A CYBERWAR OF IDEAS? DETERRENCE AND NORMS IN CYBERSPACE

Tim Stevens, King's College London

Contact: tcstevens@gmail.com

Published as:

Tim Stevens (2012), 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace',

Contemporary Security Policy, vol. 33, no. 1, pp. 148-170.

ABSTRACT This article relates US efforts to develop strategic 'cyber deterrence' as a means to deter adversarial actions in and through global cyberspace. Thus far, interests-based cyber deterrence theory has failed to translate into effective US policy and strategy, due to a divergence between the operational idiosyncrasies of cyberspace and an over-reliance on Cold War models of deterrence. Even whilst explicit cyber deterrence strategy falters, the US is pursuing a norms-based approach to cyber strategy generally, and hopes to derive deterrent effects from its attempts to broker international agreements pertaining to the 'rules of the road' for the proper and productive use of cyberspace. The US is not the only norm entrepreneur in this policy space, however, and this article examines how a range of other state and non-state actors are complicating efforts to develop normative regimes that might reduce risks to and from cyberspace. The article concludes that a norms-based approach to cyber deterrence might engender deterrent effects at the state level but is unlikely to do so in the case of 'rogue' states and many non-state actors. States will continue, therefore, to develop punitive deterrence capabilities to respond to these actors.

The contemporary ubiquity of information communications technologies (ICTs) is emblematic of the 'astonishing paradox, uncertainty and irreversibility of the patterns of global emergence'.[1] The growth of a global 'cyberspace' has occurred over a relatively short space of time and citizens, companies and states alike are, whilst eagerly exploiting the opportunities such an environment affords, still uncertain about its longer term effects and implications. Policymakers find themselves always playing 'catch-up' with respect to a dynamic and fast-moving phenomenon whose one defining characteristic seems sometimes to be the ability to confound traditional perspectives on strategy and politics. Central to governmental concerns is the potential harm that might be meted out by adversaries utilising cyberspace for their own strategic ends. Of the relationship between cyberspace and national security, US President Barack Obama said in May 2009, 'It's the great irony of our Information Age — the very technologies that empower us to create and to build also empower those who would disrupt and destroy.'[2] Information networks are essential to the proper functioning of modern states and the vulnerabilities of these systems to subversion and degradation have become greatly concerning to those charged with developing and maintaining critical information infrastructures. Such are the worries over the potential effects on national security and economic well-being should deeply interconnected and interdependent ICT systems fail due to accidents or adversarial actions that the once-obscure concerns of the information security professional have been elevated to the level of national policy and strategy.[3] Specifically, cybersecurity — cyberspace security *sensu lato* — is no longer exclusively the preserve of the engineer, the programmer, or the system administrator, but has become the responsibility of the soldier, the politician, and the diplomat too.

One key consideration for strategists and politicians has been on how to deter adversarial actions in cyberspace. Treated as an operational domain alongside land, sea, air, and space, the exigencies of cyberspace have demanded that due consideration be given to developing forms of 'cyber deterrence' in the pursuit of national and international security. In this article, I examine how the United States, as the pre-eminent Western political and military actor, has attempted to develop cyber deterrence as a strategic instrument since the 1990s. I argue that a body of cyber deterrence theory has developed, particularly since the 'cyberwars' in Estonia (2007) and Georgia (2008), but which has largely failed to translate to concrete policy and strategy. The conditions pertaining in cyberspace are such that it has been difficult to transfer the procedures and techniques of Cold War deterrence to this domain. As such, cyber deterrence may form one of a suite of 'complex deterrence' measures in a post-Cold War world, whose outcomes and objectives are less absolute and more pragmatic than those of the preceding era of nuclear bipolarity.

---

[1] John Urry, *Global Complexity* (Cambridge: Polity, 2003), p.12.

[2] 'Remarks By the President on Securing Our Nation's Cyber Infrastructure', 29 May 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[3] For an historical account of this process, see Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008), pp.41-65.

At the same time, I argue that as cyber deterrence has yet to have a great impact on the pursuits of national and international security, the US is developing another strand of cyber strategy and policy through which it hopes to derive deterrent effect. The development of norms has become a central focus of US initiatives in the global policy space, one implication of which is to nurture a variety of normative concepts intent on increasing global stability in cyberspace, to instigate a global culture of cybersecurity, and to develop 'rules of the road' for military and offensive uses of cyberspace. In conjunction with the material resources of a global hyperpower, this 'norms-based approach' to cyber deterrence is intended to deliver deterrent effect where an 'interests-based approach' has thus far struggled on its own.

This article is organised in four sections. The first relates a genealogy of US cyber deterrence in theory and in practice through which is illustrated its development, its problems, and its deployment thus far in policy and strategy. The second section outlines briefly the relationships between norms and deterrence, and the third section builds upon this by examining how norms and cyber deterrence are related in current attempts by the US to promote norms through global policy and strategy. The fourth section seeks to counterbalance the emphasis on the US by considering how other actors such as Russia and China are also acting as norm entrepreneurs and identifies where conflicts of interest and ideology have thus far arisen. I conclude by assessing the possible future trajectories of norms-based cyber deterrence.

A Genealogy of US Cyber Deterrence

The term 'cyber deterrence' continues to vary in meaning and emphasis but this section means to illustrate how it has evolved as a concept and as an element of US strategy. Although I have sympathy with Jeffrey Knopf's suggestion that it is perhaps too early to grant cyber deterrence a 'meaningful review' relative to other forms of deterrence on account of the sparseness of available sources, there are sufficient resources to at least commence a preliminary investigation ahead of the further work that is undoubtedly required.[4] The roots of cyber deterrence are in the thinking and theorising associated with the postulated information-technological Revolution in Military Affairs (RMA), specifically in considerations of information warfare (IW) in the wake of the early successful phases of Operation Desert Storm in Iraq (1991). Information warfare views information as a weapon 'in and of itself', and is therefore distinguishable from a related concept like network-centric warfare (NCW), which looks to exploit information in order to enhance the effectiveness of conventional weapons and tactics.[5] We may also distinguish between two forms of IW, as did John Arquilla and David Ronfeldt in their oft-cited 1993

[4] See, Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research', *Contemporary Security Policy*, Vol.31, No.1 (April 2010), p.2.

[5] David Betz, 'The More You Know, The Less You Understand: The Problem with Information Warfare', *Journal of Strategic Studies*, Vol.29, No.3 (June 2006), p.509.

article, 'Cyberwar is Coming!'.[6] They differentiated between strategic-level 'netwar', which constitutes a 'societal-ideational' conflict mediated by networked information communications technologies (ICT), and 'cyberwar', which connotes an operational-tactical form of information conflict between organised state militaries.[7] This distinction remains a useful one in discussions of information conflict and has been influential in the development of doctrinal thinking about IW, particularly in the United States.[8]

Also writing in 1993, futurists Alvin and Heidi Toffler quoted Duane Andrews, then Assistant Secretary of Defense for C3I (Command, Control, Communications and Intelligence), on the possibilities of 'knowledge warfare' in which 'each side will try to shape enemy actions by manipulating the flow of intelligence and information'.[9] Similarly, General John Sheehan, then commander-in-chief of US Atlantic Command, suggested that IW might have a distinct deterrent effect on a potential adversary, if it were possible 'to change his perception so that clearly before he decides to start a conflict he knows deep down he is going to lose'.[10] Arquilla and Ronfeldt noted that 'netwar might be developed into an instrument for trying, early on, to prevent a real war from arising. Deterrence in a chaotic world may become as much a function of one's cyber posture and presence as of one's force posture and presence.'[11] They recognised also, however, that the military forces made possible and perhaps required by IW strategy might look too small and 'unusual' to create an 'intimidation effect' comparable to that derived from conventional forces, 'thereby vitiating crisis and deterrence stability'.[12] To mitigate this, early warning systems would have to be developed in order to ascertain adversarial intentions, and it might be necessary to display capabilities as a means of signalling resolve to potential and actual enemies.[13]

In 1996, Arquilla and Ronfeldt focused once more on the topic of netwar, concluding that deterring netwar might be somewhat problematic. They argued that netwar would be similar in form to other low-intensity conflicts which favour the aggressor; indeed, they suggested that the 'age-old cycle of action and

---

[6] John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy*, Vol.12, No.2 (Spring 1993), pp.141-65.

