The Problem of the P3: Public-Private Partnerships in National Cyber Security Strategies

Madeline Carr[1] and Tom Crick[2]

[1]Department of International Politics, Aberystwyth University
[2]Department of Computing & Information Systems, Cardiff Metropolitan University
[1]madeline.carr@aber.ac.uk
[2]tcrick@cardiffmet.ac.uk

Abstract

Cyber security is an emerging – and high profile – national security concern; not only in terms of material vulnerabilities but also in terms of conceptualising security approaches. Many states, particularly Western democracies, have situated the 'public-private partnership' (P3) at the centre of their national cyber security strategies. However, there has been a persistent ambiguity around this fundamental concept. Policymakers regard the state as without the capability and also without the mandate to impose security requirements beyond government-owned systems. The private sector, however, is highly averse to accepting responsibility for national security and will fund cyber security only within the parameters of the profit/risk calculation appropriate for a shareholder-based arrangement. Amidst increasing suggestions that a market-led approach to cyber security has failed, a deeper look at the ideas and concepts behind this approach finds that a reliance on the P3 emerges from deeply held and shared beliefs about government legitimacy and private authority which may not be easily reconciled with wider national security issues for a modern digital economy.

1 Introduction

Cyber security is emerging as one of the most challenging aspects of the information age for policymakers and scholars of international relations. 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, 3]. In response, governments have begun to develop national cyber security strategies to outline the way in which they intend to address cyber insecurity. In many states where critical infrastructure such as utilities, financial systems and transport have been privatised, 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 US and the UK, the public-private partnership has repeatedly been referred to as the 'cornerstone' or 'hub' of cyber security strategy [1, 4, 5].

While public-private partnerships have often been developed as an appropriate means to address both non-traditional and traditional security threats [6, 7], in the context of cyber security this arrangement is uniquely problematic. There has been a persistent ambiguity with regard to any clear and agreed parameters for the partnership. The reticence of politicians to claim authority for the state to legislate tougher cyber security measures coupled with the private sectors aversion to accepting responsibility or liability for national security leaves the 'partnership' without clear lines of responsibility or accountability. Questions are now being raised (including by Obama and the US Government) about the efficacy of a market-driven approach to cyber security, although any alternative in liberal democratic states has yet to emerge [2]. Crucially, 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 [8] 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'. 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 paper develops a comprehensive understanding of how policymakers and the private sector are conceptualising 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. The paper moves onto the analysis of the public-private partnership from the perspectives of both partners. It should be noted here that there is a round of interviews yet to be completed for this project which will contribute further to the analysis. What is presented here is the conceptual framework and the outcome of documentary research.

2 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. 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 [9]. The potential implications of a large scale cyber attack on critical infrastructure are so extensive that it follows naturally that the government would recognise 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 sector in terms of the provision of security in this context.

The public-private partnership is not of course, unique to cyber security. It has been employed widely by states like 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 privatisation of critical infrastructure was regarded as economically beneficial to the state, freeing up capital and relying more heavily on the efficiencies and business practices of the private sector. There is an extensive body of literature that has developed in the wake of this shift that examines the public-private partnership in all kinds of contexts. It deals with the background of these partnerships, the range of different approaches, how to measure success and failure, and how responsibility and authority are delegated. There has also been some examination of the public-private partnership in cyber security, most notably by Dunn Cavelty and Suter [8], but this focuses on ways to improve it rather than critically analysing the political implications of it. Combined, this literature provides a solid foundation in highlighting the ways in which this partnership is distinct but also by outlining common assumptions and expectations that run through public-private partnerships more generally.

