Public–private partnerships in national cyber-security strategies

MADELINE CARR

Cyber security is emerging as one of the most challenging aspects of the information age for policy-makers and scholars of International Relations (IR). It has implications for national security, the economy, human rights, civil liberties and international legal frameworks. Although politicians have been aware of the threats of cyber insecurity since the early years of internet technology,[1] anxiety about the difficulties in resolving or addressing them has increased rather than abated.[2] In response, governments have begun to develop national cyber-security strategies to outline the ways in which they intend to address cyber insecurity. In many states where critical infrastructural systems in areas such as utilities, finance and transport have been privatized, these policy documents are heavily reliant upon what is referred to as the 'public–private partnership' as a key mechanism through which to mitigate the threat. In the United States and United Kingdom, the public–private partnership has repeatedly been referred to as the 'cornerstone' or 'hub' of cyber-security strategy.[3]

While public–private partnerships have often been developed as an appropriate means to address both non-traditional and traditional security threats,[4] in the context of national cyber security this arrangement is uniquely problematic. There has been a persistent ambiguity with regard to the parameters for such a partnership. The reluctance of politicians to claim authority for the state to introduce tougher cyber-security measures by law, coupled with the private sector's aversion to accepting responsibility or liability for national security, leaves the 'partnership' without clear lines of responsibility or accountability. Questions are now being raised (by, among others, President Obama) about the efficacy of a market-driven approach to cyber security, though in liberal democratic states at

[1] William J. Clinton, *A National Security Strategy for a new century* (Washington DC: The White House, Oct. 1998), p. 17.

[2] Barack Obama, 'Remarks by the President on securing our nation's cyber infrastructure' (Washington DC: The White House, 29 May 2009).

[3] William J. Clinton, *National Plan for Information Systems Protection Version 1.0: an invitation to a dialogue* (Washington DC: The White House, 2000); George W. Bush, *The National Strategy to Secure Cyberspace* (Washington DC: The White House, 2003); Francis Maude, *The UK Cyber Security Strategy: protecting and promoting the UK in a digital world* (London: Cabinet Office, 2011).

[4] Max G. Manwaring, 'The new global security landscape: the road ahead', *Low Intensity Conflict and Law Enforcement* 11: 2–3, Winter 2002, pp. 190–209; Barack Obama, *US National Security Strategy* (Washington DC: The White House, 2012).

International Affairs **92**: 1 (2016) 43–62

least, any alternative has yet to emerge.[5] Crucially for IR scholars, questions arise here about the extent to which the state can be seen to be abdicating not just authority but *responsibility* for national security. As Dunn Cavelty and Suter point out in their article on this topic, 'generating security for citizens is a core task of the state; therefore it is an extremely delicate matter for the government to pass on its responsibility in this area to the private sector'.[6] Essentially, this raises questions about how well the state is equipped to provide national security in this context and about how existing policies and practices of national security are being challenged by this new threat conception.

This article develops a comprehensive understanding of how policy-makers and the private sector are conceptualizing their respective roles in national cyber security, where there may be disparity in these conceptions and what implications this may have for national and international cyber security. To this end, it begins with some necessary background to the establishment of the public–private partnership in national cyber-security strategies. It then analyses the conceptions of security that are evident in these policy documents. Unpacking the assumptions about security that drive these policies is essential to developing an understanding of the goals, objectives and embedded interests that shape the partnership. The article then moves on to analyse the public–private partnership from the perspectives of both partners. It finds that there is a fundamental disjuncture between the expectations of the two 'partners' in terms of roles, responsibility and authority. Disjuncture in such relationships is certainly not unique to this context, but the particular significance here arises from the fact that what is at stake is not (for example) a civil engineering project but a *national security concern*. The conclusion is not that no kind of public–private partnership can be central to national security in the US and UK, but rather that the partnership referred to in the policy documents is deeply flawed and that, unless the problems identified here are acknowledged and addressed, it is unlikely that this arrangement will prove a durable or effective means of promoting national cyber security.

Methodology

Many states have recently produced national cyber-security strategies that place an emphasis on some kind of public–private partnership. Those examined in the course of the research underlying this article include Austria, Australia, Canada, the Czech Republic, Estonia, Finland, France, Hungary, India, Japan, Lithuania, the Netherlands, New Zealand, the Slovak Republic, South Africa, the United Kingdom and the United States. The analysis in the article itself focuses exclusively on the UK and the US. The US is an essential case because it is here that cyber-security strategies based on the public–private partnership were developed

[5] Obama, 'Remarks by the President on securing our nation's cyber infrastructure'.

[6] Myriam Dunn Cavelty and Manuel Suter, 'Public–private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection', *International Journal of Critical Infrastructure Protection* 2: 4, 2009, p. 181.

in 2000 under President Clinton. Over the ensuing 15 years, the public–private partnership has been described by successive US presidents as the 'cornerstone' of national cyber security, though none has yet explicitly defined the parameters, extent or nature of the relationship between the parties. The UK, for its part, provides a correlate case-study. Cyber-security policy in the UK has been modelled on and influenced by US policy though it is, of course, distinct. The purpose of looking closely at two states with similar approaches, similar security cultures and close ties between their intelligence communities, commercial sectors and defence relations is to look for subtle differences. An examination of two more radically different states, such as the United States and China, would be expected to show significant differences; but in such a comparison there are so many factors that could play a part that a close analysis could be difficult to pursue in a focused way. It is anticipated that this research may provide a foundation for further work in this area (a point to which I return below).

It should be noted also that the public–private partnership in national cyber security is multifaceted. Governments have diverse relations with internet service providers (ISPs), multinational information corporations (Google, Facebook, etc.), private cyber-security firms, promoters of human and civil rights, law enforcement agencies and civil society. However, both within the relevant policy documents and within the cyber-security discourse generally, the public–private partnership is often referred to as a single entity, ignoring this complexity. Unpacking the term is therefore one of the contributions this article seeks to make. In the course of doing so, it becomes clear that despite this complexity and diversity, the core focus in the strategies (and consequently in this article) is on the relationship between the government and the owners/operators of critical infrastructure—the rationale being that, while the many other aspects of cyber security are regarded as linked to the national *interest*, critical infrastructure protection is unequivocally and intrinsically linked to national *security*.

A number of informal interviews were conducted for this research over an 18-month period. Representatives from the British and American public sector entities responsible for national cyber security were asked to comment on how effective they felt the public–private partnership was in terms of critical infrastructure protection, what problems they had observed with it and how they thought it might be improved. Interviews were also conducted with representatives of the private sector in the UK and US, with a particular concentration on two specific sectors: those working for critical infrastructure owners and operators, and those working for private cyber-security firms. Relationships between the public and private sectors in this area are sensitive, particularly from the private-sector perspective. Although the comments made by private-sector participants were often mutually corroborated, being made in several interviews (as well as in those with representatives of the public sector), private-sector participants were reluctant to be identified and the interviews have therefore been anonymized. Consequently, they serve here to enhance the research findings rather than to drive them in a more substantive way.

