Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order

McCarthy, Daniel R.

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*, *6*(2), 5-12. https://doi.org/10.17645/pag.v6i2.1335

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 5–12
DOI: 10.17645/pag.v6i2.1335

Article

Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order

Daniel R. McCarthy

School of Social and Political Sciences, University of Melbourne, 3051 Melbourne, Australia;
E-Mail: daniel.mccarthy@unimelb.edu.au

Submitted: 30 December 2017 | Accepted: 28 February 2018 | Published: 11 June 2018

Abstract
Cybersecurity sits at the intersection of public security concerns about critical infrastructure protection and private security concerns around the protection of property rights and civil liberties. Public-private partnerships have been embraced as the best way to meet the challenge of cybersecurity, enabling cooperation between private and public sectors to meet shared challenges. While the cybersecurity literature has focused on the practical dilemmas of providing a public good, it has been less effective in reflecting on the role of cybersecurity in the broader constitution of political order. Unpacking three accepted conceptual divisions between public and private, state and market, and the political and economic, it is possible to locate how this set of theoretical assumptions shortcut reflection on these larger issues. While public-private partnerships overstep boundaries between public authority and private right, in doing so they reconstitute these divisions at another level in the organization of political economy of liberal democratic societies.

Keywords
capitalism; critical infrastructure protection; critical theory; cybersecurity; public-private partnerships

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

The politics of infrastructure are central to the governance of modern societies. Large Technical Systems (LTS) shape all aspects of our everyday lives, in ways both visible and hidden. The ubiquity of infrastructures and their capacity to mediate relations between different social actors demand careful analytical attention and the development of conceptual frameworks appropriate to capture the complex social, political and economic processes that drive their development and reproduction. As a practical political issue this task is important; clarifying where the power to shape modern life lies is central to understanding how our world is made, illuminating issues of political and moral responsibility that surround the politics of technology.

As this thematic issue makes clear, studies of cybersecurity require further theoretical and conceptual groundclearing to produce these insights. By and large, the literature on critical infrastructure protection and cybersecurity has remained within a problem-solving framework, in which the existing social order forms the background premises within which a problem is posed (Cox, 1981; Dunn Cavelty, 2013, p. 106). The provision of cybersecurity has been studied within a relatively narrow set of assumptions, with questions central to security studies, and politics more broadly, circumscribed. This is particularly evident in the literature on public-private partnerships (PPPs) as a route to the provision of cybersecurity in liberal democracies. Building on an emerging literature that seeks to sharpen the analytical focus of an often vague or underspecified set of issues (Carr, 2016; Dunn Cavelty, 2014), the starting point for this article is a rather simple question: what is cybersecurity and critical infrastructure protection for?

Answering this question, while not straightforward, can be clarified by problematising a set of commonsense assumptions apparent within studies of PPPs

about how political life can and should be organized. The literature on cybersecurity and critical infrastructure protection needs to be theoretically 'deepened' to clarify a broader grasp of what cybersecurity is for, and to highlight potential political alternatives. Considering what cybersecurity is for requires moving beyond a narrow issue-specific focus to consider how cybersecurity practices relate to existing social formations. To foreshadow the argument developed below, the central move in this article is an interrogation of the conceptual separation of the political and the economic, and its related binaries of public/private and state/market, in the field of cybersecurity. Once we being to question the seeming naturalness of this divide it becomes possible to articulate the wider stakes of cybersecurity with greater clarity.

This article will proceed as follows. First, it will set out the dominant approach that views cybersecurity as a public good, and thereby frames its provision as a collective action problem. The United States will serve as the empirical referent point. Understood in these terms, everyone benefits from cybersecurity. Second, it will discuss the conceptual binaries, noted above, that form the starting point for these analyses. These sections will discuss how the assumption of state autonomy in collective action models underpins the conceptual divisions between public and private, state and market, and politics and economics. Schematic in nature, these sections nevertheless draw attention to a series of problematic theoretical assumptions around these binaries. Finally, it will argue that assuming a division between these various spheres of social life obscures the role of PPPs in (re)producing the specific forms of liberal political order. PPPs are a method of collaboration designed to reproduce the privatization of political power that characterizes modern liberal capitalist society. This article thereby contributes a growing literature seeking to clarify how relations of power and accountability operate in cybersecurity PPPs, outlining the limits liberalism itself sets on making certain forms of social power accountable.