[7] Although this need not necessarily be hi-tech, as their example of 13th-century Mongol 'cyberwar' attests: ibid., pp.148-50. The original use of the term 'cyber deterrence' occurs in the battlefield context; see, James Der Derian, 'Cyber-Deterrence', *Wired*, Vol.2, No.9 (September 1994), www.wired.com/wired/archive/2.09/cyber.deter_pr.html.

[8] See, Matt Bishop and Emily O. Goldman, 'The Strategy and Tactics of Information Warfare', *Contemporary Security Policy*, Vol.24, No.1 (June 2003), pp.113-39.

[9] Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston, MA: Little, Brown and Company, 1993), p.140.

[10] Brian E. Fredericks, 'Information Warfare at the Crossroads', *Joint Force Quarterly*, Vol.17 (Summer 1997), p.98.

[11] Arquilla and Ronfeldt, 'Cyberwar is Coming!', p.146.

[12] Ibid., p.160.

[13] Ibid.

reaction between offense and defense appears to be under way again'.[14] Given the related difficulty of identifying attackers – the recurrent 'attribution problem' – deterrence-by-denial might be the only deterrent option; when attackers could be identified, retaliatory and punitive measures could be enacted to dissuade others from subsequent attacks.[15] Richard Harknett reconceptualised netwar and cyberwar in terms of the 'contestability of connectivity', and examined the implications for deterrence strategy, specifically the strategic dynamic between information-sharing and rationality at the heart of deterrence.[16] Harknett concluded that in netwar and cyberwar frameworks, in which the control of connectivity is key, deterrence would be only a 'by-product' of 'an imposing offensive capability and a formidable ability to defend', rather than the central focus of strategy as it was during the nuclear era of the Cold War.[17] Others argued that the United States required a specific declaratory policy about its response to both 'cyberwar' and 'media war' events, if deterrence was to have any chance of working.[18]

Related to this was the assertion that US 'information advantage' would be sufficient to deter external actors: deterrent effects would be generated beneath a US 'information umbrella', analogous to the extended nuclear deterrent provided by the US to its allies during the Cold War.[19] The development of international legal frameworks and concise definitions was also considered and explicit comparisons made between ICTs and nuclear technologies in terms of their potential psychological effects and impact on state sovereignty.[20] Few advances occurred in thinking about information warfare and deterrence in the latter half of the 1990s, with the exception of pointing out, first, the potential 'blowback' against one's own systems should IW be pursued,[21] and the logical endpoint of information deterrence, that it must be 'ubiquitous and universal' to forestall the temptation to launch a first strike.[22]

---

[14] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND Corporation, 1996), p.94.

[15] Ibid., p.97.

[16] Richard J. Harknett, 'Information Warfare and Deterrence', *Parameters*, Vol.26, No.3 (Autumn 1996), pp.93-107.

[17] Ibid., p.107.

[18] Richard E. Hayes and Gary Wheatley, *Information Warfare and Deterrence* (Washington, DC: National Defense University Press, 1996), p.23.

[19] William T. Owens and Joseph Nye, 'America's Information Edge', *Foreign Affairs*, Vol.74, No.2 (March/April 1996), pp.20-36; similar sentiment informs Martin C. Libicki, 'The Emerging Primacy of Information', *Orbis*, Vol.40, No.2 (Spring 1996), pp.261-74.

[20] Timothy L. Thomas, 'Deterring Information Warfare: A New Strategic Challenge', *Parameters*, Vol.26, No.4 (Winter 1996/97), pp.81-91.

[21] Peter D. Feaver, 'Blowback: Information Warfare and the Dynamics of Coercion', *Security Studies*, Vol.7, No.4 (Summer 1998), pp.88-120.

[22] Stephen Blank, 'Can Information Warfare Be Deterred?', *Defense & Security Analysis*, Vol.17, No.2 (Summer 2001), pp.121-138. A curious parallel can be found in the writings of French urbanist and critical theorist Paul Virilio, who has repeatedly noted the advent of a 'second deterrence' based upon strategic information control; see, Paul Virilio, *Strategy of Deception*, tr. Chris Turner (London: Verso, 2000).

These authors laid a firm basis for the study and practice of information warfare and deterrence but it was not until the late 2000s that what we today understand as 'cyber deterrence' came to the fore in national security discourse. The themes of earlier work persisted but were given new focus after the so-called 'cyberwar' events of Estonia (2007) and Georgia (2008), and by the Google-China 'cyber espionage' affair of 2009/10. When a prominent US military scholar wondered in a mainstream strategic studies journal if the Estonian example constituted 'Web War I', this indicated a level of institutional concern likely to account for much of the recent attention granted 'cyber' issues, not least the focus on how to protect against and prevent similar fates befalling one's own countries.[23]

Rattray notes that the 1990s was characterised more by a focus on 'the use of perception management than with digital attacks on information infrastructures'.[24] By contrast, more recent work has tended to concern itself with the deterrence of 'cyber attacks', understood as adversarial computer-mediated actions against critical information infrastructures (CII) and other IT-networked national assets, including those of the military and security services.[25] Lesser elements are dedicated to the deterrence of espionage perpetrated through computer networks ('cyber espionage'), forms of criminality mediated by computer networks ('cyber crime'), and the threat of terrorist attacks in, on or through cyberspace ('cyber terrorism'). At the technical level – which is not considered further here – cybersecurity professionals are engaged in developing and implementing preventive and protective measures for tactical CII protection in a dynamic environment characterised by near light-speed communication. At the political and strategic level, cyber deterrence theory has evolved as a body of work concerned with deterring adversarial actors from launching such actions against friendly CII, across the state and non-state spectrum. In common with other forms of deterrence, cyber deterrence connotes the use of threats to discourage or dissuade another party from taking actions against oneself, in this context usually understood as a state or, more accurately, the constituent components and assets of such. At the heart of these threats is the communication that the costs and risks associated with such potential actions outweigh any possible benefits that might accrue to the attacker. The aim of deterrence therefore is to prevent action from

[23] Stephen Blank, 'Web War I: Is Europe's First Information War a New Kind of War?', *Comparative Strategy*, Vol.27, No.3 (May 2008), pp.227-47.

[24] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: The MIT Press, 2001), p.316.

[25] A very select bibliography includes: Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009); Richard L. Kugler, 'Deterrence of Cyber Attacks', in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Dulles, VA: Potomac Books Inc., with National Defense University Press, Washington, DC, 2009), pp.309-40; Kevin R. Beeker, Robert F. Mills, and Michael R. Grimala, 'Applying Deterrence in Cyberspace', *IO Journal*, Vol.1, No.4 (February 2010), pp.21-7; Kenneth Geers, 'The Challenge of Cyber Attack Deterrence', *Computer Law & Security Review*, Vol.26, No.3 (May 2010), pp.298-303; Will Goodman, 'Cyber Deterrence: Tougher in Theory Than in Practice?', *Strategic Studies Quarterly*, Vol.4, No.3 (Fall 2010), pp.102-135.

taking place by convincing an opponent that such action would be more deleterious than advantageous to its interests.[26] Deterrence is ordinarily understood in two forms: deterrence by punishment, in which the costs borne by an attacker are maximised, or deterrence by denial, in which the benefits to the attacker are minimised.[27]

A double-move is evident in the body of work concerned with cyber deterrence. First, as stated above, attention has moved to the deterrence of a range of cyber threats rather than on strategic information warfare itself. This is due to concerns about the exploitation of inherent vulnerabilities in computer networks deemed critical to the proper functioning of modern states. As Libicki notes, 'there is no forced entry in cyberspace', and the vulnerabilities which might allow intruders access to sensitive systems are effectively intrinsic to the architecture of computer networks, even if they might take years to be identified.[28] The second move is a function of the first: as critical information infrastructures span the public-private divide, the boundaries between civilian and military responsibilities have become blurred; we therefore see a range of problems thrown up by uncertainty over proper jurisdictions at the national level. The literature has tended to present this as a crucial issue, although is far from resolving when military intervention in civilian networks is appropriate, or what the responsibility of civilian actors (principally, industry) is for issues deemed critical to national security. The lack of explicit national strategies or international strategic coordination is also a common bone of contention.

