Analogical Reasoning and Cyber Security

Published as David J. Betz and Tim Stevens (2013), 'Analogical Reasoning and Cyber Security', *Security Dialogue* 44, no. 2: 147-164.

David J. Betz

Department of War Studies, King's College London, UK

Tim Stevens

Department of War Studies, King's College London, UK

Abstract:

This article is an attempt to interrogate some of the predominant analogical reasoning in cyber security discourse, with a view to clarifying its unstated premises, major strengths and, vitally, points of conceptual failure. It aims to improve dialogue between and across the various epistemic communities involved with cyber security policy. As we adapt to the new security realities of the information age it is incumbent upon scholars and strategists to address the benefits of connectivity, in all its dimensions, as much as the threats it presents. Current cyber security discourse channels us into a winner-takes-all modality that is neither desirable nor necessary in the current strategic reality.

Keywords:

international security, security, violence, war, cyber security, cyberwar, cyberspace

Introduction

While wrestling with the complexities of cyber security, the use of analogical reasoning and metaphor is central to policymakers and their advisers' attempts to comprehend the present and plan for the future. This article interrogates such reasoning in order to improve the security dialogue between and across the various epistemic communities involved with cyber policy, practice and research. Our key conceptual frame is Libicki's (2007: 236–240) model of cyberspace, which posits three layers: the 'physical' substrate of computers themselves; the 'syntactic' layer of software and protocols; and the 'semantic' layer of information and ideas. Within this frame, we evaluate two dominant cyber-security analogies – spatial and biological – highlighting the origin, evolution, common usage, and strengths and weaknesses in each case. We conclude that while these analogies have utility, they also have their limits, with non-trivial implications for cyber-security policy and practice.

'Getting cyber right'[1]

Conceptual imprecision afflicts cyber security. A participant at one of the workshops upon which this article is partially based – a veteran of policy debates on how to counter the proliferation of weapons of mass destruction – warned from experience that 'the more inclusive the concept is regarding the domain, the harder it will be to identify what policy is, or should be, surrounding cyberspace'.[2] This basic tension is a recurring theme in the cyber-security strategies of most countries that have attempted to formalize them (Betz and Stevens, 2011: 36). Different research communities must communicate effectively to further

objectives and to engender meaningful dialogue between professionals and policymakers. Yet, there is little consensus on the meanings of concepts like 'cyber security' and 'cyberspace', despite attempts to develop common vocabularies (see, for example, Rauscher and Yaschenko, 2011). And, reporting on cyber security has at times foundered on mistranslation and misrepresentation. Threat inflation – typically using analogies such as the Pearl Harbor or 9/11 attacks or some other 'cyber doom' scenario tapping into national historical consciousness – has been used to 'add urgency' to calls for action (Dunn Cavelty, 2008; see also Lawson, forthcoming; Conway, 2008). This is 'unhelpful and dangerous' (Brito and Watkins, 2011: 38; see also Stohl, 2006). We must be wary of the way in which cyber-security discourse structures our thinking, channelling it into modalities that are misleading. The appropriate use of analogical reasoning should therefore be a priority for those involved in cyber security.

Analogies and metaphors

An analogy is a linguistic device for transferring meaning from one subject to another. With, say, a 'digital 9/11', the intent is to transfer various meanings related to 9/11 (e.g. urban catastrophe, invasion of 'the homeland', violation of the previously inviolate) as well as the political reactions such an act might elicit (see, for example, Jackson, 2005). A metaphor is a specific form of analogy, in which the case is made that one entity can be understood in terms of another. Metaphors are a common constituent of language, either in their obvious forms as deliberate or novel constructions, or as 'dead metaphors', phrases that through age and ubiquity have passed into common usage (Lakoff, 1987). One influential theory of metaphor holds that 'conceptual metaphors' are, in a primal sense, 'metaphors we live by',

which shape not only the content of our communications but also the ways in which we think and act (Lakoff and Johnson, 1980). Metaphors may therefore be powerful influences, catalysing 'groupthink' and bringing about undesirable eventualities – self-fulfilling prophecies, perhaps – as a result of their constitutive role in human thought.[3]

The 'linguistic turn' in philosophy has been the subject of debate and consternation within the social sciences for over a generation (Ball, 1994). The argument (Wittgenstein, 2009; Gadamer, 1989) that the language in which they are expressed irremediably binds our ideas of the world inspired scholars across a range of disciplines to attempt to understand various social phenomena through discourse analysis. International relations embraced the linguistic turn too sharply in the view of some scholars who have led efforts to define a progressive research programme that takes account not only of metaphor and narrative but also of their interrelation with practice (Neumann, 2002), often through the elevation of culture as a more central object of analysis (Farrell, 2002). Our approach in this article is broadly in accordance with the methodological approach of Farrell and Neumann, and is premised on the fact that, though rich in metaphor, cyber-security discourse has not been subject to such analysis, with a few partial exceptions. This hampers attempts to comprehend the present and plan for the future. As Libicki (1997: 6) warns, 'to use metaphor in place of analysis verges on intellectual abuse'; it is imperative that we avoid a situation in which analysts are 'apt to make their metaphors do their thinking for them'.

We may make further observations on the utility of metaphors and analogies, as well as the levels on which they operate. On one level, they have emotional utility according to the degree to which they resonate with possibly unconscious sentiment and preconceptions

that may be manipulated (Ferrari, 2007). A common function of cyber-security discourse is the inducement of fear. In February 2010, for example, CNN broadcast 'Cyber ShockWave', a live simulation of a devastating cyber attack on the United States. The title sequence informed viewers, 'We were warned', as if to leave people in no doubt as to the consequences of failing to secure this new environment (Bipartisan Policy Center, 2010). Similarly, a July 2010 issue of *The Economist* was titled 'Cyberwar: The threat from the Internet', its cover showing a pixelated mushroom cloud towering above a modern city. Such striking visual metaphor is all too common in the print and online media.

Recourse to Cold War concepts and constructs, martial analogies, and in particular the spectre of nuclear holocaust has been noted elsewhere in relation to cyber-security discourse, and deemed counterproductive (Singer and Shachtman, 2011). We should not be surprised at its persistence, given that the Cold War can itself be interpreted as a metaphor, one that 'encompassed a dazzlingly intricate set of assumptions, packing together anxieties so intense that it had the power both to represent and to create a whole world' (Gregory, 1989: 12). The continued use of the Cold War metaphor illustrates that much political discourse intends not to introduce new metaphors but to repeat ones that resonate with opinions already held. This results in the 'dulling' of critical faculties, rather than their 'awakening', with implications for the ability to mobilize support and implement policy and legislation (Edelman, 1964: 124–125).