The reluctance of key actors to speak openly about the problems with this particular public–private partnership is one of the constraints on researching these issues. A second constraint is that it is difficult to look in the same detail at states that are less open about their policies and practices—as is, of course, often the case with defence or intelligence research. In order to develop our understanding of the implications for International Relations of the public–private partnership in cyber security, it would be illuminating to extend this research project to look at a very different case-study. China is a major power in global cyber security, and differs markedly from the US and UK in both the relationship between its public and private sectors and its ownership of critical infrastructure. Having looked closely at these two similar states to discern the distinctive nuances in their respective approaches, it would be useful to conduct the same study in China in order to extend the analysis of potential implications for global security in the twenty-first century.

Background to the public–private partnership in national cyber-security strategy

Dunn Cavelty and Brunner have observed that one of the dominant arguments in the literature on the implications of the information age for international politics is that 'technological development enhances two trends that diminish the importance of the state, both of which have implications for security: increasing internationalisation and increasing privatisation'.[7] These two trends unite in the approach of the US and UK to national cyber security, and become manifest in the form of the public–private partnership. Understanding the history and background to this approach is important in providing context for the tensions now evident in this partnership, because these tensions embody a whole set of beliefs about the respective roles of the state and of the private sector, and about the interrelationship between economic promotion and national security.

An important catalyst for this trajectory can be traced back to the end of the Cold War, which 'decreased the demand for defense research and made national security a less compelling reason to support [technology research and development]'.[8] President Clinton's foreign policy and economic policy were to form a close and symbiotic (although not always comfortable) relationship as his ideas about democratic enlargement through trade, the promotion of human rights, and globalizing and liberating markets combined to form a kind of ideological/economic grand strategy.[9] Clinton was in favour of spending the 'peace dividend',

[7] Myriam Dunn Cavelty and Elgin M. Brunner, 'Introduction: information, power, and security—an outline of debates and implications', in Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel, eds, *Power and security in the information age: investigating the role of the state in cyberspace* (Aldershot: Ashgate, 2007), pp. 8–9.

[8] Joseph E. Stiglitz and Scott J. Wallsten, 'Public–private technology partnerships: promises and pitfalls', *American Behavioral Scientist* 43: 35, Sept. 1999, p. 57.

[9] In September 1993, President Clinton gave a speech to the UN General Assembly outlining this strategic framework, which was reiterated in several subsequent speeches by senior officials including the Secretary of State and the National Security Advisor: William J. Clinton, 'Remarks to the 48th Session of the United

International Affairs 92: 1, 2016

and by 1992 he was explicit about how it should be applied: 'Every dollar we take out of military R&D [research and development] in the post-Cold War era should go to R&D for commercial technologies, until civilian R&D can match and eventually surpass our Cold War military R&D commitment.'[10] Stiglitz and Wallsten write that these conditions 'led to a new push for public–private partnerships intended to support commercial [technology research and development]'.[11] Much of the groundwork for these partnerships was laid in the 1980s, but the Clinton administration made them 'the centrepiece of its technology program'.[12]

It was in this climate that the Clinton–Gore administration invested so heavily in internet technology. Though they were clear from the beginning about their intention that the private sector should play a primary role, they also acknowledged the value of government input. The new administration believed that 'only the private sector has the skills and abilities to manage the complex process of developing new technologies and bringing them to market, while … [the] government plays a vital role in enabling the private sector's efforts'.[13] By the mid-1980s, the internet infrastructure was fiscally supported and administered by the federal government through the National Science Foundation (NSF), though this was regarded by the government as an interim measure on the way to full private ownership and management.[14] The National High-Performance Computing Act of 1990 specified that the NSF was to support the establishment of a high-speed national network 'in a manner which fosters and maintains competition and private sector investment in high speed data networking',[15] and that the involvement of the NSF 'be phased out when commercial networks can meet the networking needs of American researchers'.[16]

A number of policy initiatives focused on stimulating private-sector investment as well as the development of network management capability. One of these initiatives was the enforcement of the 'Acceptable Use Policy' (AUP) drawn up by the NSF. This policy dictated that network traffic should be restricted to 'open research and education', specifically prohibiting commercial activity until such time as the infrastructure was privatized.[17] Through this 'carrot and stick' policy

Nations General Assembly', New York, 27 Sept. 1993; Anthony Lake, 'From containment to enlargement', speech to the Johns Hopkins University School of Advanced International Studies, Washington DC, 21 Sept. 1993; Warren Christopher, 'Building peace in the Middle East', speech at Columbia University, 20 Sept. 1993.

[10] William J. Clinton, remarks at Wharton School of Business, University of Pennsylvania, Philadelphia, 16 April 1992, http://www.ibiblio.org/nii/econ-posit.html, accessed 4 Nov. 2015.

[11] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 57.

[12] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 57.

[13] *Technology in the National Interest* (Washington DC: NSTC Committee on Civilian Industrial Technology, 1996), p. 42, cited in Stiglitz and Wallsten, 'Public–private technology partnerships', p. 63.

[14] For an account of how the funding was organized in 1990, see Brian Kahin, 'RFC1192—commercialization of the internet, summary report', issued as a 'request for comments' by the Network Working Group, Harvard University, Nov. 1990, http://www.faqs.org/rfcs/rfc1192.html, accessed 4 Nov. 2015.

[15] S.1067, National High-Performance Computing Act of 1990, 101st Congress, 2nd Session, as marked up 3 April 1990. The Federal Research Internet Coordinating Committee, established to coordinate networking research activities, issued a report in 1989 stating that the network would 'be implemented and operated so that [it] can become commercialized': Federal Research Internet Coordinating Committee, *Program plan for the National Research and Education Network* (Washington DC, 23 May 1989), pp. 4–5.

[16] S.2918, National High-Performance Computing Act of 1988, 100th Congress, 2nd Session, 19 Oct. 1988.

[17] For background on this, see the NSF website, 'The internet: changing the way we communicate', http://www.nsf.gov/about/history/nsf0050/internet/internet.htm, accessed 4 Nov. 2015.

approach, the government sought to stimulate necessary private-sector investment—and indeed, this policy did have the intended effect.[18]

The public–private partnership is not, of course, unique to cyber security. It has been employed widely by states including the US and UK as a mechanism to deal with a range of other issues, including security-related ones. The practice intensified from the 1990s, when the privatization of critical infrastructure was regarded as economically beneficial to the state, freeing up capital and drawing more heavily on the efficiencies and business practices of the private sector. In the wake of this shift, an extensive body of literature developed that examines the public–private partnership in all kinds of contexts. It deals with the background of these partnerships,[19] the range of different approaches,[20] how to measure success and failure,[21] and how responsibility and authority are delegated.[22] There has also been some examination of the public–private partnership in cyber security, most notably by Dunn Cavelty and Suter, but this focuses on ways to improve it rather than critically analysing its political implications.[23] Combined, this literature provides a solid foundation for the present research project, proving particularly useful in highlighting the ways in which this partnership is distinct but also in outlining common assumptions and expectations that run through public–private partnerships more generally.

