Space and Culture
XX(X) 1–14
© The Author(s) 2012
Reprints and permission:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/1206331211430016
http://sac.sagepub.com
SAGE

Securing Virtual Space: Cyber War, Cyber Terror, and Risk

David Barnard-Wills[1] and Debi Ashenden[1]

Abstract

This article uses a governmentality and discourse analysis approach to analyze cyber security policy literature. It examines the problems of construction of virtual space and current efforts to secure this space political and technologically. It extracts a model of cyber security discourse that constructs cyberspace as ungovernable, unknowable, a cause of vulnerability, inevitably threatening, and a home to threatening actors.

Keywords

governmentality, cyber security, virtual space, discourse, security

Introduction

In early 2010 the U.K. government's Cyber Security Strategy established two new agencies with responsibility for cyber security, while during 2009 the U.S. government appointed a new cyber security coordinator and made cyber security an explicit part of national security policy. In recent years, online attacks on Estonia and Georgia, fears of cyber terrorism, and a background of crime and espionage have indicated a substantial role for cyber conflict in international relations, including the potential for cyber diplomacy and cyber warfare. This role suggests attention to the securitization of virtual space.

It is possible to identify a relatively consistent discourse of cyber security that involves trends of uncertainty, risk perception, securitization, and potential militarization. This discourse has complex roots in military, technological, and policy discourses, but its features are not deterministically derived from these, rather occurring at their point of interaction. What has emerged is a techno-political discourse of cyber security, which draws on practice in both the fields of international relations and information technology and emerges out of an interaction between government and a wide range of technological and policy actors.

Both international security and cyber security accounts can benefit from each other's perspective. A cohesive analytical approach is needed that is capable of incorporating an understanding of the technical possibilities and limitations as well as the politics of this field. Both disciplines have been somewhat slow to respond to the demands of this conceptual space. Although accounts

[1] Cranfield University, Swindon, UK

Corresponding Author:
David Barnard-Wills, Department of Informatics and Systems Engineering, Cranfield University, Defence Academy of the United Kingdom, Shrivenham, Swindon SN6 8LA, UK
Email: d.barnardwills@cranfield.ac.uk

of cyber conflict are emerging (Karatzogianni, 2008), a selection of commonly used international relations security studies textbooks finds little mention of cyber security or any analogous terms as a core element of international relations. Such a perspective occurs occasionally in terms of intelligence studies or in accounts of military transformation. However, cyber security accounts often have a simplistic or limited view of international relations or how governments work. Political science has a rich repertoire of concepts and models that can assist with this.

The politics of cyber security demonstrates a governmental logic amenable to study using Mitchell Dean's "analytics of government." This suggests that governmentalities (mentalities of government) are constructed through discourses centered on particular problem constructions and a set of politically privileged responses to those problems. This article draws on governmentality and discourse analysis approaches to examine this emergent discourse, alongside recent governmental attempts to secure virtual space.

The article first examines the concept of cyberspace and virtual space, highlighting the importance of understanding cyberspace as a metaphor. This includes current cyber security policy developments in both the United Kingdom and United States and the explicit tensions in this area. It then proposes the use of governmentality theory and discourse analysis to better understand the construction of the problems of virtual space and the implicit tensions subsumed in the dominant discourse of cyber security. This approach is applied to the dominant discourse, identifying the dominant construction of virtual space as ungovernable, unknowable, problematically visible, vulnerable, inevitably threatening, and inhabited by a range of hostile and threatening actors. The article concludes with the implications of these findings.

Virtual Space

Although coined in *Burning Chrome* (1982), it was William Gibson's (1984) evocative metaphor of a shared virtual hallucination in the novel *Neuromancer* that brought the term *cyberspace* to prominence.

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding . . . (Gibson, 1995, p. 67)

Cyberspace should be understood as a metaphor. Gibson's (1984) understanding of a consensual hallucination suggests we examine carefully the makeup of this space and the ways in which this shared perception of the online, networked environment is collectively constructed. Similarly, the use of the term *virtual* in the title of this article refers to the nonphysical, yet fundamentally real, nature of cyberspace. It is a construction in two senses. First, it is a physical construction produced by networking information technology. Second, it is a social construction, shaped by the way that people and institutions think, understand, and talk about this space. In a very real sense, cyberspace is a system of social relations, even if many of the participants in those relations are technological or nearly automated. It is therefore constituted by a large range of articulatory practices (Glynos & Howarth, 2007). The U.K. government definition supports this wide breadth of content:

> Cyberspace encompasses all forms of networked digital activities; this includes the content of and actions conducted through digital networks. (Cabinet Office, 2009a, p. 7)

Understanding cyberspace as a constructed space allows us to consider the *processes* of is construction, avoid taking for granted the politics of this process, and examine the potential winners and losers in this construction.