Some cyber-security metaphors, like computer 'viruses' and 'Trojan' malware, have currency because of their ability to describe behaviour witnessed in the online world. These devices also have utility in commercial, political and bureaucratic terms. For example, air

forces describe ‘cyberspace’ as an environment in which one may ‘fly, fight, and win’ in the quest for cyber ‘dominance’ and ‘superiority’, in ways analogous to these actions in air and space.[4] Not infrequently, such claims are paired with arguments that air forces are uniquely suited to taking charge in ‘air, space, and cyberspace’ because of their traditional high-technology capabilities and putatively more ‘strategic’ mindset (see, for example, Hayden, 2008). That these are motivated by the desire to make political claims on responsibility and resources is self-evident.

Analogies and metaphors usually represent admixtures of emotional and instrumental utility. The same words may, of course, be used in different ways and in different contexts, and be received differently by different audiences. In the fields of security, therefore, the ‘choice of a metaphor carries with it implications about contents, causes, expectations, norms, and strategic choices’ (Bobrow, 1996: 436). Metaphors serve to shape discourse and become the premises on which decisions are made. In a very real sense, metaphors play a central role in ‘structuring political reality for manipulative purposes’ (Hook, 1984: 259).

Spatial analogies

The ‘ur-metaphor’ in cyber security is that of cyberspace itself, a spatial metaphor with many variants. These include the poetic, such as Bruce Sterling’s (1992: i) cyberspace as the ‘place between the phones’. We also find William Gibson’s (1984: 51) visually surreal description of cyberspace as a ‘consensual hallucination.... Lines of light ranged in the nonspace of the mind’. Gibson described a dimly apprehended near-future digital world he sensed emerging in the nascent computer networks and hacking subculture of the early

1980s. These views of cyberspace are ‘exclusive’ in that they treat cyberspace as a virtual environment separate from the ‘real’ world, whose integument is demarcated by its physical infrastructure but which excludes these material components from its definition. Cyberspace is not a space in any traditional sense, therefore, but we experience it as though it possesses physical attributes, if only by association and analogy.

However, the idea of cyberspace as a space separate from ‘real space’ is false, according to one well regarded account:

> Cyberspace is in and of the real-space world, and is so not (only) because real-space sovereigns decree it, or (only) because cyberspace sovereigns can exert physical power over real-space users, but also and more fundamentally because cyberspace users are situated in real-space. (Cohen, 1987: 217–218)

Some activists and scholars of cyberspace have made significant steps in changing the ‘cyberspace as a space apart from real-space’ paradigm. Internet pioneers such as John Perry Barlow (2006), who once earnestly declared the ‘independence of cyberspace’ and the emerging cyber-utopian ‘civilisation of the mind’, subsequently moderated their earlier views. Gibson himself would later confess that cyberspace was merely an ‘effective buzzword ... evocative and essentially meaningless’ (Neale, 2000). Even as the social sciences, though, have largely moved away from using cyberspace as an analytical term (Rogers, 2010), it remains fashionable in political discourse. Arguably, this allows for the maintenance of ‘cyberspace’ as a realm apart from the ‘real’ and thus as an environment of threat in need of remediation (Barnard-Wills and Ashenden, 2012).

This prompts us to wonder, though, what the 'cyber' prefix actually contributes to security discourse that is not conveyed more transparently by the words 'computer network'. A more 'inclusive' conception of cyberspace, therefore, encompasses its physical infrastructure and also the 'embodied, situated experience' of cyberspace users (Cohen, 2007: 213). This places society in the centre of frame as the primary object of security efforts, and recognizes the quotidian practices of citizens in this digital environment. However, if cyber security is contingent upon such an 'inclusive' concept of cyberspace, it becomes practically very difficult to determine what cyber security is not, because the demarcation between cyberspace and 'real' space is so ambiguous. Methodologically, this does allow for greater consideration of the role of material artefacts in relations of power and security (Deibert, 2003; Aradau, 2010), but it poses problems for defining cyber security other than as a form of security concerned with anyone or anything associated, however tenuously, with computer networks. This is the perspective favoured by Western governments – the UK, for example, defining cyberspace as 'an interactive domain of digital networks' spread across the world (Cabinet Office, 2011: 11).

Since the early 1990s, there has been extensive discussion of the impact of information and communications technology (ICT) on warfare, from which emerged the idea of 'strategic information warfare', even if it is still quite difficult to determine exactly what this might be.[5] In the mid-1990s, Libicki (1995: 91) described it as a 'lumpy stew' comprising at least half a dozen portmanteau war types to which subsequently have been added popular new variants, including 'network-centric warfare', 'hybrid warfare', 'unrestricted warfare' and 'fourth-generation warfare'.[6] All of these employ some conception of information 'as a

weapon' in and of itself or as 'force multiplier', but they vary widely in operational concept. Some consider targeting computer network infrastructures, either on their own or as part of a combined arms package, in order to degrade an enemy's command and control capabilities – that is, attacking cyberspace 'as a network'.[7] Others entertain the use of 'all available networks', including terrorism, to target the enemy's political will, using cyberspace as a conduit of ideational or semantic attack (Hammes, 2005; Liang and Xiangsui, 1999). Still others imply both concepts without working through the details or modes of interaction with other arms (Hoffman, 2007). The ambiguity of cyberspace in military thinking is evident in the US Department of Defense's (2010: 37) jargon-heavy definition of cyberspace as 'a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures'. This formulation raises more questions than it answers. What is a 'global domain' (another metaphor)? And, if this refers to cyberspace, what is the 'information environment' in which it is embedded? Superficially, the 'information environment' would seem to consist of hardware and software – the physical (computers, cables, etc.) and syntactic (software, protocols, etc.) layers of cyberspace. Yet, in doctrine and field manuals, the term is actually employed as an approximation of 'public opinion' or mood, in general or on a specific subject (Brunner and Cavelty, 2009). The US Counterinsurgency Field Manual, for instance, asserts:

> The information environment is a critical dimension [of insurgency] and insurgents attempt to shape it to their advantage ... by carrying out activities, such as suicide attacks, that have little military value but ... are executed to attract high-profile media coverage ... and inflate perceptions of insurgent capabilities. (US Department of the Army, 2007: Section I-2)

We would conclude that the exclusive model of cyberspace informs the formal definition of the information environment, but that the inclusive model is used in practice. Notwithstanding these issues, the spatial metaphor of cyberspace also has some significant strengths. One of the most important of these is that it appeals to our intuitive sense of place. Despite its limitations,

> The cyberspace metaphor is neither an arbitrary fiction that can be jettisoned nor a description of some fixed, external reality, but rather an inevitable perceptual by-product of the human cognitive apparatus.... The commitment to spatiality runs far deeper than mere politics or intellectual fashion.(Cohen, 2007: 234)