In addition to the political history outlined above, it should be noted that for many public policy scholars, the history of public–private partnerships is in large part one of discourse. Although they are often portrayed as a 'new' management approach designed to blend the best of both sectors, examples of public–private partnerships have been traced back to biblical times.[24] Without going back quite so far, Wettenhall uses the example of Drake's fleet which defeated the Spanish Armada in the sixteenth century, highlighting the fact that most of the ships were privately owned and operated though they were serving under contract to the

[18] See NSF website, http://www.nsf.gov/od/lpa/nsf50/nsfoutreach/htm/n50_z2/pages_z3/28_pg.htm; also Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, 'A brief history of the internet, part 1', *On the Internet* (The Internet Society), May–June 1997, http://www.isoc.org/oti/articles/0597/leiner.html (both accessed 4 Nov. 2015).

[19] Stephen H. Linder, 'Coming to terms with the public–private partnership: a grammar of multiple meanings', *American Behavioral Scientist* 43: 1, Sept. 1999, pp. 35–51; Roger Wettenhall, 'The rhetoric and reality of public–private partnerships', *Public Organization Review: A Global Journal* 3: 1, 2003, pp. 77–107.

[20] Stiglitz and Wallsten, 'Public–private technology partnerships', pp. 52–73; James A. Dunn, 'Transportation: policy-level partnerships and project-based partnerships', *American Behavioural Scientist* 43: 1, Sept. 1999, pp. 92–106; Philip E. Auerswald, Lewis M. Branscomb, Todd M. LaPorte and Erwann O. Michel-Kerjan, *Seeds of disaster, roots of response: how private action can reduce public vulnerability* (Cambridge: Cambridge University Press, 2007).

[21] Graeme A. Hodge and Carsten Greve, 'Public–private partnerships: an international performance review', *Public Administration Review* 67: 3, May–June 2007, pp. 545–58; Michael J. Garvin and Doran Bosso, 'Assessing the effectiveness of infrastructure public–private partnership programs and projects', *Public Works Management and Policy* 13: 2, Oct. 2008, pp. 162–78.

[22] Nutavoot Pongsiri, 'Regulation and public–private partnerships', *International Journal of Public Sector Management* 15: 6, 2002, pp. 487–95; Marco Schaferhoff, Sabine Campe and Christopher Kaan, 'Transnational public–private partnerships in International Relations: making sense of concepts, research frameworks, and results', *International Studies Review* 11: 3, Sept. 2009, pp. 451–74.

[23] Dunn Cavelty and Suter, 'Public–private partnerships are no silver bullet'.

[24] Wettenhall, 'The rhetoric and reality of public–private partnerships'.

Admiralty, to demonstrate that the practice of governments cooperating with private actors has a long historical pedigree.[25] What appears to be 'new' is the discourse around it, which Reijniers argues has reflected trends in management reform from the early 1990s that saw a turn away from 'leadership and behavioural principles and toward more structural emphases on flexibility and innovation—reinforcing partnership ideals'.[26] Linder sees the growing discourse on partnerships as a retreat from the 'hard-line advocacy of privatization' of the Reagan and Thatcher years.[27] From this perspective, he argues, they are accommodationist; 'they hold back the spectre of wholesale divestiture and, in exchange, promise lucrative collaboration with the state'.[28] Wettenhall also points out that the term has a positive relationship with the discourse on 'third way' economics and is associated with expectations of 'mutual obligation and trust'.[29]

All of this suggests a discursive and practical breaking down of boundaries or borders at a domestic level which, of course, is very much in keeping with the broader discourse around the internet. The observation by Hess and Adams that public–private partnerships emerge from 'loss of faith in both state and market' can go some way to explaining this discursive and policy shift.[30] Despite the fact that internet technology was heavily supported and promoted by the US government (and indeed, the private sector had to be pressured to some extent to take it over), there quickly developed a kind of expectation that governments had only a limited role to play in further development of the technology. However, Wettenhall argues that there is a persistent lack of precision in how the term 'partnership' is employed, and 'belief that what it refers to is "a good" thing seems much more a matter of faith than of science'.[31]

What is meant by 'cyber security'?

> Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyber space.[32]

'Cyber security' is almost as broad and indistinct a term as 'security' itself; and there are a number of reasons for this. First, the implications of internet technology are highly diverse because they penetrate many critical systems and practices on multiple levels. Cyber security is used to refer to the integrity of our personal privacy online, to the security of our critical infrastructure, to electronic

[25] Wettenhall, 'The rhetoric and reality of public–private partnerships', p. 92.
[26] J. J. A. M. Reijniers, 'Organization of public–private partnership projects', *International Journal of Project Management* 12: 3, 1994, pp. 137–42, cited in Linder, 'Coming to terms with the public–private partnership', p. 39.
[27] Linder, 'Coming to terms with the public–private partnership', p. 41.
[28] Linder, 'Coming to terms with the public–private partnership', p. 41.
[29] Wettenhall, 'The rhetoric and reality of public–private partnerships', p. 78.
[30] Michael Hess and David Adams, 'Community in public policy: fad or foundation?', *Australian Journal of Public Administration* 60: 2, 2001, p. 13.
[31] Wettenhall, 'The rhetoric and reality of public–private partnerships', p. 80.
[32] *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space* (London: Cabinet Office, June 2009), p. 5.

commerce, to military threats and to the protection of intellectual property. These areas range extremely widely, and are united only by the technology with which they engage. This of course, is also a problem with 'security' that has been recognized by scholars in IR for many years.[33] In order to arrive at some clarity about what cyber security means in the context of national cyber-security strategies, it is useful to turn to the three fundamental questions that guide those working in many areas of security studies: for whom? from what? and by what means? When these national cyber-security strategy documents refer to 'cyber security', whose security are they referring to? Exactly what threats are they responding to? And by what means do the strategies propose to mediate those threats?

Cyber security for whom?

