be true—but this is how cyber war is often presented publicly by a wide range of politicians, policymakers, defence and intelligence personnel, computer security professionals and academics. Cyber war discourses are disseminated through the general intercourse of broadcast and online news media, in popular culture—including films, television, novels—and other elements of the new media ecology (Hoskins and O’Loughlin, 2010). Explicit references to cyber war qua apocalypse are common but what we are seeking to identify is an apocalyptic aesthetic, a way of imagining and thinking cyber war rather than the overt framing of cyber war as apocalypse per se.

In the 1990s, information-technological apocalypse was something unleashed militarily on an adversarial Other. A 1995 Time magazine cover story on ‘cyber war’—in our typology, cyber warfare—drew attention to the ‘new Armageddons’ to be inflicted on America’s enemies through digital military means. The scenarios imagined by military planners resounded ‘with almost Biblical force’ as Washington ‘visits upon the offending tyranny a series of thoroughly modern plagues’ (Waller, 1995). Today, the apocalypse is also within one’s sovereign borders and, consequently, in one’s own time. In the post-9/11 mindset, ‘war’ is something that can happen ‘here’ as well as ‘there’. Strategic cyber war is couched regularly in awkward neologisms drawn from Judaeo-Christian doctrines of the end-times: cybergeddon, cyberarmageddon, cybarmageddon, cyber-apocalypse. A ‘cyber-apocalypse’, suggests one dictionary, is ‘a cyber attack that could wreak havoc on the nation by bringing down critical information infrastructures’ (Schell and Martin, 2006: 78). The scale of such an event ‘would make 9/11 look like a tea party’ (The Economist, 2012).
Cybergeddon is ‘one of the greatest existential threats facing the United States’, writes one senior lawyer in *The New York Times* (Bharara, 2012). Eugene Kaspersky, founder and CEO of information security company Kaspersky Lab, told an audience in Tel Aviv: ‘it will be the end of the world as we know it .... I’m scared, believe me’ (Cohen and Lubell, 2012). Even if few security professionals actually fear ‘cybergeddon’ is imminent (Glenny, 2011)—and many are openly skeptical—this does not detract from a widespread sense of fatalism. The ‘sky is falling’, writes one defence information security professional, albeit ‘very slowly’ (Geers, 2009).

As if to illustrate the truism that ‘all of cyberspace comes to ground somewhere’ (Goodman et al, 2007: 196-197), the sheer physicality of cyber war scenarios contrasts sharply with the ‘virtuality’ and immateriality of the informational component of ‘cyberspace’. Richard Clarke and Robert Knake (2010: 64-68) describe what happens ‘When Cyber Warriors Attack’. As critical information infrastructures fail, aircraft fall from the sky, trains derail, cars crash, gas pipelines explode, chemical plants expel poison gas, financial systems freeze, and satellites spin out of orbit. Food, water and energy distribution falters, citizens panic and, ultimately, the government is unable to maintain control and the social order disintegrates. Even sober commentators suggest that ‘concatenating these sorts of events can trigger the economic and political panic that no recent war has ever brought to an advanced society’ (Bobbitt, 2008: 96).

Although they might not always be couched in explicitly apocalyptic language, these dark futures are often reinterpreted in an apocalyptic light. One reviewer of Clarke and Knake, for example, describes the above scenario as a ‘pithy five-page vision of this coming apocalypse’ (Glenny, 2010). This suggests that the explicit language of apocalypse does manifest in discourse but also that apocalypse acts as an archetypal resource through which to frame strategic cyber war in general. In the following section, we examine in more detail how narratives of strategic cyber war exhibit signs of apocalyptic thought.
Anatomy of an Apocalypse

Apocalyptic thinking is inherently eschatological and interprets history through the prism of finitude: contemporary events are imbued with eschatological meaning and are interpreted as ‘signs’ of impending apocalypse (Robbins and Palmer, 1997: 4-5). The roll-call of signs of cyber war will be familiar: Cuckoo’s Egg, Eligible Receiver, Morris Worm, ILOVEYOU, Code Red, Estonia, Georgia, Conficker, Operation Aurora, Stuxnet, Flame, Duqu, and so on.\(^2\) This litany of signs—although internally heterogeneous—imparts metonymic gravitas to cyber war narratives and fulfils a significant mnemonic function in reminding audiences continually of the seriousness of cyber threats. They become ‘signifiers of the no-longer-future-but-reality of cyber-war’ (Cavelty, 2013). Their historical specificity is elided in their construction as discrete events, the frequency of which is always increasing (e.g. Herrera-Flanigan, 2013), and which lead inevitably to cyber war.