It is also effective didactically for policymakers and practitioners as a simile, one that draws connections between events and processes of the past and those of the current 'information society'. Britain's 2010 national security strategy, for instance, draws upon the country's self-image as an entrepôt nation with disproportionate influence on account of its geographic position and maritime orientation. The UK, it states, 'is at the heart of many global networks, has an outward-looking disposition and is both a geographical and virtual centre of global activity' (HM Government, 2010: 21). For politicians concerned with encouraging a 'knowledge economy' dependent upon secured intellectual property, financial services and electronic commerce, it makes sense to regard cyberspace as something like the sea in the age of sail. There are echoes of this in the controversy surrounding the proposed US Stop Online Piracy Act, which has aroused significant resistance from entities like Wikipedia, which argued it could 'fatally damage the free and

open Internet' (BBC News, 2012). Site-blocking by governments is widely regarded as illiberal, but the awkward reality for 21st-century 'knowledge economies' is that if they cannot prevent the plundering of their creative industries in and through cyberspace it is not clear how they can prosper (Orlowski, 2012).

Viewing cyberspace as a domain of the 'global commons' alongside the oceans, air, space and the Antarctic landmass – 'resource domains that do not fall within the jurisdiction of any one country' (Buck, 1998: 5–6) – leads to some useful comparative insights. It is undoubtedly a major part of the 'connective tissue of the international system' (US Department of Defense, 2010: 8; see also Rattray et al., 2010), but this conceptualization is also potentially misleading. Uniquely among domains, cyberspace is man-made and has various unusual properties as a result. For one, the 'geography' of cyberspace is mutable: its hardware can be switched off or destroyed, deliberately or accidentally. Similarly, its software can be altered, allowing actions that were once precluded or vice versa. Fundamentally, it is a construct, and accordingly 'there is little hard-and-fast physics of the sort that dictates what can and cannot be done in, say, outer space' (Libicki, 2007: 6). Also, cyberspace is not really held in the common weal; on the contrary, some person, company or country owns every part of its physical layer. These systems lie within the boundaries of states, which may exercise sovereign authority over them. Moreover, given an inclusive view of cyberspace, in which social relations are as much a part of the socio-technical assemblage as hardware and software, we must consider that the boundaries of 'cyberspace' extend into human brains, where individual thoughts, perceptions and consciousness reside. These differences suggest that cyberspace possesses none of the legal or logical criteria of a commons (Franzese, 2009).

Paradoxically, though, it is a spatial metaphor (of a sort) that predominates in social scientific analyses of cyberspace, in which cyberspace represents a radical expansion of the 'public sphere' (Habermas, 1991). Cyberspace becomes a place in which ideas are formed, jostle against each other, and begin to coalesce or synthesize in societal opinions on matters of the day (Rheingold, 1993). Importantly for considerations of cyber security, in this global electronic agora, 'the diversity of human disaffection explodes in a cacophony of accents' (Castells, 2001: 138).[8] Cyber security has traditionally been more concerned with 'attacks' on computer systems, for purposes of espionage, sabotage or crime or in hypothetical 'cyberwars' (Rid, 2012). The overlap of cyber security with new forms of social movements, political contestation and 'hacktivism' has received considerably less attention from scholars. This is also true of practitioners:

> Our initial assessment of the hacker threat was wrong. Initially, states envisaged defending themselves against other states because they were seen as the main threats, whereas 'hacktivists' were not perceived to be as dangerous. In hindsight, that assessment was wrong. Non-state hacking is much nearer the top of the threat.[9]

Some of the more interesting research on information-age security focuses on anti-status quo, nonstate or quasi-non-state actors using digital connectivity to increase radically their ability to enact power on the international stage through hacking, propaganda and propaganda by deed (Jordan and Taylor, 2004; Karatzogianni, 2009; Bolt et al., 2008). Scholars have also noted how insurgents use cyberspace as a place – a 'sanctuary' – to raise the visibility of their attacks, recruit, train, proselytize, finance operations and organize

themselves in networked forms that are hard to affect with the kinetic blows of conventional campaigns (Betz, 2008; Brachman and Forest, 2007; Jones and Smith, 2005). Other globally networked social movements (other, that is, than the Islamist terror groups that have dominated recent research agendas) employ similar strategies of using cyberspace for the mobilization of contention (not necessarily violent) in support of diverse causes (Lievrouw, 2011; Pickerill, 2003; Rheingold, 2002; Starhawk, 2002). Some of these, notably the Internet group Anonymous, have experimented with new forms of digital coercion not deployed on this scale before (Betz and Stevens, 2011: 114–127). Arguably, these developments should be more prominent in the cyber-security debate. If one takes an inclusive view of cyberspace, then they must be treated more prominently. The attacks of 11 September 2001, the 2004 Madrid and 2005 London bombings, the 2008 Mumbai attacks, many aspects of the decade-long campaigns in Afghanistan and Iraq, are all instances of cyberspace 'touching ground' (Goodman et al., 2007: 197). Indeed, the concept of 'global insurgency' that has caused great anxiety in security communities makes little sense without the dense web of interconnectivity that is cyberspace (Kilcullen, 2009; Mackinlay, 2009).

Investigations of the interactions of cyberspace and real-space are driving a convergence of media and cultural studies with war and strategic studies – an intriguing and important development judging by the way in which policymakers, intentionally or otherwise, have begun to echo the findings of scholars in this interdisciplinary area. Castells (2009: 49), for instance, has argued that 'networked social actors aiming to reach their constituencies and target audiences through the decisive switch to multimedia communications networks' are the key actors in the conflicts of our time. Underlying this thesis is a basic syllogism that war

reflects the societies from which it emerges; society has been transformed by ICTs into a 'network society' (Castells, 2010); therefore, warfare has been transformed in similar ways by ICTs. This idea also has currency among practitioners. Britain's most senior serving general, Sir David Richards (2010), described contemporary conflict as fought 'through the medium of the Communications Revolution' and principally about 'hearts and minds on a mass scale'. He predicted:

> Future wars of mass manoeuvre are more likely to be fought through the minds of millions looking at computer and television screens than on some modern equivalent of the Cold War's North German Plain. Indeed some might argue the screen is our generation's North German Plain, the place where future war will be won or lost.

Crucially, Richards did not imply that wars will be fought through computers, but suggested rather that they would be fought in the minds of people interacting through computer screens – a widely inclusive concept of cyberspace. We return to a core dilemma: Do we adopt a narrow concept of a cyberspace demarcated by physical architecture or software and network protocols, which makes cyber security simple, if not easy? Or do we work with a broader concept of a cyberspace not separate from real-space but in which the really big problems lie?