This later phase of literature has not effaced the theoretical efforts of earlier authors. This is to be expected, as theories of deterrence are well understood, even if the practical and technical implementations of cyber deterrence are less obvious. It is, however, fair to adduce the increased sophistication of recent contributions to the literature, of which Martin Libicki's *Cyberdeterrence and Cyberwar* (2009) RAND study for the US Air Force is exemplary.[29] This is in part due to the increased use of ICTs during the intervening period, and also to elevated awareness and understanding of attendant security concerns relative to the 1990s. All authors have therefore benefited from a substantially richer dataset and conceptual background with which to enhance their analyses.

---

[26] This is distinct from compellence, which aims to make an adversary 'perform', either by making it do something against its will or by changing the course of action upon which it has already embarked; Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), pp.69-70.

[27] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961), pp.14-16.

[28] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), pp.31-7.

[29] Libicki, *Cyberdeterrence and Cyberwar*.

Yet cyber deterrence theory has ossified around a series of conceptual sticking points. Rather than rehearse the substantial body of theory here, it may suffice to illustrate this initially with reference to classical models of rational deterrence, before suggesting how cyber deterrence fits with more expansive models of deterrence. Specifically, if we compare cyber deterrence with Patrick Morgan's six elements of classical (nuclear) deterrence theory, we see that cyber deterrence as proposed by many theorists fails to satisfy any of these conditions.[30] First, there exists no severe conflict in the military sense, despite protestations to the contrary. Second, the classical presumption of rationality is warped due to the prevalence of non-state actors as agents of cyber conflict. Third, the concept of a retaliatory threat is undermined due to the problem of attributing identities and geographic locations to adversaries. Fourth, the concept of unacceptable damage is complicated by the inability to hold adversaries' assets at repeated risk, if these can even be identified. Fifth, credibility is sorely tested by a number of factors, not least of which are the absence of rules of engagement, uncommunicated military capabilities, and the likelihood of collateral damage in response. Sixth, stability is extremely difficult to achieve given the escalatory nature of cyber conflict, and the potential for it to spill over into physical conflict.

It might therefore appear that cyber deterrence is doomed but it is axiomatic to most authors that cyber deterrence is different from nuclear deterrence.[31] In a mechanistic sense, this is incontrovertible. For example, the comparison of cyber deterrence with classical models of rational deterrence finds serious problems in operationalising the same planning assumptions in both the nuclear and cyber environments, as outlined above. Proponents of cyber deterrence therefore argue that whilst there are opportunities to derive deterrent benefit from specific forms of limited action in cyberspace these are not directly derived from conventional deterrence models. Although Jeffrey Knopf was unable to include cyber deterrence in his proposals for a 'fourth wave' of deterrence research due to a relative lack of published work, thinking on cyber deterrence does share many of the characteristics of his postulated research program.[32] First, in broad terms it is, as already mentioned, mainly 'conceptual and policy-oriented', and has undergone limited empirical testing.[33] Second, the recent work on cyber deterrence is also principally in response to actual events, as evinced by an appreciable acceleration in research output since the events in Estonia and Georgia in 2007-2008. Third, cyber deterrence theorists also work on the basis that deterrence remains 'viable and relevant', but within a wide policy framework that does not rely exclusively on the use of the tools of military power, perhaps as part of a suite of post-Cold War strategic instruments loosely bundled

[30] Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003), p.8.

[31] The most coherent exposition of this thesis is Libicki, *Cyberdeterrence and Cyberwar*, pp.39-74.

[32] Knopf, 'The Fourth Wave in Deterrence Research'; see also Amir Lupovici, 'The Emerging Fourth Wave of Deterrence Theory – Toward a New Research Agenda', *International Studies Quarterly*, Vol.54, No.3 (September 2010), pp.705-32.

[33] A conscious attempt to redress this imbalance is provided by Goodman, 'Cyber Deterrence: Tougher in Theory Than in Practice?'

under the umbrella of 'complex deterrence'.[34] Fourth and very importantly, single deterrence failures do not, unlike those of nuclear deterrence, portend societal destruction, *contra* claims of 'cyber doom' promulgated through spurious analogies such as 'electronic Pearl Harbor' and 'digital 9-11', neither of which historical event resulted in national meltdown either.[35]

It may be that cyber deterrence can be understood and developed as a form of complex deterrence which, as Knopf argues, may only be 'partially effective' and 'less than ideal' but is better than no deterrence at all; the important consideration is 'whether deterrence can make a positive contribution at the margins'.[36] For this reason alone, perhaps, cyber deterrence by denial has tended to become a default option, both in its pre-event (defence) and post-event (resilience, consequence management, 'risk absorption') forms, even if it is not always framed as such.[37] Indeed, it is debatable whether denial is technically a form of cyber deterrence: if a cyber operation is denied, it is by definition not deterred, even if the next event might be. According to Harknett *et al*, denying a cyber attack does not change an attacker's 'decision calculus' from aggressive to non-aggressive, even if it makes the attainment of his objectives that much more difficult in technical terms.[38] This does not mean then that all cyber deterrence need be defensive. As Arquilla argues, 'the prospect of warding off a bloody fight by the nonlethal means of disrupting military command and control via cyberspace-based weapons is one that should not be passed over easily'.[39] Additionally, the US should adopt 'cyber intervention' as a tactic for 'security and stability', not just as an aggressor but as a defender and provider of global human security.[40] Cyberspace might also be the medium of other deterrence efforts, such as counter-terrorism 'deterrence by delegitimisation', in which terrorists' beliefs are targeted through information and propaganda campaigns as an alternative to denial and punishment measures.[41]

---

[34] On 'complex deterrence', see T.V. Paul, 'Complex Deterrence: An Introduction', in T.V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), pp.1-27.

[35] Sean Lawson, 'Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History', *Working Paper 11-01*, January 2011, Mercatus Center, George Mason University, Arlington, VA.

[36] Knopf, 'The Fourth Wave in Deterrence Research', p.4.

[37] On pre- and post-event deterrence-by-denial, see Wyn Q. Bowen, 'Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism', *Contemporary Security Policy*, Vol.25, No.1 (April 2004), pp.54-70.

[38] Richard J. Harknett, John P. Callaghan and Rudi Kauffman, 'Leaving Deterrence Behind: War-Fighting and National Cybersecurity', *Journal of Homeland Security & Emergency Management*, Vol.7, No.1 (2010), Article 22, p.17.

[39] John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), p.129.

[40] Ibid., pp.129-31.

[41] Alex S. Wilner, 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism', *Journal of Strategic Studies*, Vol.34, No.1 (February 2011), pp.3-37.

What is clear is that cyber deterrence theory has yet to be translated into concrete US cyber deterrence strategy. We might here note the distinction made by Patrick Morgan between deterrence theory and strategy. Deterrence theory consists of the 'underlying principles on which any strategy is to rest', that strategy being 'specific military posture, threats, and ways of communicating them'.[42] In the US case, whilst cyber deterrence literature continues to stress the possibilities – and problems – of cyber deterrence, little of this has transferred to the policy realm or to national strategy. Richard Harknett and his colleagues have shown how the Bush administration, through documents such as the *National Strategy to Secure Cyberspace* (2003), the *National Strategy for Homeland Security* (2002/2007), and the *US National Security Strategy* (2002/2006), recognised the difficulties in operationalizing cyber deterrence whilst taking a 'middle ground approach' that included the need for denial measures and the ability to respond to, if not actually deter, offensive actions.[43] The subsequent Obama administration's *Cyberspace Policy Review* (2009) makes a single mention of deterrence in its introduction and, as Harknett *et al* point out, it is unclear whether this is a reference to a forthcoming deterrence strategy or 'simply the inclusion of deterrence effects achieved through denial capabilities'.[44] They argue further that cyber deterrence is so discredited as a US strategic option that it should be discarded totally and replaced by a more traditional warfighting posture designed to respond to a spectrum of acts of 'cyberaggression', thereby moving away from 'the fifty-plus year comfort zone of deterrence as the dominant strategic anchor'.[45] However, although they are correct that cyber deterrence seemed to be slipping down the strategic agenda, since 2009 it has refused to go away completely.