The prophets who read these apocalyptic signs and pronounce upon them—the ‘Cassandras of cyber warfare’ (Rid, 2012: 6)—do not, like their religious counterparts, restrict themselves to specific dates and times upon which terrible events will occur, so have no need to excuse themselves from incorrect predictions; they can never be wrong. However, they do have in common their talents as ‘masterful bricoleurs, skilfully recasting elements and themes within the constraints of their respective traditions and reconfiguring them to formulate new, meaningful endtimes scenarios’ (Wojcik, 1997: 148). The specific vectors of ‘cyber insecurity’ may change, and the timescales expand and contract, but the certainty in apocalypse does not waver. A degree of ‘apocalyptic intensity’ is maintained and can be heightened further by making predictions that are ‘imminent but indeterminate’, legitimising a constant state of readiness in which adherents ‘feel themselves to be standing poised on the brink of time’ (Bromley, 1997: 36). In fact, it is always ‘only a matter of time’ before a ‘cyber-apocalypse’ occurs (Gable, 2010). This uncertainty is shared with other forms of

\(^2\) Although it is not commonly invoked in contemporary cyber war discourses, we might add Y2K to this list, with its own particular apocalyptic connotations (Tapia, 2003).
security, which thrive on a ‘denotative imprecision .... simultaneous appeal to the hard and the vacuous, the precise and the imprecise .... vague generalities about everything and nothing’ (Walker, 1997: 63). The tension inherent in this epistemic polarity is partially resolved in the case of cyber war by reading the signs as corroboration of a deterministic ‘script’ of the future (Robbins and Palmer, 1997: 5). When events and scenarios converge, the narrative of cyber war gains explanatory power in its own right. In periods of ‘thickened history’ like this, it becomes ever more difficult to comprehend these events—‘to see the wood for the trees’, as it were—and they become part of their own causal structure (Beissinger, 2002: 27). In this case, the impression is that if cyber war is not already occurring, it very soon will be.

The initiation of the apocalypse is frequently reduced to the familiar digital motif of a finger hovering above the button or, in this case, positioned in readiness for a final, decisive mouse-click or emphatic keystroke. The former prime minister of Australia provides an excellent example of this symbolic genre: ‘There was a time when war was begun with a shot. Now it can begin with the simple click of a mouse. A silent attack that you may never even know occurred until it all unfolds in front of you’ (Rudd, 2011). During the early Cold War, the image of the US president’s finger poised above a ‘nuclear button’ became the standard symbol of military power available to the commander-in-chief (Strong, 2005: 34) but in an age of cyber war, the power to foment societal chaos is available to all: as UK armed forces minister Nick Harvey warned, ‘the finger hovering over the button could be anyone from a state to a student’ (Hopkins, 2011). The difficulties of representing cyber threats visually (Hansen and Nissenbaum, 2009: 1165) partially explain the popularity of this imagery but like the nuclear case—for which substantial visual resources were available—there is semantic power in this reduction of immense sociotechnical complexity to a simple manual action (Plotnick, 2012). Like the informational bits mediating the human will to prosecute these actions, the decision to proceed is also binary: on/off, yes or no. We might never know who hit us or why but this single
physical act brings the future rushing catastrophically into the present, the moment of ‘cosmic ecstasy’ (Chernus, 1982) in which all apocalyptic predictions are validated.

This suggests apocalypse is also an object of desire, something to be welcomed and, perhaps, brought into being (e.g. Cook, 2004). Although eschatology is concerned with the end-times, apocalypse is not merely the end but also a beginning, a time of both revelation and transformation. An apocalyptic belief in the transformation of the human condition through catastrophe informs the rhetoric of, for instance, the US-led ‘war on terror’ as much as it does the jihadism of those who prompted it (McLaren, 2002; Jackson, 2005: 103-105). This applies even if the utopian ideal of delivering a world free of ‘terror’ is as unlikely as millennial Islam’s dreams of a global caliphate (Gray, 2007). They remain visions no matter how hard one strives to achieve them and are part of a ‘catastrophic’ strand of apocalypticism which pits good against evil and privileges dystopian and pessimistic views of human nature (Wessinger, 1997). Cyber war scenarios frequently express this catastrophic apocalypticism, yet these eventualities are not entirely unwelcomed. Cyber war as apocalypse is ‘an illumination unveiled precisely at the very moment of the greatest darkness and danger’ (Aho, 1997: 65), a light to dispel the night of political foot-dragging and insufficient cyber security. The catastrophic materialisation of the ‘virtual’ threat is the necessary catalyst through which to achieve this transformation. In this respect, apocalypse operates in its primary sense of ‘revelation’, a ‘singular instant both revealing the meaning of the past and announcing the future’ (Bousquet, 2006: 756), in this case the political errors of the past and the sunlit uplands of a ‘cyber secure’ future.