Lessig (1999) argues that cyberspace is not one single type of space but, rather, many places, with a divergent range of values and norms. Spaces express their norms and values through their architecture, those practices that are enabled or disabled within any given space (Lessig, 1999). If architectures of cyberspace are rules that affect behavior within a space, then to an extent the space becomes sovereign. Lessig argues that "real-space" sovereigns will respond to this threat of an external sovereign by attempting to ensure that their regulatory power encompasses virtual spaces (Lessig, 1999, p. 198). It is to a range of such measures that we now turn.

Securing Virtual Space

We have recently witnessed a series of policy activities from various governments intended to secure virtual space and create cyber security. This article will primarily focus on U.K. and U.S. efforts. We first provide an overview of cyber security measures at the governmental level, before the rest of the article examines the drives behind these measures—the perceived insecurity of cyberspace constructed through the dominant cyber security discourse.

Former U.K. Prime Minister Gordon Brown explicitly evoked spatial metaphors of security during the launch of the first public Cyber Security strategy of the United Kingdom:

> Just as in the nineteenth century we had to secure the seas for our national safety and prosperity, and in the twentieth century we had to secure the air, in the twenty first century we also have to secure our position in cyberspace in order to give people and businesses the confidence they need to operate safely there. (Cabinet Office, 2009b)

Cyber security is positioned in a direct line of descent from previous spaces of insecurity, apparently converted to secured spaces. It also highlights some of the motivations for these moves. It is rhetorically expansive and inclusive—it is "our" position that is to be secured. Furthermore, it links cyber security to a long (imperial) tradition of securing space for (selective) movement and commerce through military force.

With the new Cyber Security Strategy, the U.K. government created two new organizations in September 2009, intended to be operational by March 2010. The Office of Cyber Security (OCS) is to "provide strategic leadership for and coherence across Government. The OCS will establish and oversee a cross-government programme to address priority areas in pursuit of the U.K.'s strategic cyber security objectives" (Cabinet Office, 2009a, p. 21). The Cyber Security Operations Centre will coordinate incident response, monitor cyberspace, and provide advice and information (Cabinet Office, 2009a). The multiagency Cyber Security Operations Centre will be hosted at Government Communications Headquarters (GCHQ), the United Kingdom's communications intelligence agency, to bring together knowledge about threats from different parts of government and industry with GCHQ's technical expertise (GCHQ, 2009). The establishment of the OCS involves the first official statement of any offensive cyber warfare capacity by the U.K. government. Cyber attacks are one of the imagined (although low probability) vectors for the reemergence of a state-led threat against the United Kingdom (Cabinet Office, 2008)

In the United States, the Obama administration aims to treat digital infrastructure as a strategic national security priority, with cyber security identified as one of the most serious economic and national security challenges facing the nation (National Security Council, 2010). The United

States recently established the new office of Cybersecurity Coordinator, appointing Howard Schmidt. The coordinator sits on the National Security Staff and the National Economic Council. This role includes a privacy and civil liberties portfolio (Obama, 2009). In March 2010, the administration has also made public parts of the previously secret Comprehensive National Cybersecurity Initiative started in 2008. The Comprehensive National Cybersecurity Initiative is intended to defend against a range of immediate threats, enhance "situation awareness" and prevent intrusions, enhance U.S. counterintelligence capabilities, and strengthen the future cyberspace environment through encouraging research, development, and training in cyber security (National Security Council, 2010). It also expands law enforcement funding in these areas. The U.S. Department for Homeland Security published a "road map" for cyber security research, which aimed to "get ahead of [the United States'] adversaries and protect [the nation's] information systems and networks into the future" (Department of Homeland Security, 2009, p. iii). The 2005 U.S. National Defense Strategy identified cyberspace as a "new theatre of operations" with the requirement of securing strategic access and global freedom of action. The strategy positioned the United States as needing to control the global commons in order to deal with "traditional, irregular, catastrophic or disruptive threats" (Rattray, Evans, & Healy, 2010, p. 139).

For both countries, cyber security is being defined as a key priority of national security. This national security rationale should also be contextualized against a broad background of attempts to secure virtual space arising from other sources: copyright, child protection, online criminality, and personal information protection.

There are a number of explicit tensions in cyber security discussions. These include the similarities and differences between physical and virtual security, the tension between securing virtual space and opening it up, the balance between the interests of the public sector focused on national interests and critical national infrastructure and those of the private sector, and the proper distribution of responsibility between the government and the citizen for cyber security.