The US *International Strategy for Cyberspace* (2011) makes numerous mentions of the need to develop deterrent capabilities. It talks of 'appropriate deterrence' (p.9), how the US 'will seek to encourage good actors and dissuade and deter those who threaten peace and stability through actions in cyberspace' (p.12), and the use of legal means to enhance 'domestic deterrence' in all states such that they can 'investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad' (p.13). It also refers to the utility of military alliances and partnerships that will 'bolster our collective deterrence capabilities and strengthen our ability to defend the United States against state and non-state actors' (p.21). Importantly, it draws attention to the requirement for 'a range of credible response options' in the context of 'dissuading and deterring' threats from 'terrorists, cybercriminals, or states and their proxies' (p.12). It treats 'military force' as a last resort but also warns against the 'costs of inaction' in this respect (p.14). In common with the preceding *Cyberspace Policy Review*, however, it gives little indication of what these deterrent strategies might look like or how they will be put into operation. It is therefore very

[42] Morgan, *Deterrence Now*, p.8.

[43] Harknett *et al*, 'Leaving Deterrence Behind', pp.2-4.

[44] Ibid., p.5.

[45] Ibid., p.20.

difficult to ascertain what prospects of success there might be for an explicit US cyber deterrence strategy, should one ever come into force.

The *International Strategy* would seem to indicate clearly that the US has no wish to default to a position based solely on deterrence by denial. So too the comments of the vice chairman of the Joint Chiefs of Staff General James Cartwright, who emphasised in July 2011 the need to develop cyber deterrence through both punitive and denial mechanisms. Rather surprisingly, Cartwright expressed the hope that the Department of Defense would within a decade change from being '90% focused on defense to 90% focused on deterrence'.[46] The US has significant offensive capabilities, located throughout the military and security services, and its force posture is demonstrated most clearly by the founding of a dedicated US Cyber Command in 2009, which became operational in October 2010. In January 2011, the outgoing commander of US Strategic Command, General Kevin Chilton, remarked that 'if we're going to use cybercapabilities to deter, that's going to beg for some demonstration of that capability', reiterating that the fundamental principles of deterrence obtain in cyberspace as they do in other domains.[47] If some form of signalling is required in order to progress US cyber deterrence capabilities, it is noteworthy that James Lewis of the Center for Strategic and International Studies has commented that the US derives 'little or no deterrent effect' from its 'pre-eminent offensive cybercapabilities'.[48] This prefigures Cartwright's comment that 'There is no penalty to attacking us now. We have to figure out how to change that'.[49] However, Lewis succinctly summarises the options available to the US for bolstering its cyber deterrence efforts. These include the aforementioned investment in deterrence by denial; a conscious effort to indicate constraints on US military activities in order to establish 'bounds' for cyber conflict and limit antagonism; and a renewed attention to pre-conflict signalling and inter-actor communication.[50] Lewis also drew attention to a fourth potential component of cyber deterrence strategy:

> Better defences could be reinforced by multilateral understandings on acceptable behavior in cyberspace – explicit norms and obligations .... Just as nations feel a degree of constraint from norms and agreements on non-proliferation, establishing explicit international norms for

[46] Julian E. Barnes and Siobhan Gorman, 'Cyberwar Plan Has New Focus on Deterrence', *The Wall Street Journal*, 15 July 2011.

[47] Bill Gertz, 'Show of Strength Urged for Cyberwar', *The Washington Times*, 27 January 2011.

[48] John Markoff, David E. Sanger, and Thom Shanker, 'In Digital Combat, U.S. Finds No Easy Deterrent', *The New York Times*, 26 January 2010.

[49] Barnes and Gorman, 'Cyberwar Plan'.

[50] James A. Lewis, 'Cross-Domain Deterrence and Credible Threats', Washington, DC, Center for Strategic and International Studies, 2010, p.4.

> behavior in cyberspace would affect political decisions on the potential risk and cost of cyber attack.[51]

Joseph Nye has argued similarly that cyber conflict 'can be managed through inter-state deterrence, and offensive capabilities if deterrence fails, but at some point in the future it may be possible to reinforce these steps with evolving rudimentary norms'.[52] Whilst neither Lewis or Nye explicitly categorise norms as a form of deterrence, they both use the language of 'reinforcement' to promote normative change as a key component of a national cyber strategy, working together with whatever deterrent effects can be derived from existing or future capabilities. I argue that it is the normative component of nascent cyber strategy which allows us to better understand how the US hopes to achieve forms of cyber deterrence above and beyond the military and the technical. To begin to show how and why this is the case, we must first revisit the relationships between norms and deterrence more generally, before turning to the specific case of cyber deterrence.

Norms and Deterrence

Norms are 'shared expectations about appropriate behaviour held by a community of actors'.[53] Expectations arise from intersubjective beliefs about the social and material worlds, and therefore do not exist in the private subjective beliefs of individuals but in the public social relations between individuals and in their mutual practices.[54] Norms are commonly differentiated into constitutive norms and regulative norms. Constitutive norms go 'all the way down', in Alexander Wendt's famous phrase, and create and define actor's identities and interests.[55] Regulative norms act as standards that define the proper behaviour of previously established identities and can be likened to obligations, permissions, and prohibitions, or 'rules of the road' which order and constrain actors' behaviours.[56] Norms therefore operate to shape both the means of social action and its ends. Norms differ from instrumentally rational behaviour because actors attempt to 'do the right thing' rather than purely maximise or optimise their given preferences.[57] We may therefore distinguish between norms and interests in our analytical approaches to international life.

---

51. *Ibid.*

52. Joseph S. Nye, Jr., 'Cyber Power', Cambridge, MA, Belfer Center for Science and International Affairs, Harvard Kennedy School, pp.16-7.

53. Martha Finnemore, *National Interests in International Society* (Ithaca, NY: Cornell University Press, 1996), p.22.

54. Alexander Wendt, 'Constructing International Politics', *International Security*, Vol.20, No.1 (Summer 1995), pp.73-4.

55. Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), pp.92-138.

56. Gregory A. Raymond, 'Problems and Prospects in the Study of International Norms', *Mershon International Studies Review*, Vol.41, No.2 (November 1997), p.214.

57. Thomas Risse, '"Let's Argue!": Communicative Action in World Politics', *International Organization*, Vol.54, No.1 (Winter 2000), p.4.

Theo Farrell identifies three principal ways in which norms, assuming they are complied with, 'channel, constrain, and constitute action': inducement and coercion; moral pressure and persuasion; and, social learning and habit.[58] These modes are seen as 'causal mechanisms' that determine action, although only probabilistically so, as actors retain the agency to reject or ignore norms within normative frameworks. Norms are institutionalised at different levels within global culture.[59] Thus we can determine that they exist at the world-systemic level, such as in formal international legal regimes, and in informal inter-state relations. They are also institutionalised in national policy and practices (strategic culture) and in military doctrine and structures (organisational culture). Norms are also operable across the porous boundaries of these entities, such as between militaries who are of different nationality yet also members of an identifiable professional transnational community. Norms operating at one of these conceptually distinct levels may shape and be shaped by culture at another level, so that we might see the influence of organisational culture on strategic culture, or of transnational norms on organisational culture. 'Norm entrepreneurs', exogenous shock, and intra-community personnel changes are important factors influencing these cultural dynamics.[60]

Although norms do not require the exercise of material power to persist or proliferate, they are more likely to do so if they either serve material interests or are supported by them – norms therefore may be followed both because an actor is interested in 'doing the right thing' and also because it is seeking to maximise personal utility in doing so. The study of norms does not therefore reject considerations of rational choice behaviour but rather seeks to augment and deepen the understanding of actors' strategic decision-making. In the study of deterrence, attention to norms is a means by which to acknowledge the social context of deterrence and its reflexive characteristics, a suite of factors and processes elided by purely rationalist approaches to deterrence.[61] As Lawrence Freedman argues, such an approach is more suited to understanding how deterrence 'actually works in practice'.[62] A 'norms-based approach' to deterrence – as opposed to a strictly 'interests-based approach' – is defined by Freedman as one which reinforces 'certain values to the point where it is well understood that they must not be violated'.[63] Importantly, this requires the exercise of many elements of foreign policy, rather than the use or threatened use of military force alone.[64]

---

58. Theo Farrell, *The Norms of War: Cultural Beliefs and Modern Conflict* (Boulder, CO: Lynne Rienner Publishers 2005), pp.10-11.