Understood not only as catastrophe but as the moment of revelation and the wellspring of transformation, apocalypse need not be viewed in a wholly negative light. Millennial beliefs in a better future are not exclusive to religion and are amply demonstrated in scientific movements like eugenics, cryonics and space exploration, all of which share a conviction humankind can be
transformed and improved through technology (Bozeman, 1997). The posthumanist movement, specifically in its attention to the coming ‘technological singularity’—the ‘rapture of the nerds’ (Doctorow and Stross, 2012)—is overtly apocalyptic in orientation but also emphasises the positive social benefits an information-technological transformation will bring (DeLashmutt, 2006). The technological singularity may be a violent rupture but not necessarily; it may, some argue, have happened already—we just didn’t notice.3 Apocalypse need not be catastrophic but can be ‘progressive’, affirming collective cooperation in bringing about earthly salvation (‘progress’) without the radical violence of divine retributive justice (Wessinger, 1997). These utopian and transformative impulses are in a long lineage of technoscientific thought, expressing secular rather than religious apocalypticism (Hughes, 2012). We must enquire further how apocalyptic cyber war is located with reference to this spirit of apocalyptic modernity and postmodernity.

**Cyber War and Apocalyptic (Post)modernity**

We might identify in the specific invocation of apocalypse as the omnipresent threat of existential catastrophe a distinct characteristic of postmodernity. Ecological disaster, nuclear cataclysm, population pressure and a range of ‘wicked problems’ (Rittel and Webber, 1973) characterise our contemporary global condition and serve to foreshorten our temporal horizons, altering our relationship with the future. Teleological notions of social progress and the open horizons of ‘positive’ futures are replaced by an ‘extended present’ in which existential concerns about the future shape the present, rather than its converse (Nowotny, 1994: 51). The roots of this sensibility are prehistoric, an epistemic crisis emerging with the separation of man from nature (Lewis, 2012), which expresses itself through religious and, in modernity and postmodernity, secular narratives of apocalypse. From Nietzsche’s ‘death of God’ (Nietzsche, 2001) to the Foucauldian ‘death of man’ (Han-Pile, 2010) and the ‘end of history’ (Fukuyama, 1992), modernity has provided multiple

---

3 This is a common discussion on trans- and posthumanist web forums and blogs. This issue is also raised with respect to cyber war: ‘what if we were at war and didn’t know it?’ (Brenner, 2009: 100).
apocalyptic (and often misunderstood) pronouncements which announce the end of the order of modernity and the birth of a ‘postmodernity’ itself.

In 1902, the English writer and social commentator, H.G. Wells, addressing the Royal Institution, advocated the application of the scientific imagination to the problems of futurity. Specifically, he wished to dispel an impression of the future as ‘a perpetual source of convulsive surprises, as an impenetrable blankness’ (Wells, 1913: 21), into which we project our dark fantasies and cultural forebodings. As a science fiction author, Wells might be impressed at the role the genre now plays in thinking imaginatively about futurity and security: imagination has become a formal resource, mobilised to generate security knowledge and to ‘dispel secrecy and ignorance, compute risk and uncertainty, and prepare for surprise and novelty’ (Aradau and van Munster, 2011: 69-70). Wells might be less sanguine about the scenarios conjured up by this process, however. Whilst acknowledging that science fiction can provide planners with useful creative frameworks for thinking about cyber security (Jagoda, 2012: 25), it also frequently casts technology ‘in a bad light’ (Silomon and Overill, 2012: 15). Formally and informally, cyber war scenarios are, as a result of an historical paucity of comparable events, necessarily imagined, and they ‘remain fiction, not to say science fiction’ (Rid, 2013a: 4). In common with the science-fictional leanings of contemporary security futurism generally, these predictions are distinctly dystopian and ‘often very grim indeed’ (Carr, 2010: 18).