2. Public-Private Partnerships, Public Goods, and Problem Solving Theories

Provision of security, physical or otherwise, is classically the function of the state. Whether applied to national security or domestic policing, in modern liberal capitalist societies it is the state that has been tasked to carry out these duties. So central is the state to the provision of security that the shift away from this liberal norm, evident in the greater use of private military and security contractors (PMSCs) globally, has generated substantial analytical and political attention (Abrahamsen & Williams, 2010; Avant, 2005). Privatizing the provision of security has generated concern around private firms' potential conflicts of interests, with PMSCs accountable to both public authorities and their shareholders.

Cybersecurity, by contrast, does not centre on the privatization of existing security functions. Concerns about the outsourcing of cybersecurity are largely misplaced; states are not contracting out security functions to the private sector, and thus security is not being privatized in the same manner as it is for other security issues (Eichensehr, 2017, pp. 471–473; cf. Carr, 2016). Cybersecurity and critical infrastructure protection policies attempt to secure infrastructures owned by both the public and private sectors. The objects of protection in this space—from critical infrastructures to information and data—are overwhelmingly in private hands, with over 90% of critical infrastructures in the United States owned by the private sector (Singer & Friedman, 2014, p. 19). This includes hardware and software infrastructures as they extend inside the homes of ordinary Americans; current estimates place internet penetration rates at 88%, an indication of how broadly the problem of cybersecurity extends (Pew Research Center, 2017). Cybersecurity requires private citizens, corporations, and the state to contribute to the provision of security for the networks on which they depend. Indeed, successive American administrations have stressed this point, emphasizing the need for 'awareness raising' to promote better 'cyber hygiene', using public health metaphors to emphasize the shared nature of the challenge (Stevens & Betz, 2013; United States Department of Homeland Security, 2017).

Cybersecurity, like national security more broadly, thereby appears to have the character of a public good: it is non-rivalrous and non-excludable (Assaf, 2008, p. 13; Shore, Du, & Zeadally, 2011). Rational choice approaches to politics suggest that public goods should be provided by the state, as private actors incentive structure pushes them to free ride, inducing market failure. However, state provision of cybersecurity is not a straightforward option. Dunn Cavelty and Suter (2009, p. 179) highlight the contradictions at the heart of critical infrastructure protection:

> [Privatization policies] have put a large part of the critical infrastructure in the hands of private enterprise. This creates a situation in which market forces alone are not sufficient to provide security in most of the CI [Critical Infrastructure] 'sectors'. At the same time, the state is incapable of providing the public good of security on its own, since overly intrusive market intervention is not a valid option either; the same infrastructures that the state aims to protect due to national security considerations are also the foundation of the competitiveness and prosperity of a nation.

The problem for governments is how to provide the public good of cybersecurity in a context in which intervention in economic decision-making presents its own distinct risks. Caught between the Scylla of market failure in cybersecurity provision and the Charybdis of state planning, policymakers face a difficult decision: too little intervention and the required public good will not be provided; but too much and other facets of national security are undermined. Navigating these dilemmas is

thereby understood as the central political task faced by policymakers.

PPPs present themselves as an effective middle way, allowing the state to engage in *ex ante* decisions regarding cybersecurity outcomes in careful consultation with the private sector. This combination of planning with market-led flexibility is embraced by policymakers as a central rationale for promoting PPPs (United States National Science and Technology Council, 2011). While cooperation is not straightforward, there are shared interests at work here, even if the precise motivations behind those interests are distinct. As Eichensehr notes, cooperation allows government to control public expenditure costs and avoid private sector interference with crucial state functions, while helping the private sector secure its intellectual property and, relatedly, its business reputation (Carr, 2016, p. 55; Eichensehr, 2017, pp. 500–504).