59. *Ibid.*, 6-7.

60. *Ibid.*, pp.12-15.

61 Lupovici, 'The Emerging Fourth Wave of Deterrence Theory', p.706.

62 Lawrence Freedman, *Deterrence* (Cambridge: Polity, 2004), p.5.

63 *Ibid.*, p.4.

64 *Ibid.*

Adler notes that deterrence strategy requires that rational actors 'hold normative assumptions about the appropriateness and proportionality of military actions'.[65] They must also be aware of the 'rules and logic of the [strategic] game', which is communicated between actors and which serves not only to inform their actions but also their identities.[66] During the Cold War, deterrence became the principal means through which strategic actors interpreted and constructed their world.[67] The norms thus internalised and institutionalised manifest as beliefs that helped shape nuclear policy and strategy for nearly half a century. One much-discussed example is that of the 'nuclear taboo', the norm of nuclear non-use which developed through the understanding that the use of nuclear weapons is *a priori* morally repugnant, regardless of any considerations of the effects of retaliation should a first strike be launched.[68] This conceptual understanding – and the general cognitive vocabulary of nuclear conflict and deterrence – was translated into concrete policy and strategy through a range of political and institutional processes, and was essential in stabilising the strategic relationship between the US and the Soviet Union.[69] Despite the ideological differences of the two superpowers, shared norms relating to nuclear weapons were a powerful binding force, without which deterrence would have been a much more complex and dangerous endeavour.

After the end of the Cold War, and in the absence of the stability afforded by the structural bipolarity of the superpower nuclear standoff, deterrence has indeed become a much more difficult proposition. This is not to say that the world itself is necessarily more complex than previously but that the entrenched deterrence mindset borne of decades of nuclear strategy has perhaps lacked a certain flexibility that would enable its continuing relevance and application to a range of strategic actors unburdened by solely nuclear considerations.[70] This applies not only to the types of 'rogue state' – nuclear or otherwise – and non-state actors such as terrorists whom states might wish to deter, but also to those collective strategic actors such as the United Nations and NATO with deterrent objectives.[71] In this more variegated strategic environment it is argued that norms-based approaches, whether through the establishment of norms of appropriate behaviours or through the development of 'deterrence communities', have more chance of

[65] Emanuel Adler, 'Complex Deterrence in the Asymmetric-Warfare Era', in Paul *et al*, *Complex Deterrence*, p.88.

[66] *Ibid.*

[67] *Ibid.*, p.89.

[68] Farrell, *Norms of War*, pp.101-114; see also, Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945* (Cambridge: Cambridge University Press, 2007).

[69] Adler, 'Complex Deterrence', p.93.

[70] This has been recognised recently by senior US defence officials; see, Jim Garamone, 'Mullen Urges New Methods of Deterrence', *American Forces Press Service*, 12 November 2010.

[71] Patrick M. Morgan, 'Collective-Actor Deterrence', in Paul *et al*, *Complex Deterrence*, pp.158-82.

success than interest-based approaches alone.[72] I argue in the following section that this observation pertains to current US 'cyber strategy' and show how this is linked to US cyber deterrence objectives.

Norms and US Cyber Strategy

In January 2008, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI) by classified joint presidential directive.[73] This was charged with reordering federal cybersecurity programs and practices, particularly with respect to adversarial actions by hackers and states. Part of its remit was to explore the possibilities for a national cyber deterrence strategy, of which its director Melissa Hathaway later confessed in an interview, 'we didn't even come close'.[74] Given our earlier comments on the relative decrease in emphasis afforded cyber deterrence in policy and strategy – even as defence academics and think-tanks are characterised by the opposite dynamic – this inability to develop a national cyber deterrence strategy should probably come as no surprise. It was around this time, however, that the issue of norms began to attract more considered attention. In the contemporary discourse and practice of US cyber strategy, norms are clearly to be understood as regulative norms. This position was set out by the non-governmental Commission on Cybersecurity for the 44th Presidency which stated in 2008:

> The U.S. willingness to cooperate with other governments on cybersecurity will be an important component of U.S. advocacy. That cooperation should focus on establishing norms, which are expectations or models for behavior .... A normative approach to international cybersecurity focuses on how countries should behave.[75]

The report proposed that all cyber strategy should reflect the national security imperatives of national defence, the advancement of US interests, and the protection of allies.[76] Norms and deterrence were grouped together as components of a proposed 'international engagement' strategy, involving 'advocacy, cooperation, norms, and deterrence'.[77]

The Commission envisaged that norms could be promoted and propagated using a combination of inducement and coercion. It noted that countries that act in violation of a norm often experience

---

[72] Adler, 'Complex Deterrence', pp.89-90.

[73]. www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[74]. Markoff *et al*, 'In Digital Combat'.

[75]. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, 2008), pp.20-1.

[76]. *Ibid.*, p.19.

[77]. *Ibid.*, p.20.

'embarrassment or stigmatization' as a result, which could presumably be avoided by respecting the norms proposed by the US. States that refused to abide by these norms could be punished with sanctions if, for example, they prosecuted cyber attacks or knowingly harboured cyber criminals within their borders. The norms in question were principally concerned with creating 'thresholds for appropriate behavior and appropriate responses'. Persuasion would also be used to encourage states to accede to the Council of Europe *Convention on Cybercrime* (2001), which the US ratified in 2006. Moral authority was evidently to be exercised initially amongst 'like-minded nations', with the intention of expanding this fraternity over time. Importantly, the US was seen as an alternative to the United Nations, which was viewed as 'politically incapable of enforcing a [global cybersecurity] treaty'.[78] This would leave the US as the principal viable authority to broker international agreements and promote behavioural norms, as well as being perhaps the only actor capable of backing punitive threats with credible and global political and military power.

Many of the ideas contained within the Commission's report were incorporated into the *Cyberspace Policy Review* (2009), commissioned by President Obama to 'assess US policies and structures for cybersecurity'.[79] The Review stated:

> The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure .... Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age.[80]

In May 2011, the US *International Strategy for Cyberspace* answered the President's call and was the first US policy document to provide, in Secretary Clinton's introductory words, 'an approach that unifies our engagement with international partners on the full range of cyber issues'.[81] Norms are promoted in the context of 'applying the broad expectations of peaceful and just interstate conduct to cyberspace' in order to effect 'stability', as obtains in 'other spheres of international relations.[82] The document stresses the collaborative and cooperative aspects of global normative change whilst reiterating states' rights to self-

78. *Ibid.*, p.21.

79. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House, 2009), p.i.

80. *Ibid.*, p.iv.

81. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, 2011).

82. *Ibid.*, p.9.

defense consistent with the UN Charter. Norms extended not only to technical issues of network functionality but also to 'upholding fundamental freedoms' consistent with several high-profile speeches by Secretary Clinton on this topic,[83] and a range of other responsibilities of states to the privacy of their citizens and so on. Importantly, the document stated, '[a]dherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict.'[84] Norms are principally therefore, although not exclusively, to be understood as regulative norms concerned with preventing interstate conflict, and can be framed as a form of norms-based deterrence.

Given the civilian context of these statements, it is perhaps not altogether surprising that norms and deterrence — with its military connotations — are not openly linked. However, explicit connections between cyber deterrence and norms are not hard to find. In late 2010, US Deputy Secretary of Defense William J. Lynn reiterated the problems inherent to cyber deterrence in an article for *Foreign Affairs*, concluding that deterrence by denial would likely bear most benefit to the United States, adding that if 'there are to be international norms of behavior in cyberspace, they may have to follow a different model [i.e. one not derived from nuclear deterrence], such as that of public health or law enforcement'.[85] Mike McConnell, formerly Director of both National Intelligence and the National Security Agency, wrote in a February 2010 op-ed largely concerned with cyber deterrence that international cooperation and engagement 'means little unless we back it up with practical policies and international legal agreements to define norms and identify consequences for destructive behavior in cyberspace'.[86] Robert J. Butler, Deputy Assistant Secretary of Defense for Cyber Policy, has stated that 'partnerships with like-minded nations' are 'actually laying a foundation for deterring bad behaviour in cyberspace'.[87]

The normative program is still at an early stage and no global US-supported framework of regulative norms has yet emerged. Nor has a coherent US strategic approach to cyber deterrence. Nevertheless, we are beginning to see the emergence of national cyber strategy in which cyber deterrence may be pursued not only through national security capabilities, but through diplomatic, information, economic and political means also, a point made explicit in the *International Strategy*.[88] Critically, the US evidently hopes that some deterrent effect can be gained through the creation of international cyberspace norms informed by US national interest. Deterrence might not obtain by these norms alone, particularly with respect to

83. Hillary Clinton, 'Remarks on Internet Freedom', Washington, DC, 21 January 2010. These remarks were reiterated and expanded in Hillary Clinton, 'Internet Rights and Wrongs: Choices and Challenges in a Networked World', Washington, DC, 15 February 2011.