What happened to the positive social futurism conjured up by the science-fictional imagination at the beginning of the last century? According to Richard Overy, British intellectual culture was deeply affected by the cataclysm of World War I, which leached Victorian optimism and faith in social progress from the bones of a tired nation (Overy, 2009). Furthermore, this ‘domestic malaise’ was deepened by uncertainties about species survival, economic security and the fear of political extremism in a time of civilisational crisis, a dystopian atmosphere which so sensitised the British
public that the ‘escape into war’ in 1939 was an apocalyptic release (Overy, 2009: 384). After Operation Barbarossa and, in the public imagination, El Alamein (Weinberg, 1994: 489), Western citizens began to look forward to a world free of tyranny, an outlook that gradually soured as superpower enmity ossified in the Cold War, a metaphor which ‘[packed] together anxieties so intense that it had the power to represent and to create a whole world’ (Gregory, 1989: 12). In a world of superpower chest-beating and one-upmanship, the spectre of nuclear apocalypse understandably altered people’s expectations of the future. Subsequent knowledge of our precarious ecological condition has served to consolidate and accentuate feelings of impending catastrophe, mobilised through apocalyptic imaginaries in discourses of climate change and environmental degradation (Swyngedouw, 2010). Existential uncertainty mediated through the cultural construct of ‘apocalypse’ foments the revelation that breaks open the illusion of social progress and the Enlightenment telos.

Eschatological discourses of cyber war are perhaps symptomatic of this apocalyptic aesthetic but they also derive from a long-standing antipathy or ambivalence to the sociopolitical effects of technology. As scholars of the social construction of cyber security threats have observed, concerns about information technology are older than we sometimes recognise (Cavelty, 2008; Lawson, 2012, 2013), even if they have taken on an urgency hitherto unprecedented in its global intensity. Disquiet about the ‘information revolution’ and its supposed benefits has, even before the last two decades of massive Internet growth, raised critical questions about the political basis of such claims (Webster and Robins, 1986) and identified the constraining logics instantiated by the ideology of the information revolution itself (Slack, 1984). More radically still, enthusiasts for information technology by their own admission sit cheek-by-jowl (Kelly, 2010) with neo-Luddites (Kaczynski, 1995) as proponents of neo-vitalist interpretations of technology as possessive of its own autogenerative ‘life force’. Under these conditions, in which technology is self-perpetuating, autonomous and somehow ‘out-of-control’ (Winner, 1977), and in which technology is implicated in a wide range
of social problems, it is a small step to concluding it is ‘a frequent circumstance of history that a culture or civilization develops the device that will later be used for its destruction’ (Woodcock, 1977: 133).

The weaponisation and attempted civilian control of nuclear energy brought with it the concept of the nuclear ‘accident’, the unavoidable catastrophe ‘normal’ to any given technology (Perrow, 1999). To ‘invent the train is to invent derailment; to invent the ship is to invent the shipwreck’ (Virilio and Der Derian, 1998: 20), and to invent the nuclear power station is to invent Three Mile Island, Chernobyl and Fukushima: the accident is the ontology of technologised society. The nuclear meltdown is qualitatively different, however, from the information accident, which substitutes interactivity for radioactivity (Virilio, 1997: 70). In the global information-technological assemblage the accident becomes not ‘local’, like the reactor or the bomb, but ‘general’ in its effects, which are ‘integral’ to large-scale sociotechnical systems (Virilio, 2007). The ‘global financial crisis’ exemplifies this integral accident, which Virilio ascribes to the highly-interconnected and automated trading systems of global financial networks (Crosthwaite, 2011). The immanence of the accident to postmodernity is, in Virilio’s hands, an explicitly eschatological dimension of the apocalypse of technology itself (Virilio, 2007: 24).

Viewed in the light of the accident, strategic cyber war appears immanent to our contemporary ‘wired’ world. All cyber war discourses stress that the vulnerability of modern societies increases as their dependency on information technologies intensifies. This dependence is not only practical, in terms of delivering services and goods, but psychological and political. The hypothetical ‘cascading failures’ catalysed by infrastructural subversion and destruction (Little, 2002) begin by revealing the materiality and functionality of ‘invisible’ yet physical information infrastructures (Dodge and Kitchin, 2004). This is followed by secondary failures of contingent sociotechnical networks like water, energy, transport and emergency response, which continue to cascade through the affective
realm of corporeal and psychological stress, before undermining completely the collective imaginary that is society. As in the global financial crisis, the accident/apocalypse is characterised by the ‘instant and simultaneous globalisation of affects and fears’ (Virilio et al, 2008).