The devil is, of course, in the details. Working out how to make these partnerships function effectively, both in the United States and elsewhere, has been the focus of sustained analysis (Carr, 2016; Givens & Busch, 2013; Harknett & Stever, 2011). Analysis revolves around determining the institutional forms, policy processes, and levels of state intervention through which PPPs can most effectively provide security. These problems have been largely (but not exclusively) understood as collective action problems—everyone has an interest in the provision of cybersecurity, but everyone also has an incentive to free ride if possible. Solutions to these problems seek ways to alter these incentive structures through, for instance, institutions designed to share information, such as the United States Department of Homeland Security's Cyber Information Sharing and Collaboration Programme (CISCP), or via the creation of trust building mechanisms between firms and between firms and the state.

Practical and normative questions are inevitably raised when considering PPPs in cybersecurity, in keeping with the broader literature on PPPs (Brinkerhoff & Brinkerhoff, 2011; Linder, 1999). Defining the scope of private sector authority and responsibility for cybersecurity, particularly as it impacts upon other aspects of national security such as intelligence collection, has generated both policy-centred proposals, such as those noted above, and more abstract reflection on the appropriate level of political authority assumed by private actors. Practically, it has involved attempts to parse apart the responsibilities of different sets of cybersecurity actors in order to develop clear rules around the scope of responsibility for the public and private sector. Understanding who has power to affect change, and how this occurs, is important for this task.

Normative discussion has focused upon issues of political authority and accountability. This last aspect begins to hint at the larger political issues posed by PPPs as a solution to cybersecurity provision. Carr (2016, p. 60) notes that 'If responsibility and accountability can be devolved to private actors, the central principle that political leaders and governments are held to account is undermined'. As with the literature on PMSCs, concern over the conflicting interests of private firms has led analysts to caution against any easy recourse to market-led cybersecurity frameworks (Assaf, 2008; Carr, 2016, p. 62). Multiple lines of accountability may, it is suggested, undermine the responsiveness of PPPs to the public.

Steps in this direction are important to deepening the study of cybersecurity. Yet, to date, this not resulted in consideration of how cybersecurity policies relate to political order. Questions of where political responsibility can and should lie—with the state, the private sector, or a combination of these—are constituted by the specific institutional order of modern liberal capitalism and its attendant social imaginaries. Accepting a series of divisions between the private and the public, the state and the market, and the political and the economic limits our view of how these options are produced and reproduced. Achieving a more holistic view of the relationship between cybersecurity practices and political order requires 'deepening' our approach to cybersecurity. It is to this task that we now turn.

3. Security for Whom? Deepening Cybersecurity Studies

Often confused with a 'levels-of-analysis' problem, in which identifying the object of security as either the individual, state, or international system is the central focus, deepening security studies requires embedding the study of security within a more fundamental political theory, from which concerns about 'security' and its operation are derived (Booth, 2007, p. 157). In Booth's (2007, p. 155) terms, 'Deepening, therefore, means understanding security as an epiphenomenon, and so accepting the task of drilling down to explore its origins in the most basic question of political theory'. Drilling down in this context requires that we examine the fundamental assumptions about politics as they exist in the literature on PPPs in cybersecurity and critical infrastructure protection. Three conceptual divisions structure this literature and its subsequent analysis of cybersecurity: (1) the distinction between the public and private and subsequently, (2) between states and markets; (3) the division between public political power and private economic power generated by the separation of the political and the economic in liberal capitalist societies.

First, and most obviously, the literature on PPPs and critical infrastructure protection and cybersecurity accepts, as its analytical starting point, the division between the public and the private in liberal societies. Viewing PPPs as requisite to grapple with complex governance challenges has been described as a 'truism' (Brinkerhoff & Brinkerhoff, 2011, p. 2). Like most truisms, however, it is revealing for the truth-conditions it contains. For the most part the nature of this divide, its historical constitution, and the role that it plays in structuring an historically specific form of political or-

der are not considered.[1] This is not to suggest that the shifting divides between greater public or greater private involvement in the management of critical infrastructure and information technologies is ignored. Privatization of telecommunications and critical infrastructure protection often forms the background to analysis of the present (e.g. Carr, 2016; Dunn Cavelty, 2013). This offers an important insight, one ignored in the most straightforward problem solving approaches. Nevertheless, these potted histories trace vacillations in the scope of public or private governance, not the constitution of these divisions as they are embedded within liberal order as such. Taking the existing division between the public and the private as given, much of the cybersecurity literature treats the public-private divide in the register of problem-solving theory, in Cox's (1981, p. 129) sense: it takes the world as it is and seeks to make it work as smoothly as possible. This allows for a fine-grained analysis of specific problems, as this literature has demonstrated, but at the cost of a more holistic consideration of how cybersecurity policies relate to, and help (re)produce, forms of political order writ large.