The referent object in these strategy documents is typically 'the state', which in turn is conceived of as comprising three main component parts: individuals, businesses and the internet itself. The way in which the individual (or citizen) is treated in these national cyber-security strategies is quite enlightening and demonstrates the value of asking these three foundational questions. The interests of the individual are generally conflated with those of the state—a common approach to security in international relations that is being challenged now by concepts of 'human security'—according to which what is 'best' for the state is, by definition, best for individual citizens. The state exists to pursue security and, by doing so, ensures that it can provide for and protect individuals. There are some references in the strategy documents that acknowledge that state security interests do not always align with individual security interests. These take the form of normative statements or principles about simultaneously pursuing greater cyber security and also upholding values of privacy and civil liberties (a tension that has been of particular pertinence since the Edward Snowden case of 2013). The 2003 US National Strategy to Secure Cyberspace states that cyber security and personal privacy need not be opposing goals and that the federal government should 'lead by example in implementing strong privacy policies and practices'.[34] The 2009 UK strategy is somewhat more forthright about the intention to exploit opportunities for data gathering[35] in balance with civil liberties and privacy, upon which 'our freedoms depend … and which form the basis of our society'.[36] The individual's cyber security, then, is important at a profound societal level—but may have to be subsumed into broader collective state concerns.

The importance of the internet to national economies makes the business sector a key focus in these strategies. In any analysis of how politicians regard cyber security as a problem for US power, economic factors feature significantly.[37]

[33] Peter Burgess, ed., *The Routledge handbook of new security studies* (London and New York: Routledge, 2010).
[34] Bush, *National Strategy to Secure Cyberspace*, pp. 14–15.
[35] *Cyber Security Strategy of the United Kingdom*, pp. 4, 15.
[36] *Cyber Security Strategy of the United Kingdom*, p. 10.
[37] Senator Daniel Akaka referred to the internet as the 'backbone of the US economy' in a statement at 'Securing cyberspace: efforts to protect national information infrastructures continue to face challenges', hearing before the Committee on Homeland Security and Governmental Affairs, and the Subcommittee on Federal Finan-

International Affairs 92: 1, 2016

Indeed, in a 2009 speech entitled 'Securing our nation's cyber infrastructure', President Obama stated definitively that 'America's economic prosperity in the 21st century will depend on cybersecurity'.[38] In the 'landscape review' of the UK cyber-security strategy, Amyas Morse makes the point that if the internet were a national economy, it would be the fifth largest in the world.[39] In addition, he writes, the UK has one of the world's largest online economies, with 8 per cent of GDP generated online—a higher proportion than for any other G20 country.[40] To this end, the UK national Cyber Security Strategy specifically addresses the financial cost to businesses of security breaches.[41] Intellectual property is also a key concern for the business sector; the US Cyberspace Policy Review quotes a 2008 estimate that set the value of losses due to data theft as high as $1 trillion.[42]

Protecting the state also means ensuring the integrity and smooth functioning of the internet itself because so many other systems rely upon it. The Obama administration's first National Security Strategy in 2010 elevated the internet to the position of 'strategic national asset' and declared that protecting it was now a 'national security priority'.[43] The UK Cyber Security Strategy states that it is the 'effective functioning of cyber space' that is of vital importance.[44] This introduces some conflation of ideas about cyber security, because in addition to being an object to be protected, the internet is also, of course, the source of threats (from what?) and the mechanism through which those threats can be addressed (by what means?). However, it is clear in these strategies that the network itself is a primary referent object for conceptions of security. It is the security of the *technology* itself, as well as the security of those who use the technology, that concerns the US and UK governments here; and the two forms of security are linked. 'Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space.'[45] The technology becomes an artefact to be protected, an asset essential to broader state security.

There exists, then, a level of conceptual confusion within this question. Who is to be protected in these cyber-security strategies? Is it individuals—and, if so, what happens when the state itself is perceived as the threat to security, as it was for some in the context of the Prism/Tempora programme?[46] If businesses are to

cial Management, Government Information, and International Security, US Senate, 19 July 2005, p. 5. In a similar context, Representative Tom Davis called the internet the 'central backbone of our global economy' in his statement at 'Computer security: cyber attacks: war without borders', hearing before the Committee on Government Reform, US House of Representatives, 26 July 2000, p. 6.

[38] Obama, 'Remarks by the President on securing our nation's cyber infrastructure'.

[39] David Dean, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda and Paul Zwillenberg, *The Internet economy in the G-20: the $4.2 trillion growth opportunity* (Boston Consulting Group, March 2012), available online at http://www.bcg.com/documents/file100409.pdf , cited in Amyas Morse, *The UK Cyber Security Strategy: landscape review* (London: House of Commons, 11 Feb. 2013), p. 5.

[40] Morse, *The UK Cyber Security Strategy*, p. 5.

[41] *Cyber Security Strategy of the United Kingdom*, p. 12.

[42] Melissa Hathaway, *Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure* (Washington DC: The White House, May 2009), p. 2.

[43] Barack Obama, *United States National Security Strategy* (Washington DC: The White House, 2010), p. 27.

[44] *Cyber Security Strategy of the United Kingdom*, p. 3.

[45] *Cyber Security Strategy of the United Kingdom*, p. 3.

[46] The Prism programme refers to the US National Security Agency's practice of collecting personal data through a range of online services like social media and search engines. It was revealed by NSA contractor

be protected, we might expect a greater contribution from that sector to finance national cyber security. Or is national cyber security to be regarded as a business subsidy? And finally, if the protection of the network is also the object of the strategies, it becomes clear that conflicts and tensions between these goals are likely to become manifest in any arrangements to achieve them.

Cyber security from what?

National cyber-security strategies tend to explicitly identify the *actors* from whom threats are expected to emerge: criminals, terrorists and hostile states.[47] This triumvirate of malicious actors is conceived as existing in a framework of offline aggression and belligerence where it is possible to identify a perpetrator and, therefore, their motivation. Online, where it can be possible to conceal the origin of attacks, these distinctions have less meaning; but they are so firmly entrenched in our political and legal systems that it has proved difficult to conceptualize threats in cyberspace beyond these terms.

Beyond articulating some conception of the actors that pose a threat in cyberspace, there are two main areas of concern that dominate the US and UK national cyber-security strategies. One is the economy, which was briefly dealt with in the previous section. The second is critical infrastructure protection; and this is also the primary focus of the public–private partnership. Critical infrastructure is defined in the US as 'systems and assets, whether physical or virtual, so vital to the nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters'.[48] The protection of critical infrastructure has been linked to cyber security for the past 25 years, during which many advanced industrialized states have privatized critical infrastructure systems such as water and sewerage, electricity, finance, communications and transport.[49] By the time the new millennium arrived, some 85 per cent of US critical infrastructure was in private hands.[50] With privatization came an increased discretion on the part of those managing the infrastructure in the choice of systems and technology to control these utilities and industries, and many of them moved from proprietary

Edward Snowden in June 2013. He also revealed details about the UK Government Communications Headquarters (GCHQ) Tempora program which gathered data through intercepts placed on fibre-optic cables: Luke Harding, *The Snowden files: the inside story of the world's most wanted man* (London: Guardian Faber, 2014).