84. *International Strategy for Cyberspace*, p.9.

85. William J. Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, Vol.89, No.5 (September/October 2010), p.100.

86. Mike McConnell, 'To Win the Cyber-War, Look to the Cold War', *The Washington Post*, 28 February 2010.

87. Jim Garamone, 'Official Details DOD Cybersecurity Environment', *American Forces Press Service*, 20 October 2010.

88. *International Strategy for Cyberspace*, p.14.

non-state actors, but they will be backed by the other instruments of US national power. These intentions are consistent with the concept of 'norms-based deterrence' proposed by Freedman and others.

The US is positioning itself as a global norm entrepreneur but it is by no means the only one. A long-running US-Canada academic study on global information control finds that 'as the Internet has grown in political significance, an architecture of control — through technology, regulation, norms, and political calculus — has emerged to shape a new geopolitical information landscape'.[89] Under this formulation, one function of the normative turn would be to normalise the exercise of power in cyberspace.[90] The US is far from alone in attempting to stake out vital ground in this politicised environment and in the following section, I examine how it is not the only norm entrepreneur in global cyberspace, and how its normative project is meeting with substantial opposition from other actors with their own agendas.

Norm Entrepreneurs in Global Cyberspace

Secretary Clinton's January 2010 speech called upon the UN Human Rights Council to adopt five new internet 'freedoms'.[91] Four of these were existing human rights transposed from the Universal Declaration of Human Rights (UDHR) to cyberspace: the freedoms of expression and worship, and the freedoms from want and fear. The fifth — the freedom to connect — is analogous to UDHR Article 20 — the right to peaceful assembly and association — in that 'governments should not prevent people from connecting to the internet, to websites, or to each other'. Clinton spoke of 'devoting the diplomatic, economic, and technological resources necessary to advance these freedoms' as part of what she called '21st century statecraft', and made it clear that technology in particular could be used 'to advance democracy and human rights'. She made reference to 'new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship', for their own local needs and to further US foreign policy goals. An editorial in the Chinese government-owned *Global Times* pulled no punches in its response to Clinton's speech: 'The US campaign for uncensored and free flow of information on an unrestricted Internet is a disguised attempt to impose its values on other cultures in the name of democracy ... the bulk of information flowing from the US and other Western countries is loaded with aggressive rhetoric against those countries that do not follow their lead'.[92]

---

89. Ronald Deibert and Rafal Rohozinski, 'Beyond Denial: Introducing Next-Generation Information Access Controls', in Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), pp.3-4.

90 This echoes the assertions in David Resnick, 'Politics on the Internet: The Normalization of Cyberspace', in Chris Toulouse and Timothy W. Luke, eds., *The Politics of Cyberspace* (New York: Routledge, 1997), pp.48-68.

91. Clinton, 'Remarks on Internet Freedom'.

92. 'The Real Stake in "Free Flow of Information"', *Global Times*, 22 January 2010.

Prior to Clinton's speech, the US had already intervened in the internal affairs of its Western Asian *bête noire*, Iran. During the 2009 Iranian election protests, the State Department is reported to have requested that micro-blogging platform Twitter delay planned maintenance operations in order to allow it to continue to be used for co-ordinating anti-government demonstrations and spreading dissent.[93] Although the significance of Twitter's role in the protests is unclear,[94] the US perceived it as important enough to approach a commercial company directly with a view to altering its internal decision-making process in the national interest, despite President Obama's reported desire not to be seen to be 'meddling' in Iran's domestic affairs.[95] Unsurprisingly, some officials from countries with traditions of media control have described Twitter as 'an American plot to destabilize foreign governments'.[96] Although this claim is otherwise unsubstantiated, it is evident that US intentions to promote norms consistent with its neoliberal outlook are being challenged by other states with different ideological stances. Russia, in particular, has tended to view US proposals in a dim light, as Sergei Korotkov of the Russian Defence Ministry argued in 2008:

> Practically any information operation conducted by a state or a number of states against another state would be qualified as an interference into internal affairs ... So any good cause, like promotion of democracy, cannot be used as a justification for such actions.[97]

This speaks to a fundamental difference between US and Russian views on cybersecurity, as summarised by an American thinktank:

> ... the United States focuses on a law enforcement approach at the domestic level with voluntary international collaboration, while Russia focuses on developing binding international regimes. There are also quite different philosophies at work: Russia favors social control of the Internet as a medium, while the United States, for the most part, does not.[98]

These 'philosophies' are manifest as normative frameworks that both the US and Russia are attempting to promote to other states and in multilateral fora.

---

93. 'U.S. State Department Speaks to Twitter Over Iran', *Reuters*, 16 June 2009.

94. Evgeny Morozov, 'Iran: Downside to the "Twitter Revolution"', *Dissent*, Vol.56, No.4 (Fall 2009), pp.10-14.

95. 'U.S. State Department Speaks to Twitter Over Iran'.

96. James Lewis, quoted in 'Seeing the Internet as an "Information Weapon"', *National Public Radio*, 23 September 2010, www.npr.org/templates/story/story.php?storyId=130052701.

97. Sergei Korotsov, quoted in *ibid.*

98. Franz-Stefan Gady and Greg Austin, 'Russia, The United States, and Cyber Diplomacy: Opening the Doors', New York, EastWest Institute, 2010, p.i.

One such contribution by the US is to the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, whose 2009-2010 report makes repeated reference to the development of 'norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure'.[99] The GGE continues to promote cooperation, dialogue, and collaboration between states, civil society, and the private sector to improve cybersecurity. For its part, the US State Department distinguishes five inter-related normative fields that together contribute towards a 'global culture of cybersecurity': the responsibility of states to ensure their own cybersecurity; the continued relevance of *jus ad bellum* and *jus in bello* to cyber conflict; the requirement to address the use of proxies in cyber conflict; the responsibility to allow the free flow of information along the lines of Clinton's five freedoms; and, the responsibility to combat terrorism.[100] To institutionalise these norms, the US favours a voluntary initiative rather than a negotiated treaty instrument, and prefers to pursue informal and non-obligatory transgovernmental cooperation rather than formally enforceable and binding intergovernmental coordination. Arguably, this would also avoid many potential legal constraints on the licit or illicit activities of the US and its allies in this security field.

The US has also consulted widely with strategic allies, and has chaired the NATO Group of Experts review on a new strategic concept for NATO that addresses 'cyber assaults of varying degrees of severity' as one of three most likely threats to member-states out to 2020.[101] Allies of the US like the UK have backed these initiatives and the UK armed forces minister Nick Harvey made explicit reference to the deterrent possibilities of collective action through the active application of NATO's Clause V commitment to mutual defence to aggressive acts in cyberspace.[102]

By contrast, Russia has tended to view cybersecurity as a matter of internal security rather than foreign policy. Its efforts to broker multilateral agreements have been founded on the need to control information ('content') within its sovereign borders rather than encourage the relatively unimpeded flow of information across those borders, as in the American model. Through the Shanghai Cooperation Organisation (SCO), Russia — along with China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan — in

99. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General, 30 July 2010, A/65/201,www.unidir.org/pdf/activites/pdf5-act483.pdf.

100. Deborah Schneider, 'Cyber Security Keynote Address', Organization for Security and Co-operation in Europe Joint Forum for Security Cooperation-Permanent Council, Vienna, 2 June 2010, FSC-PC.DEL/30/10, http://www.osce.org/documents/fsc/2010/06/44551_en.pdf.