In conceptualizing cybersecurity and critical infrastructure protection as a public good the analytical acceptance of the division between the public and the private is already operative. This becomes apparent when we consider how the state is viewed in these frameworks. Analyses of PPPs, particularly those derived from a rational choice perspective, often treat the state as a unitary actor (Christensen & Petersen, 2017; Dunn Cavelty & Suter, 2009, p. 181; cf. Givens & Busch, 2013). Seemingly innocuous, conceptualizing the state as a unitary actor carries with it a series of analytical implications. First, the state is distinguished from other actors in, for example, American society; it is one actor among a field of actors, each with their own aims and purposes.[2] The state and other actors in civil society thereby appear to be externally related to each other; as we shall see, this understanding of the state can only partially grasp the relationship between states and markets. Second, suggesting that there are clearly defined boundaries between state and society implies that the interests of the state are derived from its position as a state as such, rather than from its embeddedness within a society whose social forces shapes it policies.

This view of state and society makes it difficult to understand the purposes of cybersecurity PPPs. Treating the state as distinct from society lends itself to functionalist treatments. Functionalism portrays the aims of state policy as pre-given by its social function; the purpose of the state is to provide the conditions for the reproduction of social order. In the literature on PPPs the state is assumed to play this functional role in social organization in that its purpose is to provide public goods. That is, the role of the state is the generic provision of public goods, to the benefit of society as a whole (Dunn Cavelty, 2014; cf. Carnoy, 1984, pp. 39–40; Olson, 1971, pp. 98–102). Whereas other concepts of the state, such as instrumental or institutional approaches, view state policy as the product of struggles between competing interest groups, in functionalist approaches the security aims of the state are assumed *a priori*. Christensen and Petersen (2017, p. 1437), argue that 'Since its formation, the nation-state has been considered responsible for the provision of national security: the protection of national borders and the maintenance of internal order'. Similarly, Carr (2016, p. 62), focuses on the effectiveness and limits of PPPs in providing national security as such. From this starting point, one can outline better or worse ways for the state to achieve its generic aims of cybersecurity, but the substantive social content of this endpoint is less clear.

This is a thin understanding of cybersecurity, in which a generic goal—national security—is emptied of substantive content: what kind of internal order is sought? To whose benefit, or cost, within that society? Answering these questions entails a substantive analysis of the form and content of political order that are being secured. As Michael C. Williams notes, the separation of the public from the private is central to the modernist project of liberal societies (2011). It sets out both the publicly contestable terrain of politics and the private terrain in which decisions can be taken without the input of the state or the wider community. The institutional division between public and private within liberal order is designed to preserve a private sphere of liberty and to prevent violence over the most contested political, moral, and religious values by removing them from public contestation. A functionalist role for the state, in which it provides security in as 'thin' a manner as possible, its neutrality allowing for political pluralism, is part of the conscious project of liberalism. In these terms, state functions can be judged as more or less effective, but only because the purpose of the state has been set.

The divide between the public and the private sets out the scope of accountability in liberal societies, determining which issues and actors may be held accountable and to whom. Cybersecurity PPPs, which blur the lines between the public and the private, are problematic precisely because they appear to undermine the neutrality of the state in the provision of security as a public good. PPPs do not, then, merely solve problems of efficient governance. While the state is nominally considered to be accountable to the public, PPPs represent an encroachment of private unaccountability into the public sphere. Understood in these terms, questions around accountability in PPPs touch upon the heart of liberal political order itself.

[1] Forrer, Kee, Newcomer and Boyer (2010, p. 475) suggest that PPPs date back to the Roman Empire. Similarly, Wettenhall (2003, as cited in Carr, 2016, pp. 48–49), has asserted that PPPs date back to biblical times, and, at the very least, to the era of British privateers fighting against the Spanish in the late 16th century. These historical claims are anachronistic, and obscure questions around the role of PPPs in contemporary political ordering.