[47] *Cyber Security Strategy of the United Kingdom*, pp. 12–14; Hathaway, *Cyberspace policy review*, p. 1.

[48] Gregory C. Wilshusen, 'Cyber security: continued attention needed to protect our nation's critical infrastructure and federal information systems', testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives (Washington DC: US Government Accountability Office, 16 March 2011), p. 2. A similar definition is used in the UK: 'Those infrastructure assets ... that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life'. See Centre for the Protection of National Infrastructure, 'About CPNI: the national infrastructure', http://www.cpni.gov.uk/about/cni/, accessed 4 Nov. 2015.

[49] Information Sharing Environment, 'ISE's participation in the Open Government initiative', http://www.ise.gov/open, accessed 4 Nov. 2015.

[50] 'Agency response to cyberspace policy review', presented to the Committee on Science and Technology, Subcommittee on Technology and Innovation and Subcommittee on Research and Science Education, US House of Representatives, 16 June 2009, p. 3.

systems to more generic computer programs known as 'supervisory control and data acquisition systems' (SCADA systems). While SCADA systems boosted the productivity and efficiency of many industries and services by allowing critical infrastructure to be controlled centrally and remotely, the combination of private ownership and the vulnerabilities of SCADA systems led to a range of cyber-security concerns around critical infrastructure protection when these systems began to be connected to the internet.

An attack on critical infrastructure remains one of the dominant themes of debates about cyber insecurity in the US. In a congressional hearing on SCADA vulnerabilities, Representative Bill Pascrell stated: 'We *know* that vulnerabilities within these systems are abundant, and we *know* that the threat of a terrorist attack against these systems is real.'[51] Over the course of the past decade, this type of attack has emerged not only as a terrorist threat but also in the context of state-to-state conflict, as was demonstrated in Estonia in 2007 and Georgia in 2008 and, of course, in the Stuxnet episode of 2010. Critical infrastructure is typically discussed in terms of 'sectors', and these come under the purview of government agencies or departments.[52] For the most part, the trend has been towards industry self-regulation, best practices and some coordination in terms of information-sharing with the government. This is central to the public–private partnership, which is in large part 'the means'.

Cyber security by what means?

It is not necessary in this article to describe in detail every policy proposal and recommendation in the strategy documents. What is of interest to the core research objectives here is that two dominant lines of practice emerge in response to the question: 'By what means?' First, as discussed briefly above, there is a persistent emphasis on remaining anchored in core values and norms that are believed to underpin the national identity and power more broadly—what Hans Morgenthau referred to as the 'national character'.[53] In the 2010 US National Security Strategy, President Obama argued that: 'Fidelity to our values is the reason why the United States of America grew from a small string of colonies under the writ of an empire

[51] Representative Bill Pascrell, prepared statement at 'SCADA systems and the terrorist threat: protecting the nation's critical control systems', joint hearing before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity with the Subcommittee on Emergency Preparedness, Science, and Technology of the Committee of Homeland Security on 18 Oct. 2005, p. 3.

[52] In the UK, there are nine national infrastructure sectors: energy, food, water, transport, communications, government, emergency services, health and finance. These are further refined into 'critical' national infrastructure, defined 'according to its value or "criticality" and the impact of its loss'. See the Centre for the Protection of National Infrastructure website, http://www.cpni.gov.uk/about/cni/. In the US, there are 16 critical infrastructure sectors, set out in Presidential Policy Directive 21 (PPD-21). They are: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors materials and waste, transportation systems, and water and wastewater systems. See Department of Homeland Security, http://www.dhs.gov/critical-infrastructure-sectors (both accessed 4 Nov. 2015).

[53] Hans Morgenthau, *Politics among nations: the struggle for power and peace*, 5th rev. edn (New York: Knopf, 1978), pp. 138–40.

to the strongest nation in the world.'[54] And in the UK: 'Our approach seeks to preserve and protect the rights to which we are accustomed (including privacy and civil liberties) because it is on these rights that our freedoms depend.'[55]

The second dominant line of practice articulated in these strategies that is of consequence for the public–private partnership is information sharing. Information sharing is fundamental to conceptions of this 'partnership' and needs to be discussed at length in that context. The expectations of both partners, the challenges each faces and the impediments to greater clarity about lines of responsibility and authority are key to understanding the role of the public–private partnership in these cyber-security strategies. The next part of this article provides some context for these arrangements and also some analysis of how this particular partnership can be understood within the broader literature on public–private partnerships.

Analysis of the public–private partnership in cyber security

There are several reasons why cyber security, particularly in the context of critical infrastructure protection, has been conceived of as some kind of collaborative project for the public and private sectors. The state is understood to be responsible for the provision of security, especially national security. Protecting critical infrastructure—those assets and systems necessary for the preservation of national security (broadly defined)—is perceived as an integral part of providing security to the state. The potential implications of a large-scale cyber attack on critical infrastructure are so extensive that it follows naturally that the government would recognize some authority and responsibility here. However, because most of the critical infrastructure in the US and UK is privately owned and operated, by definition there has to be some kind of relationship between the public and private sectors in terms of the provision of security in this context.

What is this public–private partnership?

Having established the background to public–private partnerships, in terms of both discourse and practice, it is necessary now to be clear about what exactly is meant by the term in this particular context. Perhaps not unexpectedly, there is a huge range of diverse arrangements that are referred to as public–private partnerships, from the joint provision of services with some government regulatory oversight (health sector), to closely contracted outsourcing of large infrastructure projects (building bridges, hosting the Olympic Games, etc.). Much of the literature on public–private partnerships revolves around identifying and classifying partnership arrangements. This identification and classification often takes place within a framework of authority and responsibility—key concepts for this study. In examining these relationships, Wettenhall identifies two broad categories: (a) horizontal, non-hierarchical arrangements characterized by consensual decision-

[54] Obama, *United States National Security Strategy*, 2010, p. 35.
[55] *Cyber Security Strategy of the United Kingdom*, p. 10.

making; and (b) hierarchically organized relationships with one party in a controlling role. The implication is, he argues, that true 'partnerships' are of type (a) and not type (b).[56]

This distinction has implications for the public–private partnership in cyber security. National cyber-security strategies avoid suggestions of hierarchy when they refer to the public–private partnership. The language is deliberately cooperative and implies a shared purpose and shared interests. The UK Cyber Security Strategy states that achieving the goal of a safe, secure internet will 'require everybody, the private sector, individuals and government to work together. Just as we all benefit from the use of cyberspace, so we all have a responsibility to help protect it.'[57] With specific reference to the role of the private sector, it states that there is an expectation that private-sector entities will 'work in partnerships with each other, Government and law enforcement agencies, sharing information and resources, to transform the response to a common challenge, and actively deter the threats we face in cyberspace'.[58] This non-hierarchical language belies the poor alignment of perceptions about the 'common challenge' and the 'threats we face in cyberspace'. It implies that the challenge and the threats are the same for the public and the private sector, when in fact they are not. The private sector regards cyber-security challenges as financial and reputational—not as a common public good, which is how governments regard national cyber security.