101. *NATO 2020: Assured Security, Dynamic Engagement—Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO* (Brussels: NATO Public Diplomacy Division, 2010), p.17.

102 Nick Harvey, 'Cyber Warfare: Addressing the Challenge', speech, 9 November 2010, Chatham House, London.

2009 adopted an accord which defined 'information war' as 'dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States'.[103] This interpretation of 'information war' was also reported as being akin to 'mass psychologic [sic] brainwashing'.[104] In late 2011, China, Russia, Tajikistan and Uzbekistan proposed a new code of conduct for consideration by the UN General Assembly.[105] Framed in terms of 'information security', it called for a variety of sensible measures such as a curb on hostile and destabilising cyber attacks but also on the need to prevent the dissemination of information incompatible with countries' internal 'political, economic and social stability, as well as their spiritual and cultural environment'. Although we might take this to be a means of reducing external interference in domestic affairs, it has been widely interpreted as a defence of internet censorship and states' rights to prohibit access to materials deemed inimical to their ideologies.[106] Much of this document was expressed in the language of 'norms' but the unfortunate irony is that even whilst criticising the US for its hegemonic discourse, all of the SCO member-states have demonstrable histories of attempting to censor internet content, restrict access to ICTs, and otherwise shape the online media environment for the purposes of domestic political control, including through the use of physical force.[107]

Through the SCO and UN, Russia has consistently called for a global 'cyber arms control' agreement. It has been repeatedly blocked in these attempts by the US, whose chief cybersecurity coordinator in the Clinton administration viewed Russian proposals as 'largely a propaganda tool', the lack of traditional dimensionality of 'cyber arms' mitigating against the monitoring and verification of any arms control regime.[108] In addition, he noted that Russia has not signed 'the one serious international agreement on disruptive cyber activity', the Council of Europe's *Convention on Cybercrime* (2001), a conspicuous oversight given the level of cybercrime emanating from the Russian Federation.[109] These sticking points seem to be

---

[103]. Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Article 2, 16 June 2009, unofficial translation in Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law', *Texas Law Review*, Vol.88, No.7 (June 2010), fn.17.

[104]. 'Seeing the Internet as an "Information Weapon"'.

[105] Letter to UN Secretary-General, 12 September 2011, http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf.

[106] Milton Mueller, 'Russia and China Propose UN General Assembly Resolution on "Information Security"', *Internet Governance Project*, 20 September 2011, http://blog.internetgovernance.org/blog/_archives/2011/9/20/4903371.html.

[107]. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008); Deibert *et al*, *Access Controlled.*

[108]. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco Books, 2010), p.220.

[109]. *Ibid.*, p.236.

exacerbated by traditional geopolitical distrust. The United States' normative priorities derive from their outwards-facing commitments to free trade and information exchange, as well as national security concerns about offensive cyber actions against its networks. Russia's proposals also draw on concerns with security, albeit principally of an internal nature, to which are closely linked the perceived deleterious impact of Western socio-cultural norms on Russian society. Both countries are acting as international norm entrepreneurs and they do not see eye to eye. Perhaps this should not surprise us. Régis Debray, reacting to the common thesis that global information technologies render obsolescent the nation-state and 'political rivalries of yore', writes that 'territorial disputes are replaced by wars between competitors about norms, the euphemistic technological equivalent of nationalist expansion. This heralded rejection of ideology turns exorbitantly ideological in reality'.[110] This idea resonates strongly with what we are witnessing in the international political environment with respect to cyberspace and security.[111] Not least, this manifests in the degree of government intervention proposed by parties to the debate. Whereas the US wishes to devolve much of the responsibility for cybersecurity to the private companies that own and operate ICT infrastructure, Russia prefers a more interventionist and regulatory stance, for example.

Nevertheless, the prospects for some form of global cybersecurity coordination are changing. The head of the UN International Telecommunications Union has called for a treaty to prevent 'cyberwar', which would act to reduce states' inclination to launch cyber first-strikes against other states, a proposal supported by Russia, China, and many non-aligned countries, although not the US.[112] The US rejects their focus on 'content' regulation and is engaged in tortuous diplomatic negotations with the ITU on this point. Ron Deibert – himself categorisable as a left-leaning norm entrepreneur – notes that the aim of international negotiations should be 'a framework of international agreements focused on promoting norms of mutual behavior, clarification of jurisdictional responsibilities, and institutions designed to facilitate the exchange of information between security communities worldwide'.[113] Elsewhere, the Council of Europe has proposed a global internet treaty that would perform these functions and others designed to protect 'internet freedom' and the technological infrastructures of cyberspace.[114] There are also signs that the US is willing to engage with Russia on proposals to limit the military use of cyberspace,

110. Régis Debray, *Transmitting Culture* (New York: Columbia University Press, 2000), p.25.

111 On the recent US and Chinese national self-portrayals with respect to cyberspace, for example, see Stephen John Hartnett, 'Google and the "Twisted Cyber Spy" Affair: US-Chinese Communication in an Age of Globalization', *Quarterly Journal of Speech*, Vol.97, No.4 (November 2011), pp.411-34.

112. 'UN Chief Calls for Treaty to Prevent Cyber War', *Agence France-Presse*, 30 January 2010. Supporting states include many regarded as media-repressive, such as Cuba, Ethiopia, Myanmar, Sudan, Vietnam, and Zimbabwe.

113. Ron Deibert, 'Toward a Cyber Security Strategy', *Vanguard* (March/April 2010), pp.10-11.

114. 'European Cyberwar Proposal Ignites Debate at IGF', *Communications Daily*, 15 September 2010.

thereby reversing the trend of recent years.[115] In particular, an Organisation for Security and Cooperation in Europe (OSCE) resolution to share information on cyber deployments during military conflicts was co-sponsored by the US, Russia, and others in July 2011.[116] This apparent thaw led the US Cybersecurity Coordinator Howard Schmidt to comment that the 'reset' in US-Russia relations had extended itself to cyberspace.[117] However, at present, the US opposes any form of negotiated treaty instrument as robustly as Russia and her allies favour one.

At the rarefied level of state interactions, global cyberspace agreements might have some deterrent effect, serving to constrain state military and espionage activities in cyberspace, although given the problems of identity, attribution, and monitoring, its benefits may not be as obvious as with nuclear and conventional arms agreements. This is particularly pertinent if we consider the possible minimal effect on the actions of non-state actors, be they hackers, terrorists, criminals, or disgruntled citizens, especially as norms exist at many levels below the state and global society. Arquilla and Ronfeldt, for example, draw on the work of Kathryn Sikkink to illustrate their social netwar thesis, in which global information networks facilitate *inter alia* the flow of shared norms and goals, helping to form and maintain militant social activist networks, such as might be identified with online communities engaged in anti-state cyber activism.[118] Nir Kshetri has suggested that social norms may act to legitimise various forms of cybercrime, proposing that 'cybercrimes are more justifiable in some societies compared to others'.[119] Research indicates that adherence to norms of group identity in the Russophone internet community was an important factor in establishing the base of hacktivists responsible for the compromise of Estonia's internet infrastructure in 2007.[120] More generally, cyberspace is characterised by the development of 'cybernorms' as 'informal

115. Keith B. Alexander, 'US Cybersecurity Policy and the Role of US CYBERCOM', Center for Strategic and International Studies, Washington, DC, 3 June 2010, www.csis.org/event/cybersecurity-discussion-general-keith-b-alexander-director-national-security-agency.

116. Aliya Silverstein, 'US and Russia Among 22 Nations Supporting International Cyber Resolution', *NextGov*, 5 July 2011, http://www.nextgov.com/nextgov/ng_20110705_7349.php.

117 Howard Schmidt, 'US and Russia: Expanding the "Reset" to Cyberspace', *The White House Blog*, 12 July 2011, http://www.whitehouse.gov/blog/2011/07/12/us-and-russia-expanding-reset-cyberspace.

118. John Arquilla and David Ronfeldt, 'The Advent of Netwar: Analytic Background', *Studies in Conflict & Terrorism*, Vol.22, No.3 (July 1999), p.202; Kathryn Sikkink, 'Human Rights, Principled Issue-Networks, and Sovereignty in Latin America', *International Organization*, Vol.47, No.3 (Summer 1993), pp.411-41.