The U.K. strategy sets up a responsibility for maintaining and improving the security of cyberspace for "all those people that work, communicate or interact using cyberspace" (Cabinet Office, 2009a, p. 7). Supporting this, the strategy sets up a role for government to "provide better advice and information about the risk to business and the public" and identifies skills and education as a strategic priority (Cabinet Office, 2009a, p. 21). The perceived importance of online economic and social activity and the necessity of developing "digital life skills" is highlighted in the Digital Britain Report 2009 (Secretary of State for Culture, Media and Sport & Minister for Communications, Technology and Broadcasting, 2009). The focus is primarily on individuals' responsibility to protect themselves.

> Online safety is as much about behaviour as it is about technology. Fundamentally, it is about assessing risk and deciding what to do about it. You are the only person who can guarantee your own safety online. (Get Safe Online, 2010)

However, there appears to be a recognition that cyber security at the level of international relations, counterterrorism, and cyber war is not within the capacity of most citizens (in a way that protecting oneself from online fraud *might* be). There is contrast between cyber security in a discursive field marked by more traditional discourses of international security, state sovereignty and the Hobbesian promise of the state to protect citizens from external aggression, and the more diffuse field of personal information security. Similarly, there are tensions between the vision of a threatening space to be secured, as outlined in the Cyber Security Strategy, as examined in this article, and the more optimistic, economic focus of the U.K. government's *Digital Britain Report*, which focuses on the potential economic and cultural opportunities of online activity.

Bendrath (2001) regards cyber security in the United States as an example of failed securitization. In the securitization model of the Copenhagen School in international relations, issues fall into three types: nonpolitical, politicized, and securitized. Nonpolitical issues are not seen as requiring state intervention and are not frequently included in public debate. Political issues are resolved through normal governmental mechanisms, whereas securitized issues require urgent action beyond standard political practices (Buzan, Waever, & de Wilde, 1998). Securitization is the rhetorical act by which a political issue is articulated as an existential threat. A successful securitization involves the acceptance of such a threat and the implementation of special measures. Bendrath's (2001) position is that defense interests attempted to move cyber security to this position but have so far failed, keeping cyber security within the framework of conventional governmental practice. However, a securitization move need not convince the entire population of the existential threat if it is capable of capturing powerful and influential groups (Emmers, 2007). Also drawing on the literature on securitization, Nissenbaum (2005) finds two conceptions of security competing for political attention. These reflect their origins in computer science and engineering and in politics and national security.

A combination of the International Relations securitization literature with the governmentality approach provides a powerful tool for shifting between differing levels of political activity. Cyber security appears to sit at the boundary between the two fields, not quite producing exceptional measures or states of exception but bringing strong security principles into everyday governmentality.

Governmentality and Shared Discourses of Cyber Security

The theory of governmentality arises from Foucault's (2007) work on government and liberalism. Combining "government" and "mentality," governmentality seeks to distinguish the particular mentalities, arts, and regimes of government. The term *government* is used generally for any calculated direction of human conduct, any attempt to "shape with some degree of deliberation aspects of our behaviour according to particular sets of norms and for a variety of ends" (Dean, 2010, p. 18). Government involves not direct control but encouraging forms of self-direction appropriate to certain situations. Dean provides a typology of the "analytics of government" as a governmental approach to political analysis. This includes the view of governments as assemblages or regimes rather than homogenous totalities, the identification of problematizations, and the priority given to questions relating to process, mechanisms, and tactics of governance through characteristic ways of thinking and speaking.

A core aspect of governmentality highly relevant here is the awareness of the "plurality of distinct forces [that] goes into shaping modern forms of power" (Ransom, 1997, p. 16). The government is not conceived of as a unitary actor but as a wide range of agencies, bodies, institutions, practices, and discourses. The governmental perspective pays attention to the way governance is "enacted and coordinated by extra-state agents such as corporations, non-governmental agencies, international bodies and community groups"(Haggerty, 2006a, p. 40). The contemporary nation state incorporates the governance capacity embodied in civil society. In fact, government "employs and infiltrates a number of discourses ordinarily conceived as unrelated to political power, governance or the state" (Brown, 2006, p. 18). One of the strongest messages in the U.K. cyber security strategy is making it a government priority to "work closely with the wider public sector, industry and civil liberties groups, the public and international partners," while providing strategic leadership and coherence across government (Cabinet Office, 2009a, p. 21). Public–private partnerships are also crucial to the U.S. cyber security strategy. President Obama acknowledged that "the vast majority of our critical information infrastructure in the

United States is owned and operated by the private sector" (Obama, 2009) but that the administration would not dictate security standards.

Bendrath (2001) traces the development of such public–private partnerships in the United States, where despite early debates framing cyber security in military terms, the military was unable to dominate the cyber security agenda due to uncertainty over international law and the legality of offensive information operations, the *posse comitatus* act that prevents the U.S. army operating on U.S. soil, and opposition from law enforcement agencies presenting an investigative and legal paradigm for dealing with cyber security. This combined with the recognition that, as well as infrastructure, expertise and ability to deal with online threats largely resided in the private sector encouraged the government to develop partnerships and greater assemblages of governance linked to cyber security activity. The sharing of cyber security information is routinely identified as a fundamental part of cyber security strategies (National Security Council, 2010). In governmentality terms, this serves alongside dominant discourses of cyber security to pull together the disparate actors making up governmental assemblages.