It is not just war, as David Richards explains, but also on-going events like the 'Arab Spring' in the Middle East and the 'Occupy' movements since 2011 that become objects of cyber security in its widest conceptualization. For strategists concerned with the production of intended effects – how Bertrand Russell (2004: 23) viewed the exercise of power – the

problem is that digital connectivity is a key component of an emerging 'new media ecology' that is making their work decisively harder:

> instant recording, archiving and distribution of images and stories add a chaotic element to any action. Nobody knows who will see an event, where and when they will see it or how they will interpret it. Nobody knows how the reactions of people locally or around the world will feed back into the event, setting off a chain of other events, anywhere, in which anybody may get caught up. (Hoskins and O'Loughlin, 2010: 2)

In summary, cyberspace is an environment that defies easy categorization. It possesses few of the definable parameters of traditional physical domains that possess identifiable integuments, although there are some benefits to conceptualizing it in such a manner. It is also characterized by non-linear dynamics in which effects are both unpredictable and potentially highly disproportionate to their apparent causes. The spatial metaphors discussed above, however, are not the only attempts to describe and explain aspects of 'cyberspace' through analogical means, and we turn now to those drawn from the biological world and the sciences concerned with its analysis and regulation.

Biological analogies

As we attempt to explain the new through older and more familiar terms, it is little wonder that in describing and conceptualizing the artefacts and activities of an increasingly computerized world, we borrow from the natural world and the sciences that seek to

explore and regulate it. We conceptualize ICTs in natural terms because of our 'innate tendency to focus on life and lifelike processes as they appear in technology' (Thomas, forthcoming). Scholars speak of information 'environments' and 'ecosystems', and of 'media ecologies' in which ICTs and people are arrayed in complex dynamic systems. Cyber-security problems are increasingly couched in the language and methodologies of public health, epidemiology and immunology.

Perhaps the most famous analogy in cyber security is that of the virus. The concept of a self-reproducing program dates to the work of Von Neumann in the 1940s and Barricelli in the 1950s (Von Neumann, 1966; Dyson, 1997). Numerous experiments based on this work were undertaken subsequently, although it was not until 1980 that the conceptual link between self-reproducing programs and biological viruses was explored by Kraus (1980).[10] Biological viruses are not complete organisms on their own but consist mainly of coded information in the form of DNA, and rely on host cells to become active. Similarly,

> As long as a self-reproducing program is not written to a system's memory, the program is of no consequence (besides its inherent information content). Only when the program finds itself in memory, and only when it is actually executed, may a self-reproducing program actually reproduce and mutate. The program draws on energy supplied by the system. (Kraus, 2009b: 64)

For Kraus (2009a: 7), 'a thesis on self-reproducing programs represented no less than the quest for life in a primordial computer soup consisting of ones and zeros'. In 1983, the link

between biological and technological viruses was formalized and the term ‘computer virus’ attached to it (Cohen, 1987: 31). A computer virus was defined as

> a program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows (Cohen, 1987: 23).

Information security expert Bruce Schneier (2000: 152) writes that, ‘for once, the [virus] metaphor is accurate’. Others have suggested that computer viruses might actually be a form of artificial life – a seductive metaphor if ever there was one (Spafford, 1994). However, Kraus was at pains to point out its limitations:

> a biological virus may induce its own reproduction by actively intruding into a cell and leveraging its metabolic processes. A self-replicating program is incapable of such a feat, even residing on a system and drawing on said computing system’s memory and energy, it remains dependent on activation through the operating system. (Kraus, 2009b: 64)

Thimbleby et al. are less charitable, stating that ‘the medical/biological metaphor for computer virus behaviour is seriously misleading’ (Thimbleby et al., 1998: 457), though they also observe that while ‘these terms lack any precise meaning in relation to computers, we know roughly what they mean’ and they can be used to generate ‘computational ideas’, for

better or for worse (Thimbleby et al., 1998: 444). This reference to analogical heuristics suggests that while computer viruses – being pure code – operate on the syntactic level, with effects on the performance of the physical substrate, their most substantial effects are on the semantic level. Viruses may of course directly inhibit the proper exchange of information at the syntactic level, but it is the semantic load the term carries that is of more significance in cyber-security discourse.

A rich vocabulary has developed around the concepts of viral infection (Wood, 1987; Kephart et al., 1993; Charney, 2012). As one author notes of the heuristic function of this dynamic, 'community, population, carrier, portal of entry, vector, symptom, modes of transmission, extra-host survival, immunity, susceptibility, sub-clinical, indicator, effective transfer rate, quarantine, isolation, infection, medium and culture are all terms from epidemiology that are useful in understanding and fighting computer viruses' (Murray, 1988: 140). Similarly, others observe that although 'there are many differences between living organisms and computers, the similarities are compelling and could point the way to improved computer security' (Forrest et al., 1997: 88).

The key to success in correlating the behaviours of biological and digital 'pathogens' is to select carefully the traits one wishes to compare; 'close comparisons between the physical mechanisms of infection are bound to fail due to the fundamental differences in construction between biological and digital systems' (Li and Knickerbocker, 2007: 340). Computer scientists and computer security specialists, while enthusiastic about the possibilities that such analogical reasoning may provide, are generally rather circumspect about adopting wholesale the metaphor of viruses, worms, etc., as forms of life that can be

treated through processes and practices directly analogous to medical interventions. That said, the very existence of such conceptual metaphors illustrates a profound structuring effect on how computing professionals perceive and combat computer security threats (Helmreich, 2000).

These forms of analogical reasoning have spread from computer security professionals to the realm of national security. Human immunology and the wider 'fight' against infectious disease have long been discussed using metaphors of war (Wallis and Nerlich, 2005: 2630–2631). This may be seen within the context of a gradual cultural process of the 'militarization' of language, which has occurred – in English, at least – over several centuries (Thorne, 2006: 1–2). A 2010 report from the Center for a New American Security describes an 'environmental model' of 'cyber public health' to provide a 'cleaner, healthier cyber environment in order to secure a broad range of United States and international interests' (Rattray et al., 2010: 140). The report utilizes concepts like 'the disease of malicious activity', 'methods of transmission', 'the duration of infectiousness', and so on. The remedies are presented as 'universal sanitization', 'inoculation', and 'quarantine and isolation'. The authors suggest that insights from public health are useful in 'developing innovative approaches to achieve a cleaner cyber commons. The fundamental lesson of biology is that survival and success is not necessarily the reward for the biggest, strongest or meanest, but rather for the most adaptable' (Rattray et al., 2010: 172). Notions of adaptation and fitness are also drawn directly from the biological sciences. As Kraus's translators note, in his early experiments on viruses, he 'had them compete for resources – complete with mutations and crossovers and fitness functions' (Bilar and Filliol, 2009: 2).