On a more granular level, Stephen Linder identifies six distinctive uses of the term 'public–private partnership' and links them to neo-liberal or neo-conservative ideological perspectives. In doing so, he draws out questions about their intended purpose and significance as well as 'what the relevant problems are to be solved and how best to solve them'.[59] Two of these 'types' can shed light on what is meant by the public–private partnership in cyber security: *partnership as management reform* and *partnership as power sharing*.

Linder argues that *partnership as management reform* refers to the expectation that government managers will learn 'by emulating their partners' and shift their focus from administrative processes to deal-making and attracting capital in a more entrepreneurial and flexible approach.[60] Significantly, this is regarded as one of the objectives of the partnership, because of the belief that the market is inherently superior and 'its competitive character stimulates innovation and creative problem solving'—a view embedded in neo-liberalism.[61]

Perhaps not surprisingly, although this is reflected in the strategies of both states, it is much more pronounced in the US documents. The Bush administration's National Strategy to Secure Cyberspace argued that in the US 'traditions of federalism and limited government require that organizations outside the federal government take the lead' in cyber security.[62] This interpretation of the

[56] Wettenhall, 'The rhetoric and reality of public–private partnerships', p. 90.
[57] *UK Cyber Security Strategy*, p. 22.
[58] *UK Cyber Security Strategy*, p. 23.
[59] Linder, 'Coming to terms with the public–private partnership', p. 42.
[60] Linder, 'Coming to terms with the public–private partnership', p. 43.
[61] Linder, 'Coming to terms with the public–private partnership', p. 43.
[62] Bush, *National Strategy to Secure Cyberspace*, p. xiii.

government's limited authority is combined here with an assumption of its limited capability. 'The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector.'[63] This assertion is based on the belief that 'in general, the private sector is best equipped and structured to respond to an evolving cyber threat',[64] and reflected in the statement by Attorney General Eric Holder that decision-makers in the US 'believe strongly that the private sector should take the lead in protecting private computer networks'.[65] In testimony before a hearing on internet security, the FBI's Michael Vatis argued that cyber security is 'clearly the role of the private sector. The Government has neither the responsibility nor the expertise to act as the private sector's system administration.'[66]

There is a rejection here of government liability for private networks that is framed in the belief that the government has neither the authority nor the capability to deal with cyber security. It is an approach in keeping with the *partnership as management reform* type identified by Linder—though the government rejects the objective of change inherent within that type. Rather, it promotes two 'truths' about the private sector. First, it must accept responsibility *and liability* for its own network security; and second, its superior capacity for flexibility and innovation means that it *is best placed* to take the lead on this particular security problem. The problem, of course, is that some of these networks—particularly with regard to critical infrastructure—are central to national security; and therein lies the problem from the perspective of the private sector.

The private sector develops a cyber-security strategy within a very different framework from the government's 'public good' conception. For the private operators of critical infrastructure, decisions are made within a business model that responds to profit margins and shareholder interests. This is largely incompatible with the promotion of a 'public good'. The private sector raises two main objections to the role that the government perceives for it in cyber-security strategies. First, it argues that the expense of ensuring cyber security to a *national* security level would be significant; second, it argues that the litigious nature of (especially American) society means that industry would be very resistant to accepting liability for the security of its products or systems.[67]

Stiglitz and Wallsten make some important observations about this dichotomized approach to public–private partnerships in the context of technology innovation. 'Theory predicts,' they argue, 'and many empirical studies confirm, that profit-maximizing firms invest less than the socially optimal level of

[63] Bush, *National Strategy to Secure Cyberspace*, p. 11.
[64] Bush, *National Strategy to Secure Cyberspace*, p. 11.
[65] Eric Holder Jr, Deputy Attorney General, US Department of Justice, prepared statement for 'Internet Security', hearing on 8 March 2000, p. 12.
[66] Michael A. Vatis, Deputy Assistant Director, Federal Bureau of Investigation, National Infrastructure Protection Programs, prepared statement for 'Internet security', hearing on 8 March 2000, p. 26.
[67] Alan Paller of the SANS Institute, testimony before 'SCADA systems and the terrorist threat', p. 62. See also Richard A. Clarke and Robert K. Knake, *Cyber war: the next threat to national security and what to do about it* (New York: Ecco, 2010).

[technology research and development].'[68] What is in society's best interest with regard to cyber security is not always in the best interests of the private sector. This is because, they argue, social benefits do not translate in terms of private profitability—no matter how desirable the outcome.[69]

Private-sector owners of critical infrastructure accept responsibility for securing their systems—to the point that it is profitable; that is, as far as the cost of dealing with an outage promises to cost more than preventing it. However, they tend to make a distinction between protecting against low-level threats such as 'background noise, individual hackers, and possibly hacktivists' and protecting against an attack on the state (national security).[70] In testimony at a US hearing on privately owned critical infrastructure cyber security, one witness explained that 'it is industry's contention that government should protect against the larger threats—organized crime, terrorists, and nation-state threats—either through law-enforcement or national defense'.[71] We saw this distinction play out in the 2014 attack on Sony Pictures, where the focus on the likely source shifted from an 'insider threat' attack (which the security community regarded as most likely[72]) to a North Korean initiative in response to the release of a film about the fictional assassination of Kim Jong Un.[73]

This disjuncture in perceptions is arguably at the heart of the tension in this 'partnership'. Typically, the rationale articulated in the literature for partnering is that neither partner on its own can achieve its desired objectives. Either each must need the other to achieve its own goals or there must be a financial arrangement that makes the partnership attractive to both parties. It is difficult to ascribe either of these rationales comprehensively in the single most emphasized practice in this partnership—information sharing. Although there may be a financial component to information sharing (paying for intelligence on vulnerabilities and attack vectors) and although there may also be some shared incentives, neither of these adequately encompasses the dynamics of the public–private partnership in this context. Perhaps information sharing can best be understood in the second of Stephen Linder's 'types' of public–private partnerships—*partnerships as power sharing*.