2.1 What is this public-private partnership?

It is necessary to be clear about what exactly is meant by the term public-private partnership in this particular context. Perhaps not unexpectedly, there is a huge range of diverse arrangements that are referred to as public-private partnerships, ranging from the joint provision of services with some government regulatory oversight (health sectors), to closely contracted outsourcing of large infrastructure projects, (building roads and bridges, the Olympics, etc). Much of the literature on public-private partnerships revolves around identifying and classifying partnership arrangements. This often takes place within a framework of authority and responsibility - key concepts for this study. In examining these relationships, Wettenhall [10] identifies two broad categories: a) horizontal, non-hierarchical arrangements characterised by consensual decision-making and b) hierarchically organised relationships with one party in a controlling role. The implication being, he argues, that true 'partnerships' are of type a) and not type b).

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 [11] 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.' With specific reference to the role of the private sector, it states that there is an expectation that the private sector 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' [12]. This non-hierarchical language belies the poor alignment of perceptions about the 'common challenge' and the 'threats we face in cyberspace' [13]. It assumes that those are the same for the public and 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, Linder [14] identifies six distinctive uses of the term P3 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.' 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. 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 [14]. Perhaps not surprisingly, although this is reflected in the strategies of both states, it is much more pronounced in the US documents.

The [George W.] Bush Administrations National Strategy to Secure Cyberspace [4] argued that in the US "traditions of federalism and limited government require that organizations outside the federal government take the lead" in cyber security. This interpretation of the 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." This is based on the belief that "in general, the private sector is best equipped and structured to respond to an evolving cyber threat" and, at a US Congressional hearing in 2000, Deputy Attorney General Eric Holders statement that decision makers in the US "believe strongly that the private sector should take the lead in protecting private computer networks." [15] 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 sectors system administration." [16].

So 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, they must take responsibility and liability for their own network security and second, their superior capacity for flexibility and innovation means that they are best placed take the lead on this particular security problem. The problem of course, is that these networks are central to national security and therein lies the problem from the perspective of the private sector.

The private sector develops security strategy within a very different framework to that of 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 them in the cyber security strategies. First, they argue that the expense of ensuring cyber security to a national security level would be significant and second, that the litigious nature of (especially US) society means that industry would be very resistant to accepting liability for the security of their products or systems [17].

Stiglitz and Wallsten [18] make some important observations about this dichotomised approach to public-private partnerships in the context of technology innovation. 'Theory predicts' they argue, 'and many empirical studies confirm, that profit-maximising firms invest less than the socially optimal level of [technology research and development].' What is in societys 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.

So private sector owners of critical infrastructure accept responsibility for securing their systems – to that point that it is profitable. That is, that the cost of dealing with an outage promises to cost more

than prevention. However, they tend to make a distinction between protecting against the low-level threat such as "background noise, individual hackers, and possibly hacktivists" and protecting against an attack on the state (national security). In testimony at a US hearing on privately owned critical infrastructure cyber security, one witness explained that "it is industrys contention that government should protect against the larger threats – organized crime, terrorists, and nation-state threats – either through law-enforcement or national defense." [19].

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 their desired objectives. They must either need each other or there must be a financial arrangement that makes the partnership attractive. This, we can observe most readily in the single most emphasised practice in this partnership – information sharing. And information sharing can be understood in the second of 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 in which there is some mutually beneficial sharing of responsibility, knowledge, or risk. In most instances, he writes, 'each party brings something of value to the others to be invested or exchanges'. Finally, 'there is an expectation of give-and-take between the partners, negotiating differences that were otherwise litigated.' [14]. The previous section explains how rather than shared responsibility, this partnership is characterised 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.

2.2 The practice of information sharing as a partnership

There can be little doubt that the main form of cooperation within the public-private partnership is found in the shared emphasis on information sharing [8]. In July 2010, the US Government Accountability Office published a report entitled *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed* [20]. The purpose of the study was to clarify the partnership expectations of both the public and private sectors and to determine the extent to which those expectations were being met. The study was limited to five key critical infrastructure sectors deemed to be most reliant on cyber security: communications, defence industrial base, energy, banking and finance, and information technology.

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 sectors but there are a number of obstacles to sharing information from both perspectives. 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. In addition, it sometimes runs counter to their commercial interests to report vulnerabilities. Finally, for private security firms, sharing information with the government about attacks, could lead to it being shared with their competitors. Their business model is reliant on obtaining, holding and selling information, not sharing it [20].