There is little evidence that cascading failures are likely to happen, or that cyber war will reach the level of a global accident. There is no firm indication that a cyber attack of any kind has caused physical damage on this scale, let alone human deaths (Rid, 2013a). This may, of course, change in time. One might object that the version of cyber war presented here is constructed between human adversaries rather than between humankind and its technologies but this would be to forget the interconnectedness and interdependence of the sociotechnical infrastructures of postmodernity. So unpredictable are they, we cannot know if the effects of cyber war would be restricted to the target systems alone, or would spread beyond them and potentially back across one’s own borders. This ‘blowback’ effect would diminish the strategic utility of these operations to high-tech societies, including most of those with the capacity to launch an attack in the first place (Feaver, 1998; Rathmell, 2003). There is no guarantee an act of cyber war would not cause a global accident and this thought leads once again to imagining cyber war as potential apocalypse. What, however, are the political implications of these apocalyptic visions: what political ‘work’ does the framing of cyber war as apocalypse perform in the present?

**Chronopolitics of Cyber War**

Due to the lack of precedents, appeals are often made to catastrophic historical events to analogue the possible effects of future cyber war—Pearl Harbor, 9/11, Katrina, and so on. These historical analogies serve as proxies for foundational events in other fields of security, as does Hiroshima in the nuclear case, for example (Hansen and Nissenbaum, 2009: 1164). In this context, nuclear and ‘cyber’ are occasionally explicitly linked: ‘Stuxnet is the Hiroshima of cyber-war’ (Gross, 2011). Commentators often draw attention to the inaccuracies of these historical analogies but pay rather less attention to their political implications. The principal outcome of Pearl Harbor, for instance, was
to jolt the United States into a global war: ‘a threat that had been sketchy, abstract, and distant
became personal and immediate’ and its principal effects were in ‘policy, law, and national
commitment to respond to a recognizable threat’ (Cebrowski, 1998). This dynamic is transferred to
the field of cyber security, in which a catastrophic event—an act of cyber war—is required to spur
government into appropriate action (Bliss, 2010; Goldsmith and Hathaway, 2010). Critical scholars
also invest in the catastrophic event the power to shock the private sector into accepting a greater
role for government in cyber security (Bendrath, 2001). The maintenance of a low level of fear and
concern may also desensitise audiences to the trauma of the catastrophe when and if it finally
arrives (Grusin, 2010), although this does not detract from the construction of cyber war as a
catalyst for political action.

Cyber war is therefore both necessary and in some sense desired. Whether transformative cyber war
can be brought about by apocalyptic discourses alone is unknown but the potentially self-fulfilling
aspect of cyber war discourse is summarised by Ron Deibert: ‘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’ (Deibert, 2012: 261). ‘Like the monsters in your imagination’, writes
former White House cyber security advisor Howard Schmidt, ‘these phantoms can take on a persona
of an unrelenting danger that easily surpasses their true capabilities’ (Schmidt, 2006: 174). In
contrast to apocalyptic environmental discourses, however, in which there is quite literally no long-
term future and therefore no hope (Swyngedouw, 2010, 2013), cyber war apocalypses are not
characterised by pure negativity and still offer redemption through cyber security measures in line
with the desires of capital and the national security state. Of course, it is precisely those who nurture
fear of apocalypse that promise salvation the most and will, ultimately, they hope, be in a position to
deliver it (Swyngedouw, 2013).
Cyber war may be immanent to postmodernity but immanence does not tell us when cyber war will occur, for which we require a more active intimation of tense than such vague futurity provides.

Cyber war discourses, however, do not do this. Cyber war may be immanent but it is also perpetually in abeyance. The existential aspects of cyber war are comparable in some respects to environmental discourses, particularly in their emphasis on catastrophe rather than crisis (Aradau and van Munster, 2011) and in their irreversibility (Hansen and Nissenbaum, 2009). They differ in that cyber threats gain their potency from cascading failures developing rapidly from originary stimuli, in contrast to the gradual accumulation of environmental security issues to a threshold beyond which the frequency of significant events accelerates markedly. This difference ‘establishes different modalities of urgency and hence different spaces for political intervention’ (Hansen and Nissenbaum, 2009: 1164). Cyber security presents a strong sense of temporality in ‘cyber-doom’ scenarios ‘constructed as inevitable and imminent but perpetually postponed’, thus ignoring increasingly extensive and visible cyber security measures (Barnard-Wills and Ashenden, 2012: 9). As strategic cyber war is currently a speculative concept only, so narratives of cyber war fulfil precisely this political function, particularly in furthering the allocation of resources to companies and institutions charged with cyber security and the prevention and prosecution of cyber war (e.g. BBC News, 2013), whilst also stressing the need for more security to postpone the inevitable.