[2] This view is not uniform—Eichensehr (2017) treats state managers as possessing their own set of interests, akin to Weberian state theory.

4. Cybersecurity, States and Markets, and Property Rights

If the division between the public and the private, and the subsequent appearance of the state as autonomous from civil society and the market, is an ongoing historical product, it is important to understand how this division is produced and maintained. Maintaining that the state itself, as an actor, reproduces this separation assumes what needs to be explained. To avoid hypostatizing the state, and the public-private divide that liberal states actively constitute, requires engaging concepts of the state that can grasp the historically concrete process whereby state policy is shaped by domestic interest groups. This allows us to study the particularity of different states and how they are formed, rather than treating the state as an entity with naturally given functions.

States are not naturally liberal, of course, but require that the social forces that dominate the state are themselves liberal and shape the state to perform this role, as opposed to potential alternative roles. A range of work in security studies and International Relations, from a variety of perspectives, has stressed the central importance of domestic social forces in constituting the national security interests of states (Homolar, 2010; Moravcsik, 1997, p. 518, *passim*; Teschke, 2003). In contrast to the public goods approach, the state in this work is viewed as an institution that mediates between different social forces within society (Jessop, 2008). State form is not neutral; instead, the form of the state shapes political outcomes, favouring the interests of some actors over others. Rather than merely occupying a sphere denoted as 'public', state power, operationalized by different groups in civil society, constitutes this division in the first place. Liberal states are liberal because liberals make them this way.

Understood in these terms, the idea that the state provides neutral public goods, or that states and firms or markets can be considered as separate without difficulty, becomes tricky. Viewing the state as an institution draws attention to the various interest groups that occupy the state apparatuses. Analytically, political struggles that focus on controlling the apparatus of the state to realize the distinct aims of different interest groups are brought into relief, with the distinct political strategies the form of the state enables clarified. Furthermore, viewing the state as an institution highlights how the state and market are not opposed to each other. Instead, liberal state institutions are used to create the conditions for the market to operate. A range of tasks, such as protecting and enforcing property rights, providing basic research and development for technological innovation, and correcting market-failures when they arise, as in the provision of cybersecurity, are undertaken because specific interest groups that control the state apparatus view these policies as valuable, necessary or desirable. To give one example, there was a clear distinction between the view of state intervention into the field of cybersecurity provision between the Bush and Obama administrations. The Bush administration viewed public intervention into private markets as inevitably disruptive and inefficient; by contrast, the Obama administration, with its different political constituency and worldview, supported a strong role for the state in organizing critical infrastructure protection and cybersecurity. Similarly, while the private sector is often treated in uniform terms in the literature, there are divisions and distinctions between them, as illustrated in the Net Neutrality debates that often pitted telecommunications companies against software providers. Which set of policies the state pursues is shaped by which of these interest groups can use state power to enact its political strategies.

How cybersecurity PPPs seek to maintain liberal political order, and where along the spectrum of possible divisions of responsibility between public and private cybersecurity policy ultimately lies, is determined by the shifting control of the state by domestic interests. Liberals fearful of the growth of unaccountable power may draw this line differently than those focused on economic growth powered by unfettered markets. For our purposes, the central point is that, while cybersecurity PPPs blur the public-private distinction at the level of security provision, they seek to maintain this in the wider political order. They represent one political strategy to solve the problem of cybersecurity, shaped by the liberal form of the state and liberal social forces.[3] In concrete terms, PPPs aim to reproduce existing liberal political order by securing central institutional features of liberal capitalist societies, such as the protection intellectual property rights (IPRs). William Lynn III (2010), echoing United States government policy, highlights intellectual property theft as the most significant cybersecurity threat

> Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term….As military strength ultimately depends on economic vitality, sustained intellectual property losses could erode both the United States' military effectiveness and its competitiveness in the global economy.