Dean (2010) highlights a concern for technical aspects of government: means, mechanisms, procedures, instruments, and (critically) vocabularies, ideas, and values. The analytic also considers government as a rational and thoughtful activity—how does government as an assemblage think? How does it approach problems, and how does it attempt to overcome those problems? He asks "How do these practices of governing give rise to specific forms of truth?" Thought is embedded in institutions and practices and therefore made practical and technical (Dean, 2010, p. 27).

From this perspective, thought is a collective rather than an individual activity. It is not a matter of the representation of the individual mind or consciousness but instead collective bodies of knowledge, opinions, and beliefs. Mentalities are collective, relatively bounded unities of thought that are not readily or perfectly accessible to those who are inside them. An analytics of government attempts to show that taken for granted ways of thinking about things, in our case cyber security, are not self-evident or philosophically necessary (Dean, 2010).

Mentalities are highly associated with the discursive construction of the "problem space." This is the construction of the nature of the various problems to which government can be addressed; the ways in which those who would exercise rule have posed to themselves the question of the reasons, justifications, means, and ends. In simpler terms, the way that a problem becomes understood as *being a problem* is politically important, with implications for the types of solutions and responses that are directed toward that problem.

> An analytics of government focuses upon characteristic forms of visibility, ways of seeing and perceiving; distinctive ways of thinking and questioning, including technical vocabularies and procedures for producing truth or knowledge; specific ways of acting, techniques and technologies; and characteristic ways of making up subjects and actors. (Dean, 2010, p. 33)

Applied to cyber security, this suggests the following direction: we should pay attention to the way that cyber security is understood as a problem of government, the particular vocabularies and discourses that construct this problem, and the solutions those problematizations privilege. Given the attention to vocabularies and terminologies of government, a logical choice for analytical methods is some form of discourse analysis, of which the governmentality framework is supportive. This allows the mapping of struggles over meaning and the process by which meanings become conventionalized and "natural" (Philips & Jørgensen, 2002, p. 13).

Foucault's (2007) conception of discourses as relatively rule-bound sets of statements, which impose limits on what gives meaning (Philips and Jøgensen, 2002), fits with the analytics of government's attention to language and the way that structures of government are constructed.

For Laclau and Mouffe (1985), a discourse is a fixation of meaning within a particular domain and, in that sense, a reduction of possibilities that excludes the remainder of the field of discursivity. Discourse is therefore a continuous attempt to suture the social space and fix meaning in certain dominant ways (Andersen, 2003). We present *cyber security discourse* as the working term for a set of concepts and ways of thinking, thought of as a regularity in dispersion (Foucault) or a set of concepts of cyber security with a family resemblance (Wittgenstein). Rather than making a claim that *Cyber* is an accurate term (*pace* Singel), it reflects a discourse with continuity and certain presumptions and axioms. What makes an organization or institution part of the governmental assemblage of cyber security is the extent to which it engages with this dominant cyber security discourse. It is fundamentally a security discourse, with an orientation toward the securing of virtual space. We move now to examine the characteristic features of the cyber security discourse.

(Problem) Construction of Virtual Space

> The net is truly vast and infinite—Major Motoko Kusanagi, *Ghost in the Shell: S. A. C. Solid State Society* (2006).

There has been remarkable consistency in the construction of the information and cyber warfare “problem” over the past two decades. The following section examines these regularities in the cyber security discourse. As analysts we do not regard these regular assertions, which have achieved the status of near-unquestioned commonsense as necessarily true. Neither do we deny any value to these statements. Rather, we wish to call attention to the fact that they are frequently taken for granted and assumed to be true rather than being rigorously established through empirical research. Furthermore, there are political consequences to holding and perpetuating these assumptions. The five characteristics of the cyber security discourse that we draw attention to here are that cyberspace is ungovernable, unknowable, makes us vulnerable, is inevitably threatening, and is inhabited by a range of threatening and hostile actors on which it confers a number of advantages. These characteristics have been derived from an empirical examination of cyber security texts and discourse.

For privacy advocates, surveillance researchers and nonsecurity Internet analysts in contrast, the visibility, threats, and strategic advantages of cyberspace are constructed in near fundamental opposition. The digital environment is highly visible, with every action leaving a machine readable, potentially permanent record that can be shared and distributed. Websites leave cookies on individual computers and keep records of IP addresses, whereas Internet service providers are capable of monitoring all traffic and potentially passing this onto government. Furthermore, the structure of cyberspace is thought of as a medium that privileges the powerful, a site of powerful social sorting and surveillance (Gandy, 2003; O’Hara & Shadbolt, 2008). The individual, rather than a locus of power (and threat), is constructed as at risk, lacking fundamental skills and also little political power to determine the architecture and processes of cyberspace.