Michael Dillon identifies the centrality of eschatology to the politics of security more generally. This is ‘politics thought in the light of last things’, which articulate both a sense of ending and of ‘ends’—as in aims and desires—but also the beginning of a new politics (Dillon, 1996: 31). Cyber war read as apocalypse marks the birth of a new cyber security future in which political order is transformed into one that takes full account of the exigencies of cyber security. But this future is not post-apocalypse—the ‘catastrophic threat-event of the dissolution of the temporal order of things’ (Dillon, 2011: 782)—but pre-apocalypse. Indeed, the central task of the politics of security is to constantly defer the apocalypse so that the future becomes not the infinity of Christian heaven (on
earth, or otherwise) but a circumscribed—finite—future of infinite possibilities for the workings of politics and security (Dillon, 2011). The temporal distance between now and the apocalypse—situated at the secular ‘limit’ of time, rather than the religious ‘end’ of time—must be maintained, a project for which energy and resources are required. The constant deferral of apocalyptic cyber war may be a product of this project and in the gap between present and apocalypse the cyber security project can be reworked in perpetuity. Although the future constantly threatens to irrupt into the present, the future never arrives.

**Conclusion**

This article has not attempted to determine whether or not strategic ‘cyber war’ will happen, or within what timescale. ‘Is it possible for one of these events to happen? Sure. Is it likely? Absolutely not’ (Schmidt 2006: 172). If the odds of such an event occurring are so small, it is arguably more important that resources are focused on less spectacular cyber security issues—crime, espionage, sabotage—from which cyber war is an unwelcome distraction (Lewis, 2005; Lawson, 2012, 2013; Guitton, 2013). Given that strategic cyber war may even be a theoretical impossibility, the odds that cyber war *qua* war will take place vanish to zero. This does not exclude the possibility that large-scale disruptive and destructive events may occur which look very similar to the phenomena currently described as cyber war but such scenarios presently reside in the minds of the prophets of ‘cyber-doom’ and those who believe them. Apocalypse is a discursive means to frame cyber war that mobilises deep cultural resources but apocalyptic cyber war is also an unconscious expression of apocalyptic postmodernity.⁴ Clearly, apocalyptic thinking can be discerned in *non-* war cyber security contexts too, although we must imagine that if an adversarial action is raised to the hypothetical level of apocalypse it will probably also be of sufficient magnitude to qualify as an act of war.

---

⁴ It is argued elsewhere that ‘an apocalyptic necro-realism is the dominant mode of representation of our times’ (Dawson, 2013).
We might alternatively enquire if the prophets of cyber war will be ‘on the right side of history’ (Rid, 2013a: xiv). We do not know, but we might consider the response of Primo Levi, when asked why we should not peer too far into the future: ‘Because it is almost impossible to distinguish a true prophet from a false one. They sound exactly the same’ (Levi and Di Caro, 2001: 174). We should not necessarily turn deaf ears to all prophets of cyber war but this does remind us, as in the case of climate change, in which apocalyptic thinking is perhaps easier to sustain and identify, that apocalyptic logic is characterised by an ‘anti-epistemology—the impossibility of knowing’ and a state of ‘systematic ignorance’ (Methmann and Rothe, 2012: 330). In this light, all cyber war prophecies begin to sound hysterical when they portend cataclysms with a tenuous claim on the existential. We might accuse speculative futurism of hype or exaggeration—in marketing jargon, the promotion of fear, uncertainty and doubt (FUD)—but we should also accept that ignoring these warnings is fraught with its own risks (Hansen and Nissenbaum, 2009: 1164). If cyber war does have the undesirable qualities attributed to it, we should perhaps hope it ‘remains science fiction for a while longer’ (Cavelty, 2010: 139). However, the final, destructive event that wakes the state from its somnambular inattention to reality is constantly deferred: it is inevitable but always imminent. To play, as so many others have done before, upon the title of Arquilla and Ronfeldt’s original article: cyber war is always coming!

References


BBC News (2013) US Cyber Command in ‘fivefold’ staff expansion, 28 January,


Rudd K (2011) Just a mouse click away from war. The Daily Telegraph (Australia), 19 September.


*The Economist* (2012) Hype and fear. 8 December.