Another suite of analogies takes a still more holistic approach to ICTs and finds inspiration in the natural world through the lens of ecology and ecosystems. The way in which these analogies operate is slightly different from how the epidemiological approach functions, and they present alternative opportunities for the security professional and the policymaker. Kraus's early experiments with viruses occurred within a 'digital biotope' (Bilar and Filliol, 2009: 2). A 'biotope' is 'an environmentally uniform region of a habitat, occupied by a particular biological community'.[12] This is an apt description of Kraus's controlled experimental conditions, but virus analysts are now likely to speak of viruses occurring and replicating 'in the wild', 'out there' on the Internet. An early example of a virus 'in the wild' is the 1981 Elk Cloner virus that spread across Apple II operating systems via infected floppy disks (Dwan, 2000: 13). As in virology, viruses may be created in the 'laboratory', and later brought back for study – the 'dissection' and testing of code – but the principal 'environment' in which viruses occur is the Internet, perhaps better understood metaphorically as a 'biome' or, if we consider cyberspace as interwoven with the physical world, as part of the wider 'biosphere'. Given the wide variety of 'creatures' in the wild – viruses, worms, Trojans, spyware, adware, rootkits, keystroke loggers, diallers, etc. – it is unsurprising that considerations of the wider Internet 'environment' have been couched in terms derived from 'ecology' and 'ecosystems' approaches (see, for example, Furnell, 2008).

Ecological metaphors are common in computer science, yet their utility extends beyond the description of computer networks as environments in which malware competes for resources. As befits the holistic perspective implied by ecological approaches, these terms encompass the benign components of such systems as well as the malign. In addition to software agents operating mainly in the syntactic layer of cyberspace, the Internet ecology

or ecosystem includes the physical hardware that mediates communications and the human agents who communicate with one another at the semantic layer. As with the term 'digital environment', we might consider this form of metaphor as 'a macro label ... attached to any area of human interaction that is facilitated by digital technology' (Murray, 2007: 59). Furthermore, this metaphor can also be expanded to include all media devices and users. Formal models of the 'new ICT ecosystem' speak of an 'evolving' system and the 'symbiotic relationships' between, for example, network element providers; network operators; platform, content and applications providers; and end consumers (Fransman, 2007). Other authors posit 'biodiversity' in ICT ecosystems as the means to bolster systemic resilience to endogenous and exogenous shocks (Jackson et al., 2011).

There are always difficulties in translating concepts from one scientific discipline to another, in this case from the biological sciences to computer science. There is, of course, a long heritage of computing concepts travelling in the opposite direction, and the assertion, for example, in neuroscience and artificial intelligence that human brains can be literally understood and modelled as computers continues to be a source of both experimental fecundity and ethical disquiet. The deployment of biological analogies in computer security is relatively unproblematic in technical terms – operational efficacy aside – but cyber security is more than just computer network security: it is national security. Similarly, computer networks are more than just machines: they are people too. The deployment of public health metaphors in pursuit of cyber security is perhaps of a piece with a general 'medicalization of insecurity' (Elbe, 2012), in which the focus on the human body shifts to the body politic as constructed in and through sociotechnical ICT assemblages. An uncritical reliance on direct analogies between the biological and digital milieus risks concealing, for

example, that computer viruses are ‘created by human beings for the purpose of invading the programs of other human beings without their knowledge’ (Helmreich, 2000: 482).

As such, they are often created as a result of cultural and political perspectives at mutual odds: ‘The origins of viruses ... [lie] in the relationships that obtain between political economic systems and those who wish to critique or disrupt the concretization of such systems in computer networks’ (Helmreich, 2000: 483). To ascribe agency solely to entities external to the metaphorical body is potentially to omit social factors from analyses of security issues, thereby reducing the likely beneficial effects of policies and strategies thereby derived. Operating at the semantic level, the discourse of non-human agency serves to disenfranchise further those who may be dissatisfied with the dominant political system in the first place, although this is an argument unlikely to impress security professionals. The resulting ‘battles’ are played out principally in the syntactic layer of ‘cyberspace’.

Aside from the veracity or utility or otherwise of analogizing the biological and the digital, we must wonder also at the implications of these analogies moving from computer science to national security and (inter)national politics. It may be that ‘scientific metaphors are intended to be analytic and ultimately to imply formulas to calculate specific relations and predictions ... political metaphors are designed to stir emotions, not to be analytic’ (Mio, 1997: 123). Disease has long been identified as a popular ‘root metaphor’ in politics: ‘Quite clearly, it is the job of governments to promote the “infection” of good ideas and to “cure” or at least “immunize against” bad ideas’ (Mio, 1997: 124; see also Bell, 2012a,b). The ‘germ’ metaphor – which we might here equate with ‘virus’ – has been shown, historically, to be a dominant metaphor of ‘social menace’, suggesting that ‘the social organism was

inherently pure but susceptible to invasive agents' (Mio, 1997: 125). Haraway (1991: 252n4) notes that, 'like the body's unwelcome invaders, the software viruses are discussed in terms of pathology as communications terrorism, requiring therapy in the form of strategic security measures'.

The use of biological and medical analogies by elites may not be intended necessarily to elicit negative emotions in the public imagination, but it would not be unwarranted to suppose they might be deployed for such a purpose. We might argue that 'virus', in particular, has the power to fascinate and instil fear, given that viruses are 'a liminal form of life ... associated with death and disorder, the cessation of life activity' (Helmreich, 2000: 488). At present, however, martial analogies such as 'defence' are far more commonly used in politics, and the language of threat continues to be the main conceptual frame likely to stir fearful responses. That viruses and other forms of malware are increasingly spoken of in the public sphere with reference to their 'payloads' is another indication of the persistence of martial metaphors in this discursive space.

Conclusion

In this article, we have examined only two popular forms of analogical reasoning that occur in cyber-security discourse – spatial and biological – as well as the military language that pervades the usage of both. Our choices in this case are suggested by the fact that 'cyberspace' is not a traditional space in the Euclidean geometric sense and by the recognition that biological concepts are being extended to an entirely digital realm. In general, we find also that the language of cyber security is permeated by military metaphor.