Cyberspace Is Ungovernable

The first generation of Internet theorists tended to see the Internet as essentially ungovernable in nature (Lessig, 1999) and that information communications technology inherently favored decentralized groups over hierarchies. Instead, Lessig (1999) argues this rhetoric ignored the constructed nature of virtual space and that regulation depends on chosen architectures, which are in turn based on active, political decisions. This rhetoric has been largely adopted by cyber security discourse with the result that virtual space is assumed to be anarchic, both currently ungoverned and in the more defeatist moments, structurally ungovernable. The metaphors at play here are cyberspace as an ungoverned "global commons" or the American "Wild West" prior to the establishment of proper government (Rattray et al., 2010, p. 149) populated by antagonistic "white hats" and "black hats." Cyberspace is constructed as unbounded, or at least missing the familiar boundaries of physical space around which much military and state strategies (and relations) have been formed. A concern is "jurisdictional arbitrage"—in which cyber attacks originate from uncovered physical areas (Bhalla, 2003, p. 329; see also Ksheti, 2005). Cyberspace is also constructed as technologically protean:

> There is a critical difference between security of cyberspace and the security of other domains such as land, sea and air; in cyberspace, the domain itself is constantly changing through continuous and fast-paced innovation. (H. Lewis, 2010, p. 5)

> A unique characteristic of cyberspace is its rapid pace of change. Although nations have long competed in the sea and air, thanks to advantages derived through technological innovation, the fundamental physical forces and terrain of those environments do not change.(Rattray et al., 2010, p. 142)

Wall argues that science fiction accounts of cyber crime have constructed cyberspace as "criminogenic"—it actively encourages criminal behavior that would not have otherwise occurred (Wall, 2008, p. 869).

Cyberspace Is Unknowable

Dean's analytics of government suggests attention to the "fields of visibility" of government, those maps and pictures by which relations of power and authority are constituted in space, and what is to be governed is described; "by what kind of light it illuminates and defines certain objects and with what shadows and darkness it obscures and hides others" (Dean, 2010, p. 41). Dean's example of crime risk management strategies present "social and urban space as a variegated field of risk and crime in which high-risk spaces suffer from a lack of visibility and inspectability" (Dean, 2010, p. 41). Haggerty (2006b) emphasizes the importance of visibility and fields of vision in military conflict. Part of the problem of cyber security in this discourse arises from the very unintelligibility of the space; it is unknown and potentially unknowable, shifting and protean, anonymous, and full of dark corners in which threats may hide. This is constructed in contrast to traditional military and governmental security problems, in which actors, intentions, and capabilities were supposedly identifiable (Bendrath, 2001). Lack of visibility is problematic for risk management approaches in that risk becomes opaque. For "E-Crime" ACPO finds barriers to a clear understanding that include underreporting, lack of awareness of a crime being committed, and the structure of crime recording framework (Amoo & Thomson, 2009, p. 2). Wall (2008) argues that rather than cyberspace being anonymous, investigators simply lack the human and technological resources to follow available trails. Therefore, this security discourse conceals a call for greater resources. The U.K. Cyber Security Strategy reflects these concerns about the visuality of the space of cyberspace:

> Cyberspace cuts across almost all of the threats and drivers outlined in the National Security Strategy: it affects us all, it reaches across international borders, it is largely anonymous, and the technology that underpins it continues to develop at a rapid pace. (Cabinet Office, 2009a, p. 3).

This parallels the offline distinction drawn between safe (modern, postmodern) zones of order and dangerous, premodern “zones of chaos” (Cooper, 2003). This aspect of the field of visibility in cyber security discourse can be anticipated by the governmentality studies’ understanding of the international as striated, multiple, hierarchical space, marked by various attempts to constitute and govern by a wide range of agencies to a variety of ends (Dean, 2010).

Cyberspace Makes Us Vulnerable

Many cyber security professionals consider that countries and societies reliant on information technology are at greater risk from information warfare. This is repeatedly echoed in the cyber security literature:

> The UK is increasingly dependent on cyberspace. As cyberspace continues to evolve, we will pursue the increasing number and variety of benefits that it can offer; however, with growing dependence also comes a greater exposure to the rapidly evolving threats. (Cabinet Office, 2009a. p. 9)

This vulnerability is often associated not only with a sense of the potential of technology to cause damage but also our reliance on the technology itself. It is worth critically engaging with both the probability (rather than brute possibility) of such threats and assessing concrete impacts, of which there is a paucity of open research. J. A. Lewis (2002) is skeptical of the vulnerability of critical national infrastructure to cyber war or cyber terrorism. Infrastructure, he argues, would require persistent, repeated, and simultaneous attacks to have an impact greater than routine system failure (J. A. Lewis, 2002). The consistent message of vulnerability is an example of what Furedi calls the culture of fear and the invitation to be terrorized. It involves focusing on vulnerability rather than resilience, or the benefits arising from a technology or capacity. Technological achievements are interpreted as a problem not as potential tools. The problem, however, arises from our own anxious fantasies (Furedi, 2007).