The protection of IPRs is linked here to the provision of national security, but of a specific kind, in which the public sphere of the state is differentiated from the private sphere of the market via the political institution of property. State-coordinated programs of information sharing about threats and intrusions aim to combat threats to the integrity of property rights. PPPs involve the cooperation of the public and private sectors, or the state and the market, but this blurs the separation of these spheres only at the issue specific level of security provi-

[3] Comparison to non-liberal states makes this clear—non-liberal states do not face the same set of contradictions generated by PPPs in the United States or the United Kingdom (Carr, 2016, p. 62).

sion. Viewed holistically, the protection of IPRs through PPPs operates to secure these divides in the wider social formation.

Thus, while critical infrastructure protection once referred to publicly-owned and operated infrastructures, such as power plants or waterworks, it increasingly refers to private infrastructures (Aradau, 2010, p. 507). Dunn Cavelty has noted that (2014, p. 707) cybersecurity and critical infrastructure protection secures a wider political economy that distributes economic benefits unequally: 'It is not a given, then, that cyber-security is truly a public good. Quite the opposite: the type of security that emerges mainly benefits a few and already powerful entities and has no, or even negative effects for the rest'. The content of security—what cybersecurity and critical infrastructure protection is for—is the reproduction of a specific liberal political economy.

In the United States, for example, cybersecurity and critical infrastructure protection directly benefits the material interests of the large firms that participate in, for example, the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council (CIPAC) (United States Department of Homeland Security, 2017). The levels of wealth found among the private sector partners of cybersecurity are substantial: Google's Sergy Brin and Larry Page are worth approximately $23 billion each (Dyer-Witherford, 2015), while Bill Gates net-worth is some $90 billion dollars (Kroll & Dolan, 2017). Dyer-Witherford (2015, pp. 141–142) draws attention to the larger structural impact of cybersecurity policy when he highlights the place of ICTs in contemporary capitalist order, arguing that 'this is not the most important measure of the importance of cybernetics to capital…The real significance of ICT capital is what it has done for capital in general'. The share of national income going to labour has declined in tandem with the diffusion of information technologies throughout the American economy. ICTs have enabled increased levels of automation, the downsizing and outsourcing of manufacturing industry, and the creation of a vast surplus of unemployed and underemployed workers in the United States economy, all undermining the bargaining power of unions (Kristal, 2013; Rotman, 2014). Job market insecurity and precarity characterize this technologically underpinned settlement. Cybersecurity and critical infrastructure protection policies aim to reproduce the process of 'class-biased technological change' (Kristal, 2013), designed to protect intellectual property and to enable market-led technological innovation. The provision of this public good secures and reproduces the unequal distribution of income in American society based upon property ownership. That cybersecurity is a public good does not mean its benefits are equally distributed; this is not what liberal cybersecurity is for.

5. Cybersecurity and the Privatization of Political Power

Securing IPRs facilitates the reproduction of contemporary high technology capitalism, with its attendant consequences for the unequal distribution of wealth. The reproduction of the division between the public and the private is equally important for determining how different forms of social power are, or are not, made accountable to the public. Public and private power within liberal societies substantively maps onto the institutional separation between the political and the economic that characterizes capitalism. As Wood (1981) notes, the interlinked division between the public, private, political, and economic, effectively privatized what had previously been constituted as public political power. Pre-capitalist social formations united political power and economic appropriation—the right to appropriate the output of others depended on one's political position in society. Under capitalism, by contrast, the right to appropriate the wealth of others is divorced from political roles; when politicians use their office for private economic gain this is identified as corruption and punished. Economic actors have the right to goods produced by virtue of private property ownership. Capitalism privatizes a form of social power previously considered 'political', and thereby subject to norms of accountability.

This takes two forms. First, it confers onto capitalists the right to direct and organize the labour process. Private property rights, underwritten by the judicial and coercive apparatus of the state and reproduced, in the context of cybersecurity and critical infrastructure protection, through the cooperation of PPPs, give firms the right, and ability, to direct the activity of others. Capitalists exercise significant power in shaping the everyday lives of their employees—they decide how products (including software) will be produced, allocate resources including labour, set work targets, organize the process of production, and oversee the production process in general.