As an analogical heuristic, this resonates well enough with the day-to-day of cyber-security professionals – also sometimes described in terms of public health (for example, practising good 'computer hygiene') – to be useful. It does not take much conceptual stretching to see the parallel between these duties and those of company sergeants major from Julius Caesar's day to our own – testing perimeter fortifications and alarms, shoring up trench lines and overhead cover, and constantly checking that pickets are awake with their weapons and equipment in good order. Ultimately, though, this line of reasoning is imperfect and somewhat misleading. For one thing, as Libicki (2007: 35) has argued, 'there is no forced entry in cyberspace. If a destructive message gets into a system, it must be entirely across pathways that permit such a message to get through.' Perhaps more importantly, a martial conceptualization of cyberspace is an important determinant of groupthink and reduces scope for collective problem-solving and creativity. One of the major advantages of spatial and biological analogies in cybersecurity discourse should be that they are not martial in origin. They do not necessarily speak directly to a nascent militarization of cyberspace (Deibert, 2008), though they can be and have been harnessed to the imagination of major security threats and remedial actions dependent more on military force than other more sophisticated resources and skills. The art of strategy has never been simply about manning the parapets; nor should it now be about securing its digital analogues.

If we return to the notion that scientific metaphors are 'intended to be analytic and ultimately to imply formulas to calculate specific relations and predictions' (Mio, 1997: 123), we find that this resonates well with many of the forms of analogy and metaphor discussed above. However, we also find that some modification to this view is necessary: Hoskins and

O'Loughlin (2010: 2), for example, seek 'to find intelligibility, not order' through the new media ecology lens. In this sense, metaphor is deployed as a powerful heuristic for explaining socio-technical phenomena at the physical, syntactic and semantic layers, and for proposing policy, although it does not claim any prescriptive theoretical role. However, we should be aware that metaphor is intrinsic to social relations and, as in the historical development of military affairs, can construct them as much as it can help to describe, explain and understand them (Bousquet, 2009). As computer scientists have found of the virus metaphor, it is only possible to analogize so far before analogy fails. As well as finding that metaphors and analogies have utility in describing and explaining socio-technical worlds, we can also determine that such usage has catalysed the development of regimes of counter-measures. These analogies and metaphors have shaped the evolution of computer science and are increasingly important as the basis for cyber-security policy.

Getting cyber 'right' is, and will likely remain, an enormously challenging task for governments, industry and private citizens. Digital networks have brought about a degree of global connectedness that is unparalleled in history. Furthermore, the speed and extent of connectivity is increasing, not just in the developed world but everywhere. Yet, the problems of security are not confined to cyberspace's physical and syntactic elements; they are manifest also in the 'real space' of which cyberspace is an inseparable and, in practical terms, unmappable part. Moreover, however grave the threats to open societies that emanate from cyberspace may seem, the opportunities for more vibrant and rewarding social lives of citizens, more effective and representative patterns of politics, and profitable types of innovative enterprise are greater. It is little wonder that we attempt to classify – often productively – the unfamiliar present and unknowable future in terms of a more

familiar past, but we should remain mindful of the limitations of analogical reasoning in cyber security, no matter where we draw our inspiration from. As an illustration, it is often argued that the 'Great Firewall of China' and other measures taken by China to restrict the physical entry points of the Internet make it more secure than Western societies that have been more promiscuously wired up (Clarke, 2010: 148). In fact, China's national firewall is not designed so much to protect its computer networks from attack on the physical and syntactic levels of cyberspace as it is to defend its political regime by slowing the infiltration into its semantic cyberspace of ideas that might corrode the population's continuing consent to be governed as they have been. China's digital great wall – which, as Clayton et al. (2007) have illustrated, is easily breached – is unlikely to prove more effective than did the real space bricks-and-mortar one after which it is named. By contrast, as another participant at one of our workshops remarked, even in terms of cyber security there are advantages to being ineradicably connected:

> you are probably more vulnerable if you rely on other people, but you may be more resilient from a threat perspective. From an attacker's perspective, for instance, if you take the UK off the Internet, you would automatically take off half of Western Europe.

As we adapt to the new security realities of the information age, it is incumbent upon scholars to comprehend the benefits of connectivity as much as the threats thus engendered. The dominant metaphors of cyber-security discourse have the potential to channel our thinking into a 'walled garden' (Deibert, 2012: 271) modality that is neither

desirable nor necessary. The true challenge of cyber security is to find a positive-sum formulation based on transparency, accountability and restraint, and to put it into practice.

Funding

This article was partially funded by a grant from the UK's Government Communications Headquarters (GCHQ) and by a US Defense Department Minerva grant entitled 'Strategy and the Network Society'.

References

Aradau C (2010) Security that matters: Critical infrastructure and objects of protection. *Security Dialogue* 41(5): 491–514.

Arquilla J and Ronfeldt D (1993) Cyberwar is coming! *Comparative Strategy* 12(2): 141–165.

Ball T (1994) *Reappraising Political Theory: Revisionist Studies in the History of Political Thought*. Oxford: Oxford University Press.

Barlow JP (2006) Lecture to the European Graduate School, Saas-Fee, Switzerland. 29 May. Available at: http://www.egs.edu/faculty/john-perry-barlow/videos/independence-declaration-ofcyberspace/ (accessed 20 February 2012).

Barnard-Wills D and Ashenden D (2012) Securing virtual space: Cyber war, cyber terror, and risk. *Space & Culture* 15(2): 110–123.

BBC News (2012) Wikipedia joins blackout protest at US anti-piracy moves. 18 January. Available at: http://www.bbc.co.uk/news/technology-16590585 (accessed 20 February 2012).

Bell C (2012a) Hybrid warfare and its metaphors. *Humanity* 3(2): 225–247.

Bell C (2012b) War and the allegory of medical intervention: Why metaphors matter. *International Political Sociology* 6(3): 325–328.

Benford G (2011) How to lose a billion dollars in your spare time. Available at: http://www.gregorybenford.com/science-fiction-2/how-to-lose-a-billion-dollars-in-your-spare-time/(accessed 20 February 2011).

Berkowitz B (2003) *The New Face of War: How War Will Be Fought in the 21st Century*. New York: The Free Press.

Betz DJ (2008) The virtual dimension of contemporary insurgency and counterinsurgency. *Small Wars & Insurgencies* 19(4): 510–540.

Betz DJ and Stevens T (2011) *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon: Routledge.

Bilar D and Filliol E (2009) Editors/translators foreword. *Journal in Computer Virology* 5(1): 1–3.

Bipartisan Policy Center (2010) Cyber ShockWave. Available at: http://www.bipartisanpolicy.org/events/cyber2010 (accessed 20 February 2012).

Bobrow DB (1996) Complex insecurity: Implications of a sobering metaphor: 1996 presidential address. *International Studies Quarterly* 40(4): 435–450.

Bolt N, Betz DJ and Azari J (2008) *Propaganda of the deed 2008: Understanding the phenomenon*. Whitehall Report 3-08. London: Royal United Services Institute.

Bousquet A (2009) *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. London: Hurst & Company.

Brachman J and Forest JJF (2007) Exploring the role of virtual camps. In: Innes MA (ed.) *Denial of Sanctuary: Understanding Terrorist Safe Havens*. Westport, CT: Praeger Security International, 124–138.