Cyberspace Is Inevitably Threatening

There is a strong temporal dimension in cyber security discourse. The problem of cyber security is constructed as inevitable and imminent but perpetually postponed. Arquilla and Ronfeldt’s (1997) paradigm-setting article “Cyberwar is Coming!” is continuously invoked yet deferred. Defenders “lag behind”’ attackers, and any current attacks, even if they have little impact, are taken as a “warning of the future” (Bhalla, 2003) and should be interpreted as a “wake-up call.” This security paradox prevents falsification of the cyber insecurity hypothesis. Although an attack with severe impact would be proof of the insecurity of cyberspace, an attack with no impact is not taken as a sign of security. Rather, it is always interpreted as a “near miss.” The perpetually deferred specter of cyber security is the “digital pearl harbor”; a cyber attack of such impact that it equals the Japanese surprise attack that “woke up” the United States to World War II. This specter has been invoked for nearly two decades, with each cyber incident that reaches the media articulated as proof of its encroaching inevitability. J A. Lewis (2002) identifies that much of the early literature on cyber attacks has a strong resemblance (and “unspoken debt”) to strategic bombing literature, because of its focus on asymmetry and the difficulty of defense. The concern associated with the cyber security discourse is that states have failed to sufficiently integrate information technologies such as the Internet into their security activity at organizational and tactical levels, while their opponents are assumed to have achieved just this.

> "We are in the stages before warfare," he says. "We are in the stages where people are poking around. They are trying to figure out what are the rules, the thresholds, and what the other guys are up to." Cyberspace. (Jim Lewis, CSIS, quoted in Miller, 2010)

The impact of this discourse is that existing cyber security activities are ignored. Combined with cyberspace perceived as currently ungoverned, a perception of threat with no security measures in place to counter it emerges despite existing government and private sector activity.

Cyberspace Is Inhabited by Threatening Actors

The governmentality approach suggests attention to the formation of identities (Dean, 2010). This is echoed by discourse theory, where subject positions are important elements of discourses' political character. The cyber security discourse distinguishes between legitimate and malicious actors ("white hat" and "black hat" again). Constructions of positively evaluated actors are strongly universalizing, constituting a security-supporting attitude as the default moral position. It is therefore "society" that is placed at risk by hostile and malicious actors.

Although the identity of antagonists is *unproven*, it is not *unknown*. McAfee's survey finds that security professionals believe they are under attack from "high-level" state actors and have firm beliefs about which states (Baker, Waterman, & Ivanov, 2010). J. A. Lewis (2002, p. 9) contends that stories of cyber threats often recycle threats between threat actors. "The risk remains hypothetical but the antagonist has changed from hostile states to groups like Al Qaeda." However, potentially hostile states remain active in the discourse. The states most frequently identified as having or developing a cyber war capacity are China and Russia (Billo & Chang, 2004). However, a significant element of the cyber security discourse is the way that it constructs the fundamental anonymity of cyberspace. The specificity of hostile actors is effaced, leading to a focus on possibilities and risk. Cyber security discourse constructs a fundamental and structural asymmetry between defender and attacker. This arises from the nature of networked communications technology, understood as creating "offence dominance" (Rattray et al., 2010, p. 14). U.S. National Director of Intelligence Dennis Blair told the senate select committee on intelligence that

> while both the threats and technologies associated with cyberspace are dynamic, the existing balance in network technology favours malicious actors, and is likely to continue to do so for the foreseeable future. (Miller, 2010)

Cyber security texts focus on the anonymity of cyberspace and the advantages this confers on any attacker. The identity of any responsible party is unknown or difficult to confirm; the most frequently articulated example being responsibility for the 2007 attacks on Estonian Internet infrastructure.

Wall (2008) identifies a recurring figure in cyber crime discourse—the "super-hacker" arising from the highly skilled protagonists of cyberpunk literature, with the ability to control others resulting from a massive power differential. This figure reoccurs at an international cyber security level although more likely identified with the Chinese state or the Russian Mafiya.