Second, and most significantly for our purposes, securing private property rights via cybersecurity PPPs secures the right of private actors to direct the design and development of new hardware and software infrastructures as they see fit. This enables the continuation of market-led technological innovation, a significant source of social power. Technological infrastructures are the materialization of the norms and values of their designers. In Andrew Feenberg's (1991, p. 14) terms, 'it stands at the intersection between ideology and technique where the two come together to control human beings and resources'. Conferring this right on private actors allows them to shape political orders in the long-term, as the path dependency of technology structures social life. For, in this infrastructure, the United States government is not merely talking about the security of its economy, its military and defence, or its critical public infrastructure. Increasingly, what is being secured is the way of life of Americans themselves in their full digital articulation.

When the privatization of political power is considered in these terms, the concerns over the role of the private sector in cybersecurity and critical infrastructure protection via PPPs is complicated. As clear lines of ac-

countability are demanded of the private sector participation in public sector functions, it is possible to press this further to ask how and why boundaries around private sector accountability for the development of infrastructures, within the scope of their authority in the market, are set and maintained.

6. Conclusion

Taking the full measure of cybersecurity and critical infrastructure protection policies requires analysis of their place in reproducing specific forms of political order. Reorienting our conceptual lenses to consider the deeper political theory within which security thinking is rooted is one small step in this direction. A range of theoretical positions are compatible with this aim. While the approach favoured here is rooted in Critical Theory and historical materialism, this does not exhaust a programme of 'deepening' cybersecurity studies. Asking for a deeper analysis is merely a request to clarify the foundational assumptions that shape our inquiries. Cybersecurity studies informed by a plurality of theoretical frameworks can only be a positive development.

Nevertheless, the analysis presented above favours Critical Theory as the most fruitful way to pursue this project. Space prevents a full discussion its epistemological, ontological, and methodological dimensions; three central claims will suffice. First, Critical Theory is interdisciplinary in nature. As we know, cybersecurity is a complex and multifaceted issue. While no single study could possibly capture this complexity, a research programme attending to the breadth of its varied aspects—the political economy of cybersecurity, its normative suppositions and impact, the discursive representations that inform and support these—can provide a more comprehensive reconstruction of the challenge of cybersecurity.

Second, Critical Theory (tempered by historical materialism) is historically sensitive. Recognizing the public-private divide as an historically produced outcome of liberal orders opens our conceptual and political horizons. In turn, it emphasizes how structural pressures, such as those imposed by markets, condition forms of power available to various social forces in specific contexts. To this extent, the analysis above cannot be easily generalized to non-liberal societies. Indeed, the use of cybersecurity PPPs to meet broader political aims may be pursued quite differently in different contexts. The normative commitment to PPPs in the United States, with the ideological weight around property and liberty that underpins them, may differ substantially from a merely instrumental use in non-liberal states. Stressing an historical understanding allows for nuanced treatment of how various social forces—in liberal and illiberal states—shape the plurality of approaches to cybersecurity we witness in world politics.

Finally, Critical Theory draws attention to the question that implicitly structures the concerns over private sector accountability in the literature: democracy. Fear of unaccountable power is central to existing criticism of cybersecurity PPPs. As a normative aim, a Critical Theory approach to cybersecurity is committed to the democratization science and technology as a vehicle for greater social and political equality. To give just one example, greater democratic participation in defining how cybersecurity risks are determined, proceeding along the lines of similar consultative exercises around food standards in the United Kingdom (Jasanoff, 2003, pp. 237–238), could provide a different account of how cybersecurity risks are defined and to whose benefit. Answering the question of what cybersecurity is both an analytical task and a practical question in need of democratically derived answers.

Acknowledgments

I would like to thank the anonymous reviewers for their helpful comments on the manuscript and Tim Stevens for his editorial guidance, particularly during the initial formulation of this article.

Conflict of Interests

The author declares no conflict of interests.

References

Abrahamsen, R., & Williams, M. C. (2010). *Security beyond the state: Private security in international politics*. Cambridge: Cambridge University Press.

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491–515.

Assaf, D. (2008). Models of critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *1*, 6–14.

Avant, D. (2005). *The market for force: The consequences of privatizing security*. Cambridge: Cambridge University Press.