Brito J and Watkins T (2011) Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *Working Paper 11-24*. Arlington, VA: Mercatus Center, George Mason University.

Brunner E and Cavelty MD (2009) The formation of in-formation by the US military: Articulation and enactment of infomanic threat imaginaries on the immaterial battlefield of perception. *Cambridge Review of International Affairs* 22(4): 629–646.

Buck SJ (1998) The Global Commons: An Introduction. Washington, DC: Island Press.

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

Castells M (2001) *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press.

Castells M (2009) *Communication Power*. Oxford: Oxford University Press.

Castells M (2010) *The Rise of the Network Society. The Information Age: Economy, Society, and Culture*. Vol. 1, 2nd edn. Malden, MA: Wiley-Blackwell.

Cebrowski AK and Garstka JJ (1998) Network-centric warfare: Its origin and future. *Proceedings of the US Naval Institute* 124(1): 28–35.

Charney S (2012) Collective defense: Applying the public-health model to the internet. *IEEE Security & Privacy* 10(2): 54–59.

Clarke R (2010) *Cyberwar: The Next Threat to National Security and What To Do About It*. New
York: Harper Collins.

Clayton R, Murdoch S and Watson R (2007) Ignoring the Great Firewall of China. *I/S: A journal
of Law and Policy* 3(2): 271–296.

Cohen F (1987) Computer viruses: Theory and experiments. *Computers & Security* 6(1): 22–35.

Cohen JE (2007) Cyberspace as/and space. *Columbia Law Review* 107(1): 210–256.

Conway M (2008) Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. In: Dunn Cavelty M and Kristensen KS (eds) *Securing 'the Homeland': Critical Infrastructure, Risk and (In)security*. London: Routledge, 109–129.

Deibert RJ (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium* 32(3): 501–530.

Deibert RJ (2008) Black code redux: Censorship, surveillance and the militarization of cyberspace. In: Boler M (ed.) *Digital Media and Democracy: Tactics in Hard Times*. Cambridge, MA: MIT Press, 137–163.

Deibert RJ (2012) The growing dark side of cyberspace (... and what to do about it). *The Penn State Journal of Law and International Affairs* 1(2): 260–274.

Dunn Cavelty M (2008) *Cyber-Security and Threat Politics: US Efforts To Secure the Information Age*. London: Routledge.

Dwan B (2000) The computer virus – From there to here: An historical perspective. *Computer Fraud & Security* 2000(12): 13–16.

Dyson GB (1997) *Darwin Among the Machines: The Evolution of Global Intelligence*. Reading, MA: Addison-Wesley.

Edelman M (1964) *The Symbolic Uses of Politics*. Urbana, IL: University of Illinois Press.

Elbe S (2012) Bodies as battlefields: Toward the medicalization of insecurity. *International Political Sociology* 6(3): 320–322.

Farrell T (2002) Constructivist security studies: Portrait of a research program. *International Studies Review* 4(1): 49–72.

Ferrari F (2007) Metaphor at work in the analysis of political discourse: Investigating a 'preventive war' persuasion strategy. *Discourse & Society* 18(5): 603–625.

Forrest S, Hofmeyr SA and Somayaji A (1997) Computer immunology. *Communications of the ACM* 40(10): 88–96.

Fransman M (2007) Innovation in the new ICT ecosystem. *Communications & Strategies* 68(4): 89–110.

Franzese PW (2009) Sovereignty in cyberspace: Can it exist? *Air Force Law Review* 64: 1–42.

Furnell S (2008) It's a jungle out there: Predators, prey and protection in the online wilderness. *Computer Fraud & Security* 2008(10): 3–6.

Gadamer HG (1989) *Truth and Method*. 2nd edn. London: Continuum.

Gibson W (1984) *Neuromancer*. New York: Ace Books.

Goodman S, Kirk J and Kirk M (2007) Cyberspace as a medium for terrorists. *Technological Forecasting & Social Change* 74(2): 193–210.

Gregory DU (1989) The dictator's furnace. *Peace Review* 1(1): 12–16.

Habermas J (1991) *The Structural Transformation of the Public Sphere*. Cambridge, MA: MIT Press.

Hammes TX (2005) War evolves into the fourth generation. *Contemporary Security Policy* 26(2): 189–221.

Haraway DJ (1991) *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.

Hayden DL (2008) Air mindedness. *Air & Space Power Journal* 22(4): 44–45.

Helmreich S (2000) Flexible infections: Computer viruses, human bodies, nation-states, evolutionary capitalism. *Science, Technology & Human Values* 25(4): 472–491.

HM Government (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Norwich: The Stationery Office.

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

Hoffman FG (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*. Washington, DC: Potomac Institute.

Hook GD (1984) The nuclearization of language: Nuclear allergy as political metaphor. *Journal of Peace Research* 21(3): 259–275.

Hoskins A and O'Loughlin B (2010) *War and Media: The Emergence of Diffused War*. Cambridge: Polity.

Jackson J, Creese S and Leeson MS (2011) Biodiversity: A security approach for ad hoc networks. *IEEE Symposium on Computational Intelligence in Cyber Security* April: 186–193.

Jackson R (2005) *Writing the War on Terrorism: Language, Politics and Counter-Terrorism*. Manchester: Manchester University Press.

Jones DM and Smith MLR (2005) Greetings from the cybercaliphate: Some notes on homeland security. *International Affairs* 81(5): 925–950.

Jordan T and Taylor P (2004) *Hacktivism and Cyberwars: Rebels with a Cause?* Abingdon: Routledge.

Karatzogianni A (ed.) (2009) *Cyber Conflict and Global Politics*. London: Routledge.

Kephart JO, Chess DM and White SR (1993) Computers and epidemiology. *IEEE Spectrum* 30(5): 20–26.

Kilcullen D (2009) *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. London: Hurst & Company.

Kraus J (1980) Selbstreproduktion bei programmen [Self-reproducing programs]. MA thesis.

Universität Dortmund.

Kraus J (2009a) Foreword. *Journal in Computer Virology* 5(1): 7–8.

Kraus J (2009b) On self-reproducing computer programs. Trans. Bilar D and Filliol E. *Journal in Computer Virology* 5(1): 9–87.

Lakoff G (1987) The death of dead metaphor. *Metaphor & Symbolic Activity* 2(2): 143–147.

Lakoff G and Johnson M (1980) *Metaphors We Live By*. Chicago, IL: University of Chicago Press.

Lawson S (forthcoming) Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*.

Li J and Knickerbocker P (2007) Functional similarities between computer worms and biological pathogens. *Computers & Security* 26(4): 338–347.

Liang Q and Xiangsui W (1999) *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.

Libicki MC (1994) The mesh and the net: Speculation on armed conflict in an age of free silicon. *McNair Paper 28*. Washington, DC: National Defense University.