Cyber security discourse focuses on the (unknown, threatening) capabilities of nonstate actors. However, states benefit from a number of factors and still maintain a distinct advantage in cyberspace. If a small group can acquire a laptop cheaply, then a nation state can acquire an enormous number of laptops, run training programs, and form institutions that reap economies of scale. Nation states can develop relationships with industry. Nation states retain a political legitimacy associated with their use of violence and force within a territory or in line with international rules of war that substate groups lack or must actively campaign for. Information systems capacity—and the capacity to mount a defense against cyber warfare—is linked to a nation's technological capacity (in a broad sense, including management, skills, and innovation). The information technology on which we are constructed as reliant does not emerge fully formed from nowhere but has been developed. If reliant on technology, then some technological capacity can be assumed (this is not to say that government does not have a role in maintaining this capacity, encouraging innovation and skills development).

An example of a contemporary conflict that featured maneuvers in cyberspace were conflicts between the Russian state and Chechen militants. The Russian government was able to shut down websites used by Chechen militants and coordinate an information warfare campaign, combined with traditional kinetic operations to kill several leaders (Moore & Barnard-Wills, 2010). This combination of military power, cyber power, and political power is what gives states their advantageous position in cyber security, which is *never* isolated from "meatspace" security politics.

Implications and Conclusions

This article has developed an overview of the dominant cyber security discourse, drawing on governmentality theory and discourse analysis. It identified a particular way of constructing the "problem of cyberspace" that focused on threat, risk, and vulnerability arising from technological sources and the nature of virtual space. Discourses attempt to suture the political space. For Laclau, this is the *operation of ideology* (a term he strips of some of its pejorative connotations). All discourses contain ideological elements, and there could not be a society without an ideological dimension. We attempted to show that cyber security discourse, which is currently serving as a basis for cyber security policy in the United Kingdom and United States, and perhaps elsewhere, is but one way of understanding and conceptualizing virtual space. There are a number of implications that arise from this discourse.

First, cyber security discourse supports the militarization of online space. Haggerty argues that information war, understood as an ongoing feature of the contemporary international environment, means that war essentially becomes permanent, part of the "ongoing military gamesmanship of cyberspace" (Haggerty, 2006b, p. 252). Constructing cyberspace as a source of national security threat encourages the application of security practices from other environments that may be inappropriate or actively harmful to online activity. The language of attack and defense and of "cyber war" risks pushing out the needs of the civil sector and individual Internet users, reducing openness and increasing surveillance. Security discourses risk shutting down discussion about Internet policy, moving it from relatively open areas of government to the closed world of national security decision making. This risks excluding an important range of actors. Furthermore, constructing cyberspace as a site of risk and threat poses the potential of a self-fulfilling prophecy as that space is increasingly militarized by various parties. Nations do not operate in a vacuum and there is the possibility (although not the necessity) of a cyberspace security dilemma.

Governmental assemblages can make political accountability and transparency of decision making diffused through amorphous partnerships. Lessig (1999) argues that indirect regulation misdirects responsibility. When government uses other structures of constraint to affect a constraint it could impose directly, it muddies the responsibility for the constraint, thus undermining political accountability. Burying policy choices in complex networks of actors potentially blurs the link between regulation and its consequences (Lessig, 1999). Care should be taken that cyber security relationships between the public sector and private sector should be transparent and democratically accountable.

Focusing purely on technological capabilities and vulnerabilities, wielded or exploited by faceless hostile actors, pushes out a consideration of the wider political, legal, and normative structure that surrounds these. Presenting technologically advanced societies as highly vulnerable is to invert a much deeper structural asymmetry between developed and developing countries and between states and individuals. It also confuses risk calculations, driven by possibility rather than probability or intention. Focusing purely on technological possibilities exaggerates the impact of "asymmetric" actors and ignores other resources of states. A greater attention needs be paid to the political and international dimensions surrounding cyber security.

Finally, the perpetually deferred threat and assumption of vulnerability arises from limited quantitative and qualitative data in the public domain. This allows a cyber security discourse to operate from a position of power derived from "expertise" and makes it hard to debate the claims made by industry for the prevalence of serious cyber threats. This leads to policymaking dominated by possibility and technological capability excluding the broader social, political, and international complex that surrounds and contextualizes cyber security.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Amoo, P., & Thomson, N. (2009). *ACPO E-crime strategy*. London, England: Association of Chief Police Officer of England, Wales and Northern Ireland.

Andersen, N. A. (2003). *Discursive analytical strategies: Understanding Foucault, Koselleck, Laclau, Luhmann*. Bristol, England: Policy Press.

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is coming! In J. Arquilla & D. Ronfeldt (Eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 23-60). Santa Monica, CA: RAND.

Baker, S., Waterman, S., & Ivanov, G. (2010). *In the crossfire: Critical infrastructure in the age of cyber war*. Santa Clara, CA: McAffee.

Bendrath, R. (2001). The cyberwar debate: Perception and politics in U.S. critical infrastructure protection. *Information & Security, 7*, 80-103.

Bhalla, N. (2003). Is the mouse click mighty enough to bring society to its knees? *Computers & Security, 22*, 322-336.