The public sector also encounters limitations to sharing information. Classified contextual information cannot be shared with individuals who do not have adequate security clearances. Even those working in the private sector who do have security clearance can often do nothing with classified information because to take action on it would expose it. 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 also delay the release of time critical information [20]. This problem of sharing information has persistently been regarded as a key impediment to cyber security and in testimony before a US Congressional hearing on cyber security in 2011, a senior official highlighted this as one of two main areas that needed improvement [21].

2.3 Key objectives and markers of success

By the late 1990s, the critical literature looking at public-private partnerships was maturing and there was a realisation that evaluating these arrangements was complex and under-researched. Essentially, there was little evidence to suggest what the success/failure rate of these arrangements was. In fact,

there was not really even a conceptual framework for doing so. In 1999, *American Behavioural Scientist* published a special issue dedicated to these questions. In the introduction, Rosenau summarises [22] many of the journal arguments when she writes 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 identifies a set of criteria for the measurement of success – some of which are useful in considering this case, particularly accountability and possible conflicts of interest.

In terms of conflict of interest, she 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 like care for the vulnerable (for example, old age homes) then the government must monitor and regulate to ensure the profit motive does not supersede the intended delivery of service [22]. 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 their 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 US Government Accountability Office report [23] found that many of the experts they consulted argued that the private sector had not done enough to protect critical infrastructure against cyber threats. The private sector explanation for not fully engaging in the governments cyber security strategy was that the government had failed to make a convincing business case that mitigating threats warranted substantial new investment. Dunn Cavelty and Suter argue that while public private cooperation is necessary, the way it is organised and conceptualised needs to be rethought. They propose to do so through governance theory and they find that 'CIP policy should be based as far as possible on self-regulating and self-organising networks'. By this, they mean that '...the governments 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.' [8]. This may provide some forward momentum though Rosenau makes the point here 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'. Perhaps more problematically for Dunn Cavelty and Suters recommendation is the problem of accountability.

On accountability, 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 [22]. 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. In addition, Stiglitz and Wallsten [18] observe that in doing so, 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. In cases such as cyber security, in which the public good is the end goal for government, as with the alignment of interests discussed above, accountability does not appear to emerge from market forces alone, nor is it a trivial undertaking [24]. 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' [18].

The 2010 US GAO report [20] referred to previously is also useful for the analysis of key objectives of this partnership and for measuring its success. 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 was expected that they would commit to execute plans and recommendations such as best practices. 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, 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. In fact, the IT sector meets only one out of ten services expected by the government to a 'great/moderate' degree

technical expertise. On all other criteria, this sector ranked at 'some' or 'little/no' [20]. Given the reliance of the other sectors on the IT sector, this deficit is particularly concerning and to some degree, has to undermine the others' compliance.

The second key expectation (apart from information sharing) identified in the GAO report is that the private sector will provide appropriate staff and resources. Only banking/finance and commerce were reported to be meeting this expectation to a 'great/moderate' degree with defence industrial base, energy and IT all being ranked at 'some'.

3 Conclusions

At this stage, prior to the fieldwork interviews, it is possible to draw preliminary conclusions. First, and somewhat surprisingly given its centrality in successive cyber security policies, exactly what this 'partnership' entails has always been unclear. Unpacking it has revealed that there are inherent tensions and misaligned objectives that are not in keeping with expectations of public-private partnership arrangements. The partnership is consistently referred to in strategy documents using normative, value based language rather than clear statements outlining legal authority, responsibility and rights. Although politicians subscribe to the notion that there exists (or should exist) a deeply entrenched norm of cooperation between the government and private sector this appears not to be the case. Rather, the private sector has consistently expressed an aversion to accepting responsibility for national security and regard cyber security within a cost/benefit framework rather than a 'public good' framework.