119. Nir Kshetri, 'Pattern of Global Cyber War and Crime', *Journal of International Management*, Vol.11, No.4 (December 2005), p.548.

120. Rosanna E. Guadagno, Robert B. Cialdini, and Gadi Evron, 'Storming the Servers: A Social Psychological Analysis of the First Internet War', *Cyberpsychology, Behavior, and Social Networking*, Vol.13, No.4 (August 2010), pp.447-53.

constraints on human behavior' within online communities, rather than imposed from without.[121] The roles of non-governmental organisations in effecting normative change at the transnational level should also not be underestimated.[122] Even in the field of security, Mueller notes that most of the routine cybersecurity work of 'identifying, preventing and responding' to threats to cyberspace systems 'seems to be done by a transnational network that relies on cooperative frameworks and norms that were developed independently of states'.[123]

As the CSIS 2008 report correctly noted, the US is 'not indispensable, a hegemon, or unchallenged, and the evolution of cyberspace clearly reflects this'.[124] There are many different actors who have access to cyberspace and are capable of using it to their own strategic ends, and whom as individuals and communities are subject to differing normative constraints and opportunities. States attempting to develop global normative frameworks for cyberspace may find their efforts have limited effect on cyberspace non-state communities. Cyber deterrence, even if it can be made to work between states, in conjunction with other tools of state power, is a far more problematic proposition at the sub-state level, precisely because, in contrast to traditional military domains, the tools and 'weapons' of cyber conflict are readily available to non-state actors who operate under different normative regimes. In the US context, for example, Duncan Hollis notes that 'non-attribution' — one of the characteristics of cyberspace making cyber deterrence difficult — 'is a value to be celebrated' and is deeply entrenched in US culture, on- and offline.[125] Attempts to alter this by government fiat are likely to meet substantial domestic resistance, not to mention external accusations of hypocrisy given the tenets of the stated US commitment to 'internet freedom'. Calls by US national security actors to 're-engineer', redesign, or even replace the Internet to facilitate personal identification of users and their activities are deeply problematic in this context.[126] Nevertheless, as 'norms' are one of the regulative 'laws' of cyberspace, alongside code, the market, and physical 'architecture', states will continue to explore ways in which to influence this aspect of cyberspace.[127]

---

121. April Mara Major, 'Norm Origin and Development in Cyberspace: Models of *Cybernorm* Evolution', *Washington University Law Quarterly*, Vol.78, No.1 (Spring 2000), pp.59-111.

122. Richard Price, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines', *International Organization*, Vol.52, No.3 (Summer 1998), pp.613-44.

123. Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010), p.164.

124. *Securing Cyberspace for the 44th Presidency*, p.18.

125. Duncan B. Hollis, 'An e-SOS for Cyberspace', *Harvard International Law Journal*, Vol.52, No.2 (Summer 2011), p.28.

126 For example, McConnell, 'To Win the Cyber-War'; Aliya Sternstein, 'Former CIA Director: Build a New Internet to Improve Cybersecurity', *National Journal*, 7 July 2011, http://www.nationaljournal.com/nationalsecurity/former-cia-director-build-a-new-internet-to-improve-cybersecurity-20110707.

127. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Conclusions

It is too early to tell quite how norms will emerge in this developing field, although we have tried to delineate the broad outlines of strategy, political discourse, and policy proposals. As such, we cannot tell what the consequences of these developments will be, although further moves will be made towards bi- and multilateral technical and information-sharing agreements and frameworks, even whilst the utility of these actions will continue to be hotly debated. It is likely that the ability to broker global agreements or treaty mechanisms will be hampered as much by cultural differences between, for example, the US and Russia, as it will by the tactical and operational difficulties in achieving technical security regimes satisfactory to all parties. The central unstated purpose of these activities is to normalise the exercise of state power in cyberspace. In this respect, all state parties agree; the differences emerge in how this is pursued.

Even as states attempt to regulate the use of cyberspace for, *inter alia*, military first strikes, they will retain significant military and intelligence cyber capabilities to be exercised below the level of an as-yet unascertained cyber conflict threshold. The latter may require legal definition at the global level, or it may yet fall to unilateral declarations of tolerance, or displays of force posture or operational capacity, most likely in conjunction with strategic allies. It may be that the norm that emerges from this situation is not of non-use but of 'acceptable' use, which serves to demonstrate where the 'red lines' of cyber operations are. It is unlikely, therefore, that a 'cyber taboo' analogous to nuclear and chemical weapons taboos will be constructed.[128] In the absence of any firm notion of what, for example, a 'cyberwar' might actually look like, there may be little immediate societal pressure to avoid one, and plenty of latitude afforded states to develop capabilities that might conceivably be used in one, if such a thing even exists.[129] Nevertheless, as Nina Tannenwald argues with respect to the nuclear taboo, a norm of non-use may stand a greater chance of being adopted by alliances of democracies than by authoritarian states.[130] However, given the possible US-Israeli involvement in the Stuxnet sabotage of Iranian nuclear technology, we must wonder if we are already past this point.[131] The lure of a voluntary framework banning the offensive use of cyberspace may prove irresistible to many 'like-minded nations', even if its actual applicability is strictly limited. Importantly, an international normative regime not backed with coordinated and credible force will serve no deterrent function against exactly those 'rogue' and non-state actors most likely to conduct

128. Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945* (Cambridge: Cambridge University Press, 2007); Richard M. Price, *The Chemical Weapons Taboo* (Ithaca, NY: Cornell University Press, 1997)

129 See, Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* (forthcoming, 2011).

130. Tannenwald, *The Nuclear Taboo*, pp.153-4.

131 Rid, 'Cyber War'.

disruptive cyber operations.

Yet the question remains: how effective is a norms-based approach to cyber deterrence likely to be? How can we tell what aspects of a deterrence strategy are working, or which aren't? In truth, it is much too early to know. Even if it were possible to get all parties to comply with a set of norms hammered out through diplomacy and other forms of negotiation, what guarantees are there that these would be adhered to? Again, there are no such guarantees. It may be that states can be persuaded to comply with international normative frameworks through a mix of inducement, coercion and moral pressure. So too might industry and civil society be persuaded to do their part through a gradual process of cultural learning, and all parties work together to achieve the 'global culture of cybersecurity' currently aspired to. Even were these norms to operate strongly and bind together these actors such that norms of non-use or acceptable use became institutionalised, they are never likely to persuade all who might have the capabilities to prosecute actions in cyberspace that constitute strategic threats. For this reason alone, states and their militaries and security services will, even whilst pursuing denial strategies and improving defensive cybersecurity, be loath to abandon the search for effective punitive measures through which deterrence might be achieved. In turn, the norm of retaliatory punishment may prove to be a powerful deterrent in itself.

In this article, I have argued that the pursuit of cyber deterrence is characterised by two principal activities. The first is the continued attempt to find forms of deterrence in cyberspace that actually deliver deterrent effects in an environment unsuited to traditional models of deterrence. This is principally a technical and military debate that has yet to translate into strategy or doctrine due to the acknowledged defects in available models, although deterrence by denial is an assumed and important practice. The second is a normative turn in nascent cyber strategy that focuses on the non-military aspects of national power as means to effect behavioural change in global cyberspace that may produce deterrent effects. It may be the case that the latter is partly a response to the inability to deliver cyber deterrence by military power alone. The nature of these regulative norms is disputed in the international policy arena, a situation reflecting domestic political considerations and the unique cultural aspects of the states in question.

The study of cyber deterrence and cyberspace norms is hampered by its relative novelty and more work is required to tease out the processes of cyber deterrence strategy development and normative change, particularly as national strategies and global policy frameworks emerge. Even whilst the instruments of 'soft' cyber power are being developed, there is a substantial build-up of military cyber capabilities across the globe, which perhaps indicates that states see little real utility in global cyberspace agreements to deter or prevent cyber conflict, or are attempting to develop punitive capabilities through demonstration of massive offensive capabilities and force structures and posture. The promotion of global cyberspace

norms in order to deter adversarial cyber actions is perhaps, therefore, as much about being seen to 'do the right thing' as it is to actually do it.