Billo, C., & Chang, W. (2004). *Cyber warfare: An analysis of the means and motivations of selected nation states*. Hanover, NH: Institute for Security Technology Studies at Dartmouth College.

Brown, W. (2006). *Regulating aversion: Tolerance in the age of identity and empire*. Oxford, England: Princeton University Press.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.

Cabinet Office. (2008). *The national security strategy of the United Kingdom: Security in an interdependent world*. London, England: TSO.

Cabinet Office. (2009a). *Cyber security strategy of the United Kingdom: Safety, security and resilience in cyberspace*. London, England: TSO.

Cabinet Office. (2009b). *National security strategy—2009 update published*. Retrieved from http://www.cabinetoffice.gov.uk/newsroom/news_releases/2009/090625_security.aspx

Cooper, R. (2003). *The breaking of nations: Order and chaos in the twenty-first century*. New York, NY: Grove Press.

Dean, M. (2010). *Governmentality: Power and rule in modern society* (2nd ed.). London, England: SAGE.

Department of Homeland Security. (2009). *A roadmap for cybersecurity research*. Retrieved from www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

Emmers, R. (2009). Securitization. In A. Collins (Ed.), *Contemporary security studies* (pp. 136-151). Oxford, England: Oxford University Press.

Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France 1977-1978*. Houndmill, England: Palgrave.

Furedi, F. (2007). *Invitation to terror: The expanding empire of the unknown*. London, England: Continuum.

Gandy, O. H. (2003). Data mining and surveillance in the post-9/11 environment. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime, terrorism and warfare in the information age* (pp. 26-41). London, England: Pluto Press.

Get Safe Online. (2010). *Security is your responsibility*. Retrieved from http://www.getsafeonline.org/nqcontent.cfm?a_id=1143

Government Communications Headquarters. (2009). *GCHQ to host UK cyber security operations centre* [Press Release]. Retrieved from http://www.gchq.gov.uk/Press/Pages/Cyber-Security-Operations-Centre.aspx

Glynos, J., & Howarth, D. (2007). *Logics of critical explanation in social and political theory*. London, England: Routledge.

Haggerty, K. (2006a). Tear down the walls: On demolishing the Panopticon. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and beyond* (pp. 23-45). Cullompton, England: Willan.

Haggerty, K. (2006b). Visible war: Surveillance, speed and information war. In K. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 250-278). Toronto, Ontario, Canada: Toronto University Press.

Karatzogianni, A. (2008). *Cyber-conflict and global politics*. Oxford, England: Routledge.

Ksheti, K. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11*, 541-562.

Laclau, E., & Mouffe, C. (1985). *Hegemony and socialist strategy*. London, England: Verso.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.

Lewis, H. (2010). Cyber security intelligence: Time for some perspective. *RUSI Monitor, 8*(3), 4-6.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Centre for Strategic & International Studies.

Miller, J. (2010). Government needs to define cyber war. *Federal News Radio*. Retrieved from http://www.federalnewsradio.com/index.php?sid=1880751&nid=35

Moore, C., & Barnard-Wills, D. (2010). Russia and counter-terrorism: A critical appraisal. In A. Siniver (Ed.), *International terrorism post 9/11: Comparative dynamics and responses* (pp. 144-167). London, England: Routledge.

National Security Council. (2010). *The comprehensive national cybersecurity initiative*. Retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7*, 61-73.

Obama, B. (2009, May 29). *Remarks by the president on securing our nation's cyber infrastructure* [Speech]. Retrieved from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

O'Hara, K., & Shadbolt, N. (2008). *The spy in the coffee machine: The end of privacy as we know it*. Oxford, England: Oneworld.

Philips, L., & Jøgensen, M. W. (2002). *Discourse analysis as theory and method*. London, England: SAGE.

Ransom, J. S. (1997). *Foucault's discipline: The politics of subjectivity*. Durham, England: Duke University Press.

Rattray, G., Evans, C., & Healy, J. (2010). *American security in the cyber commons*. In A. M. Denmark & J. Mulvenan (Eds.), *Contested commons: The future of American power in a multi-polar world* (pp. 137-176). Washington, DC: Center for a New American Security.

Secretary of State for Culture, Media and Sport & Minister for Communications, Technology and Broadcasting. (2009). *Digital Britain: Final report*. London, England: TSO.

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society, 11*, 861-884.

Bios

David Barnard-Wills is a Research Fellow in the Department of Informatics and Systems Engineering at Cranfield University. Research interests include surveillance, security studies, and the politics of information technology. His research blog can be found at www.surveillantidentity.blogspot.com.

Debi Ashenden is Senior Lecturer in the Department of Informatics and Systems Engineering at Cranfield University. Specialises in information assurance, risk assessment, human factors and information security awareness.