The second conclusion to arise from this study is that we are witnessing a unique approach to 'outsourcing' national security that has implications for conceptions of state power, global security and international partnerships and resource-sharing. 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 and agency. This is of particular relevance to emerging UK cyber security strategy and needs to be considered more thoroughly from a research, policymaking and national infrastructure perspective.

References

[1] Bill Clinton. Speech on the economy at Wharton School of Business, University of Pennsylvania. http://www.ibiblio.org/nii/econ-posit.html, April 1992.

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

[3] House of Commons. Scientific advice and evidence in emergencies. HC 498, Science and Technology Select Committee, February 2011.

[4] George W. Bush. The National Strategy to Secure Cyberspace. The White House, February 2003.

[5] Francis Maude. Cyber Security Strategy one year on, speech on the 2012 Information Assurance Conference. https://www.gov.uk/government/speeches/francis-maude-speech-at-ia12-cyber-security-strategy-one-year-on, December 2012.

[6] Max G. Manwaring. *The Inescapable Global Security Arena*. Strategic Studies Institute, US Army War College, 2002.

[7] US Department of Commerce. White House Announces Public-Private Partnership Initiatives to Combat Botnets. http://www.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b, May 2012.

[8] 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):179–187, 2009.

[9] Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda. Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, 20(2):96–121, 2014.

[10] Roger Wettenhall. The Rhetoric and Reality of Public-Private Partnerships. *Public Organization Review*, 3(1):77–107, 2003.

[11] Cabinet Office. Cyber Security Strategy. UK Government, 2011.

[12] Cabinet Office. National Cyber Security Strategy 2013: forward plans and achievements. UK Government, 2013.

[13] Amyas Morse. The UK Cyber Security Strategy: Landscape Review. UK National Audit Office, 2013.

[14] Stephen H. Linder. Coming to Terms With the Public-Private Partnership: A Grammar of Multiple Meanings. *American Behavioral Scientist*, 43(1):35–51, 1999.

[15] Eric H. Holder, Jr. Statement before the Subcommittee on Communications, Senate Committee on Commerce, Science and Transportation. http://www.justice.gov/archive/dag/testimony/holderinternet38.htm, March 2000. US Deputy Attorney General.

[16] Michael A. Vatis. Statement before the Senate Armed Services Committee. http://fas.org/irp/congress/2000_hr/000301mv.pdf, March 2000. Deputy Assistant Director, Federal Bureau of Investigation.

[17] Alan Paller. SCADA Systems and the Terrorist Threat: Protecting the Nations Critical Control Systems. Statement before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, House Committee on Homeland Security. http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg32242/html/CHRG-109hhrg32242.htm, October 2005. Director of Research, The SANS Institute.

[18] Joseph E. Stiglitz and Scott J. Wallsten. Public-Private Technology Partnerships: Promises and Pitfalls. *American Behavioral Scientist*, 43(1):52–73, 1999.

[19] Sam Varnado. SCADA Systems and the Terrorist Threat: Protecting the Nations Critical Control Systems. Statement before the Subcommittee on Emergency Preparedness, Science and Technology, House Committee on Homeland Security. http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg32242/html/CHRG-109hhrg32242.htm, October 2005. Director of Information Operations Center, Sandia National Laboratory.

[20] David A. Powner. Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. US Government Accountability Office, July 2010.

[21] Gregory C. Wilshusen. Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems. Statement before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, House Committee on Homeland Security. http://www.gao.gov/assets/130/125787.html, March 2011. Director Information Security Issues, US Government Accountability Office.

[22] Pauline Vaillancourt Rosenau. The Strengths and Weaknesses of Public-Private Policy Partnerships. *American Behavioral Scientist*, 43(1):10–34, 1999.

[23] Gregory C. Wilshusen and Nabajyoti Barkakati. Cyber Security: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. US Government Accountability Office, February 2013.

[24] Colin Williams. Security in the cyber supply chain: Is it achievable in a complex, interconnected world? *Technovation*, 34(7):382–384, 2014. Special Issue on Security in the Cyber Supply Chain.