Booth, K. (2007). *Theory of world security*. Cambridge: Cambridge University Press.

Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public-private partnerships: Perspectives on purposes, publicness, and good governance. *Public Administration and Development*, *32*, 2–14.

Carnoy, M. (1984). *The state and political theory*. Princeton, NJ: Princeton University Press.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Christensen, K. K., & Petersen, K. L. (2017). Public-private partnerships on cybersecurity: A practice of loyalty. *International Affairs*, *93*(6), 1435–1452.

Cox, R. W. (1981). Social forces, states and world orders: Beyond international relations theory. *Millennium: Journal of International Studies*, *10*(2), 126–155.

Dunn Cavelty, M. (2013). From cyber-bombs to politi-

cal fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715.

Dunn Cavelty, M., & Suter, M. (2009). 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.

Dyer-Witherford, N. (2015). *Cyber-proletariat: Global labour in the digital vortex*. London: Pluto Press.

Eichensehr, K. E. (2017). Public-private cybersecurity. *Texas Law Review*, *95*, 467–538.

Feenberg, A. (1991). *Critical theory of technology*. Oxford: Oxford University Press.

Forrer, J., Kee, J. E., Newcomer, K. E., & Boyer, E. (2010). Public-private partnerships and the public accountability question. *Public Administration Review*, *70*(3), 475–484.

Givens, A. D., & Busch, N. E. (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *6*(1), 39–50.

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, *71*(3), 455–460.

Homolar, A. (2010). The political economy of national security. *Review of International Political Economy*, *17*(2), 410–423.

Jasanoff, S. (2003). Technologies of humility: Citizen participation in governing science. *Minerva*, *41*(3), 223–244.

Jessop, B. (2008). *State power*. Cambridge: Polity.

Kristal, T. (2013). The capitalist machine: Computerization, workers' power, and the decline of labor's share within U.S. industries. *American Sociological Review*, *78*(3), 361–389.

Kroll, L., & Dolan, K. A. (2017). Forbes 2017 billionaires list: Meet the richest people on the planet. *Forbes*. Retrieved from https://www.forbes.com/sites/sites/sites/kerryadolan/2017/03/20/forbes-2017-billionaires-list-meet-the-richest-people-on-the-planet/#6bee40c862ff

Linder, S. H. (1999). Coming to terms with the public-private partnership. *American Behavioral Scientist*, *43*(1), 35–51.

Lynn III, W. J. (2010). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Moravcsik, A. (1997). Taking preferences seriously: A liberal theory of international politics. *International Organization*, *51*(4), 513–553.

Olson, M. (1971). *The logic of collective action*. Cambridge, MA: Harvard University Press.

Pew Research Center. (2017). *Internet use over time*. Retrieved from http://www.pewinternet.org/fact-sheet/internet-broadband

Rotman, D. (2014). Technology and inequality: The disparity between the rich and everyone else is larger than ever in the United States and increasing in much of Europe. Why? *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/531726/technology-and-inequality

Shore, M., Du, Y., & Zeadally, S. (2011). A public-private partnership model for national cybersecurity. *Policy & Internet*, *3*(2), 1–23.

Singer, P., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.

Stevens, T., & Betz, D. (2013). Analogical reasoning and cybersecurity. *Security Dialogue*, *44*(2), 147–164.

Teschke, B. (2003). *The myth of 1648*. London: Verso.

United States Department of Homeland Security. (2017). *Information technology sector: Council charters and members*. Retrieved from https://www.dhs.gov/information-technology-sector-council-charters-and-membership

United States National Science and Technology Council. (2011). *Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

Williams, M. C. (2011). The public, the private, and the evolution of security studies. *Security Dialogue*, *41*(6), 623–630.

Wood, E. M. (1981). The separation of the political and the economic in capitalism. *New Left Review*, *I/127*, 66–95.

About the Author

Daniel R. McCarthy is Lecturer in International Relations at the University of Melbourne. He is author of *Power, Information Technology and International Relations Theory* (Palgrave 2015) and editor of *Technology and World Politics: An Introduction* (Routledge 2017). His work has appeared in *Review of International Studies*, *Millennium*, and the *European Journal of International Relations*.