Linder writes that *partnerships as power sharing* are based on an ethos of cooperation where 'trust replaces the adversarial relations endemic to command-and-control regulation' and where there is some mutually beneficial sharing of responsibility,

[68] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 53.
[69] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 53.
[70] Sam Varnado, written response to questions from Representative Bennie G. Thompson at 'SCADA systems and the terrorist threat', p. 95.
[71] Varnado, written response, 'SCADA systems and the terrorist threat', p. 95.
[72] Kim Zetter, 'The evidence that North Korea hacked Sony is flimsy', *Wired Magazine*, 17 Dec. 2014, http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/; Marc Rogers, 'Why I still don't think it's likely that North Korea hacked Sony', *Marc's Security Ramblings*, 21 Dec. 2014, http://marcrogers.org/2014/12/21/why-i-still-dont-think-its-likely-that-north-korea-hacked-sony/; Bruce Schneier, 'More data on attributing the Sony attack', *Schneier on Security*, 31 Dec. 2014, https://www.schneier.com/blog/archives/2014/12/more_data_on_at.html (all accessed 4 Nov. 2015).
[73] Barack Obama, 'Executive Order—imposing additional sanctions with respect to North Korea' (Washington DC: The White House, 2 Jan. 2015).

knowledge or risk. In most instances, he writes, 'each party brings something of value to the others to be invested or exchanged'. Finally, 'there is an expectation of give-and-take between the partners, negotiating differences that were otherwise litigated'.[74] The text above has explained how this partnership is characterized not by *shared* responsibility but by *disputed* responsibility. Sharing knowledge, however, is certainly regarded by both partners as integral to this relationship, and building trust and collaboration is a dominant theme running through not only the strategy documents but also the responses from the private sector.

The practice of information sharing as a partnership

There can be little doubt that the main expectation of cooperation within the public–private partnership is found in the emphasis on information sharing.[75] In July 2010, the US Government Accountability Office (GAO) published a report entitled *Critical infrastructure protection*, with the subtitle: *Key private and public cyber expectations need to be consistently addressed*.[76] The purpose of the study was to clarify the partnership expectations of both the public and the private sectors and to determine the extent to which those expectations were being met. This study was limited to five key critical infrastructure sectors deemed to be most reliant on cyber security.[77]

The provision of timely and actionable cyber-threat and alert information emerges as a key expectation of the partnership from both the public and the private sector, but there are a number of obstacles to sharing information from both perspectives.[78] The private sector reports that it is not always easy to immediately distinguish between some kind of technical problem, a low-level attack and a large-scale sustainable attack.[79] In addition, it sometimes runs counter to their commercial interests to report vulnerabilities, particularly if understanding and rectifying a problem before competitors become aware of it could offer a market edge.[80] Finally, if a private security firm shares information with the government about an attack, that information may be shared with its competitors.[81] For private-sector security firms, their business model is reliant on obtaining, holding and selling information, not sharing it.[82]

The public sector also encounters limitations to sharing information. Classified contextual information cannot be shared with individuals who do not have adequate security clearance. Even those working in the private sector who do have security clearance can often do nothing with classified information because to take

[74] Linder, 'Coming to terms with the public–private partnership', p. 47.
[75] Dunn Cavelty and Suter, 'Public–private partnerships are no silver bullet, p. 181.
[76] David A. Powner, *Critical infrastructure protection: key private and public cyber expectations need to be consistently addressed* (Washington DC: Government Accountability Office, July 2010).
[77] Powner, *Critical infrastructure protection*, p. 27.
[78] Powner, *Critical infrastructure protection*, p. 23.
[79] Author's interview with UK-based private cyber-security firm, 2014.
[80] Author's interview with UK-based private cyber-security firm, 2014.
[81] Powner, *Critical infrastructure protection*, p. 22.
[82] Author's interview with US-based private cyber-security firm, 2014.

action on it would be to expose it.[83] In addition, there is a high expectation that threat information shared from the public to the private sector will be accurate, and this leads to extensive and stringent review and revision processes that delay the release of time-critical information.[84] This problem of sharing information has persistently been regarded as a key impediment to cyber security, and was highlighted by a senior official in testimony before a congressional hearing on cyber security in 2011 as one of two main areas that needed improvement.[85]

Significantly, private-sector interviews consistently revealed that personal relationships were central to effective information sharing.[86] That is, people were much more inclined to share information with colleagues with whom they had a strong personal and/or professional bond. This human factor is important and should be further investigated in order to identify ways to establish and strengthen these relationships in sectors of network security and the public service, which are characterized by a relatively high turnover of staff.

Key objectives and markers of success

By the late 1990s, the critical literature looking more broadly at public–private partnerships was maturing and there was a realization that evaluation of these arrangements was complex and under-researched. Essentially, there was little evidence to suggest what the success or failure rate of these arrangements was. In fact, there was not really even a conceptual framework for doing so. In 1999, *American Behavioral Scientist* published a special issue dedicated to these questions. In the introduction, Pauline Vaillancourt Rosenau summarized many of the arguments set out in the contributions to the journal issue in writing that:

> in general, partnering success is more likely if (a) key decisions are made at the very beginning of a project and set out in a concrete plan, (b) clear lines of responsibility are indicated, (c) achievable goals are set down, (d) incentives for partners are established, and (e) progress is monitored.

She also identified a set of criteria for the measurement of success—some of which are useful in relation to the case considered here, particularly accountability and possible conflicts of interest.[87]

In terms of conflict of interest, Vaillancourt Rosenau makes the case that partnerships do not (as many assume) necessarily reduce regulation. If the interests of the private sector are misaligned with normative goals such as care for the vulnerable (for example, in respect of homes for the elderly), then the government must monitor and regulate to ensure the profit motive does not supersede

[83] Author's interview with UK-based private cyber-security firm, 2015.
[84] Powner, *Critical infrastructure protection*, p. 17.
[85] Wilshusen, 'Cyber security', p. 8.
[86] Author's interviews with UK and US private-sector representatives from critical infrastructure owners/operators, 2014–15.
[87] Pauline Vaillancourt Rosenau, 'The strengths and weaknesses of public–private policy partnerships', *American Behavioral Scientist* 43: 1, Sept. 1999, pp. 11–12.

International Affairs 92: 1, 2016

the intended delivery of service.[88] Here we see the profile of one of the central problems of this public–private partnership: the expectation that the private sector will invest in cyber security beyond its cost/benefit analysis to fully accommodate the public interest—in other words, to ensure national security. Because market incentives are not adequate to promote this level of security, oversight and some level of regulation are necessary. A 2013 GAO report found that many of the experts consulted argued that the private sector had not done enough to protect critical infrastructure against cyber threats.[89] The private sector explanation for not fully engaging in the government's cyber-security strategy was that the government had failed to make a convincing business case that mitigating threats warranted substantial new investment.[90]

Dunn Cavelty and Suter argue that while public–private cooperation is necessary, the way it is organized and conceptualized needs to be rethought. They propose to do so through governance theory and they find that critical infrastructure protection policy 'should be based as far as possible on self-regulating and self-organising networks'.[91] By this, they mean that 'the government's role no longer consists of close supervision and immediate control, but of coordinating networks and selecting instruments that can be used to motivate these networks for CIP tasks'.[92] This may provide some forward momentum, though Vaillancourt Rosenau makes the point that a public–private partnership cannot be regarded as a success if it 'results in lower quality of public policy services, the need for more government oversight, and the need for expensive monitoring, even if it appears to reduce costs'.[93] Perhaps more problematic for Dunn Cavelty and Suter's recommendation is the question of accountability.