Libicki MC (1995) *What Is Information Warfare?* Washington, DC: National Defense University Press.

Libicki MC (1997) *Defending Cyberspace and Other Metaphors*. Honolulu, HI: University Press of the Pacific.

Libicki MC (2007) *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.

Lievrouw L (2011) *Alternative and Activist New Media*. Cambridge: Polity.

Lobban I (2010) Cyber: Threats and security. Speech to International Institute of Strategic Studies, London, 12 October. Available at: http://www.iiss.org/recent-key-addresses/iain-lobban-address/(accessed 20 February 2012).

Mackinlay J (2009) *The Insurgent Archipelago*. London: Hurst & Company.

Mio JS (1997) Metaphor and politics. *Metaphor & Symbol* 12(2): 113–133.

Mitchell WJ (1995) *City of Bits: Space, Place, and the Infobahn*. Cambridge, MA: MIT Press.

Murray AD (2007) *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon: Routledge-Cavendish.

Murray WH (1988) The application of epidemiology to computer viruses. *Computers & Security* 7(2): 139–150.

Neale M (director) (2000) *No Maps for These Territories* [documentary film]. New York: Docurama.

Neumann IB (2002) Returning practice to the linguistic turn: The case of diplomacy. *Millennium* 31(3): 627–651.

Orlowski A (2012) White House shelves SOPA ... now what? *The Register*, 17 January. Available at: http://www.theregister.co.uk/2012/01/17/beyond_sopa/ (accessed 20 February 2012).

Owens B (2000) *Lifting the Fog of War*. London: Johns Hopkins University Press.

Pickerill J (2003) *Cyberprotest: Environmental Activism Online*. Manchester: Manchester University Press.

Rattray GJ (2001) *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.

Rattray GJ, Evans C and Healey J (2010) American security in the cyber commons. In: Denmark AM and Mulvenon J (eds) *Contested Commons: The Future of American Power in a Multipolar World*. Washington, DC: Center for a New American Security, 139–172.

Rauscher KF and Yaschenko V (2011) *Critical Terminology Foundations*. New York: EastWest Institute.

Rheingold H (1993) *The Virtual Community: Homesteading on the Electronic Frontier*. Reading, MA: Addison-Wesley.

Rheingold H (2002) *Smart Mobs: The Next Social Revolution*. Cambridge, MA: Basic Books.

Richards D (2010) Future conflict and its prevention: People and the information age. Speech to
International Institute for Strategic Studies, London, 18 January.

Rid T (2012) Cyber war will not take place. *Journal of Strategic Studies* 35(1): 5–32.

Rogers R (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(2–3): 241–260.

Russell B (2004) *Power: A New Social Analysis*. London: Routledge.

Schafer M and Crichlow S (1996) Antecedents of groupthink: A quantitative study. *Journal of Conflict Resolution* 40(3): 415–435.

Schneier B (2000) *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons.

Singer PW and Shachtman N (2011) The wrong war. *Government Executive*, 15 August.

Spafford EH (1994) Computer viruses as artificial life. *Artificial Life* 1(3): 249–265.

Starhawk (2002) *Webs of Power: Notes from the Global Uprising*. Gabriola Island, British Columbia: New Catalyst Books.

Sterling B (1992) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam.

Stohl M (2006) Cyber terrorism: A clear and present danger, the sum of all fears, breaking point, or patriot games? *Crime, Law & Social Change* 46(4–5): 223–238.

Thimbleby H, Anderson S and Cairns P (1998) A framework for modelling trojans and computer virus infection. *The Computer Journal* 41(7): 444–458.

Thomas S (forthcoming) *Technobiophilia: Nature and Cyberspace*. London: Bloomsbury Academic.

Thorne S (2006) *The Language of War*. London: Routledge.

US Department of the Army (2007) *US Army/Field Corps Counterinsurgency Manual No. 3-24*. Chicago, IL: Chicago University Press.

US Department of Defense (2006) Information operations. *Joint Publication 3-13*. Washington, DC: US Department of Defense.

US Department of Defense (2010) *Quadrennial Defense Review Report*. Washington, DC: US Department of Defense.

Von Neumann J (1966) *Theory of Self-Reproducing Automata*. Edited by Burks AW. Urbana, IL: University of Illinois Press.

Wallis P and Nerlich B (2005) Disease metaphors in new epidemics: The UK media framing of the 2003 SARS epidemic. *Social Science & Medicine* 60(11): 2629–2639.

Wittgenstein L (2009) *Philosophical Investigations*. 4th edn. Oxford: Wiley-Blackwell.

Wood CC (1987) The human immune system as an information systems security reference model. *Computers & Security* 6(6): 511–516.

David Betz is a Senior Lecturer in the War Studies Department, King's College London, and a Senior Fellow of the Foreign Policy Research Institute. **Tim Stevens** is a PhD candidate in the Department of War Studies, King's College London, and an Associate of the Centre for Science and Security Studies. Together, they are the

authors of *Cyberspace and the State: Towards a Strategy for Cyber Power* (International Institute for Strategic Studies, 2011).

Notes

1. The turn of phrase employed in a rare public address by the director of the UK's Government Communications Headquarters (GCHQ) (Lobban, 2010).

2. Funded by UK Government Communications Headquarters (GCHQ), the workshops entitled 'Cyber Security: Lacunae of Strategy' were held on 25 October 2011 and 31 January 2012 at King's College London. The workshops responded to UK government calls for interdisciplinary initiatives to meet the cyber-security 'challenge'. See HM Government (2011: 18).

3. 'Guiding metaphors and analogies' play a role in 'closed-mindedness', a contributory factor to group decision-making errors (Schafer and Crichlow, 1996).

4. 'To fly, fight, and win ... in air, space, and cyberspace' is, for example, the subtitle of the US Air Force's *Air & Space Power Journal*.

5. Although see Rattray (2001).

6. See Arquilla and Ronfeldt (1993); Berkowitz (2003); Cebrowski and Garstka (1998); Libicki (1994); Owens (2000).

7. A type of warfare adequately subsumed under the term ‘computer network operations’ (US Department of Defense, 2006).

8. The link between democracy and the city of and in cyberspace is another important strand of analogical reasoning. See, for example, Mitchell (1995).

9. Workshop participant, King’s College London, 25 October 2011.

10. Although the first known use of the term and concept of a computer virus was by Gregory Benford in 1970. See Bilar and Filliol (2009: 2n1); Benford (2011).

11. Kraus also wrote, ‘we consider self-reproducing programs to be contenders for the existence of lifeforms on computer systems’ (Kraus, 2009b: 10).

12. Oxford English Dictionary, online; available at www.oed.com.