On accountability, Vaillancourt Rosenau writes that because these partnerships often see policy decisions and practices that are normally reserved for elected officials delegated to the private sector, accountability is essential to maintaining a healthy democratic order. If responsibility and accountability can be devolved to private actors, the central principle that political leaders and governments are held to account is undermined.[94] For many scholars, to ensure effective accountability in a public–private partnership, the specifics of roles and responsibilities must be made clear at the outset and goals must be clearly articulated.[95] Stiglitz and Wallsten observe that in the process of doing this, it becomes clear when additional incentives and resources are necessary to achieve agreed goals, and these must be provided if accountability is to be sustained.[96] In cases such as cyber security, in which the end goal for government is the public good, accountability—like the

[88] Vaillancourt Rosenau, 'The strengths and weaknesses of public–private policy partnerships', pp. 18–19.
[89] Gregory C. Wilshusen and Nabajyoti Barkakati, *Cybersecurity: national strategy, roles, and responsibilities need to be better defined and more effectively implemented* (Washington DC: GAO, Feb. 2013), p. 49.
[90] Wilshusen and Barkakati, *Cybersecurity*, p. 49.
[91] Dunn Cavelty and Suter, 'Public–private partnerships are no silver bullet', p. 180.
[92] Dunn Cavelty and Suter, 'Public–private partnerships are no silver bullet', p. 180.
[93] Vaillancourt Rosenau, 'The strengths and weaknesses of public–private policy partnerships', p. 18.
[94] Vaillancourt Rosenau, 'The strengths and weaknesses of public–private policy partnerships', p. 19.
[95] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 57.
[96] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 57.

alignment of interests discussed above—does not appear to emerge from market forces alone.[97] This is not to suggest that public–private partnerships cannot be successful when interests and objectives diverge; but, in the view of Stiglitz and Wallsten, in these cases 'more attention needs to be placed on the incentive-accountability structure'.[98]

The GAO report referred to above is also useful in analysing the key objectives of this partnership and in measuring its success.[99] The report found that in addition to information sharing, there were two main expectations that the government holds of the private sector in this partnership. First, it is expected that private-sector partners will commit to executing plans and recommendations such as best practices.[100] This is important, because it is an example of the government shifting responsibility to the private sector in the understanding that if the private sector responds adequately, then regulation can be avoided. The study reported that four of the five sectors examined were meeting government expectations to a 'great/moderate' degree. The exception was the IT sector, which was reported as demonstrating 'little/no' commitment to execute plans and recommendations such as best practice.[101] In fact, the IT sector meets government expectations to a 'great/moderate' degree on only one out of ten criteria—technical expertise. On all other criteria, this sector is ranked as meeting expectations to 'some' or 'little/no' degree. Given the reliance of the other sectors on the IT sector, this deficit is particularly worrying and must undermine the others' compliance to some extent. It also highlights the fact that the private sector is not accountable to the same degree that the public sector would be if it were offering the same services.[102]

Conclusion

Somewhat surprisingly, given its centrality in successive cyber-security policies produced by the UK and the US, exactly what the public–private 'partnership' entails has always been unclear. In the face of the continuing challenge of conceptualizing cyber security within a national security framework, this article has argued that a sensible starting-point would be to speak with clarity about the tensions and competing agendas that characterize the public–private partnership (particularly in the context of critical infrastructure protection) rather than to shroud them in normative 'new management' language.

Although politicians often appear to subscribe to the notion that there exists (or should exist) a deeply entrenched norm of cooperation between the government and private sector, this is clearly not the case. Rather, the private sector

[97] H. M. Levin, 'The public–private nexus in education', *American Behavioral Scientist* 43: 1, 1999, pp. 124–37; M. S. Sparer, 'Myths and misunderstandings: health policy, the devolution revolution, and the push for privatization', *American Behavioral Scientist* 43: 1, 1999, pp. 138–54, both cited in Vaillancourt Rosenau, 'The strengths and weaknesses of public–private policy partnerships', p. 21.
[98] Stiglitz and Wallsten, 'Public–private technology partnerships', p. 57.
[99] Powner, *Critical infrastructure protection*, pp. 22–3.
[100] Powner, *Critical infrastructure protection*, pp. 22–3.
[101] Powner, *Critical infrastructure protection*, p. 22.
[102] Author's interview with UK cyber-crime law enforcement representative, 2014.

has consistently (and perhaps understandably) expressed an aversion to accepting responsibility or liability for national security and regards cyber security within a cost/benefit framework rather than a 'public good' framework. The public–private partnership is consistently referred to in strategy documents using normative, value-based language rather than clear statements outlining legal authority, responsibility and rights across the diverse set of relationships that these governments maintain with the private sector. While this article does not argue that this latter type of regulation is necessarily the answer, it does point out why the partnership arrangement cannot work effectively in its current form. Successful public–private partnerships are either characterized by shared interests or, if the interests of the partners are not well aligned, governed by rules. This arrangement has neither shared interests nor rules in sufficient quantity.

In essence, while states like the UK and the US are relying on the private sector for a key element of national security, in the context of critical infrastructure protection (a persistent and key concern for national cyber-security policymakers) this entails reliance on a dysfunctional partnership. Several possible conclusions arise from this analysis. First—the core contribution of this article—the weaknesses in the partnership must be openly acknowledged so that we may begin to develop mechanisms to address them. Second, it could be more useful to cease to use the term 'partnership' and talk instead of a 'relationship'. Third, we might begin to think more laterally about how cyber security fits within a national security framework. It might be more appropriate to develop a national cyber-*resilience* strategy instead of a national cyber-*security* strategy. Finally, it would be useful to look more closely at how states that have retained public ownership of critical infrastructure deal with cyber security in this context and how states with more control over their private sector are addressing similar national cyber-security concerns.

Although it may not be entirely surprising that there are significant problems with this public–private partnership, it is important to remember that this is the 'cornerstone' of UK and US national cyber-security strategies. In both the UK and the US, we are witnessing a unique approach to 'outsourcing' national cyber security, and this raises questions about how well the state is equipped to provide this security and about how existing policies and practices of national security are being challenged by this partnership for the provision of national security. States with greater government control over critical infrastructure and also over their information infrastructure potentially have a significant advantage in that they are able to control and shape their response to cyber insecurity with greater autonomy. It is possible that a market-led approach to national cyber security will prove to be less effective than a state-led approach. It is also possible that we need to rethink the breadth and depth of security that we can usefully attach to expectations of national cyber security. Acknowledging these uncomfortable facts is essential to developing a more robust approach to state security in the information age.