Politics and Governance
Open Access Journal | ISSN: 2183-2463
Volume 6, Issue 2 (2018)

Global Cybersecurity: New Directions in Theory and Methods

Editor
Tim Stevens

COGITATIO

Politics and Governance, 2018, Volume 6, Issue 2
Global Cybersecurity: New Directions in Theory and Methods

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070-129 Lisbon
Portugal

Academic Editor
Tim Stevens, King's College London, UK

Available online at: www.cogitatiopress.com/politicsandgovernance

Table of Contents

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 1–4
DOI: 10.17645/pag.v6i2.1569

Editorial

Global Cybersecurity: New Directions in Theory and Methods

Tim Stevens

Department of War Studies, King's College London, London, WC2R 2LS, UK; E-Mail: tim.stevens@kcl.ac.uk

Submitted: 8 May 2018 | Published: 11 June 2018

Abstract
This thematic issue advocates a range of novel theoretical and methodological directions applicable to cybersecurity studies. Drawing on critical International Relations theory, Science and Technology Studies, participant observation, quantitative political science, and other social science methods and theory, the contributors advance modes of invigorating the exploration of cybersecurity as an assemblage of sociotechnical practices. In so doing, this issue seeks to enhance understanding of the politics and strategies of cybersecurity, one of the most complex and diverse technical and political challenges of our contemporary world.

Keywords
assemblage; critical infrastructures; critical theory; cybersecurity; ethnography; power; science and technology studies; security; security politics; sociotechnical systems

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

1. Introduction

This thematic issue suggests novel theoretical and methodological approaches to the analysis of global cybersecurity. From obscure technical origins in computer science and information security, cybersecurity has emerged as a major political consideration for states, multilateral organizations, firms and civil society in the early twenty-first century. The briefest survey of news headlines will reveal diverse cybersecurity issues affecting contemporary societies, from low-level Internet-enabled criminality to military cyber operations and strategic interventions via computer networks in the domestic affairs of world powers. These are functions of economic and political motives but are enabled and exacerbated by our increased reliance on and imbrication with transnational assemblages of information technologies. To date, the struggle to regulate and govern this complex landscape is mirrored by a lack of diversity in the theory and methods used to comprehend this novel environment and to understand political responses to its problems. This thematic issue hopes to offer ideas for redressing this imbalance.

2. Cybersecurity Studies: The State of the Field

Cybersecurity studies are affected by the conditions of the historical and discursive emergence of the object of its enquiry. The term 'cybersecurity' can be traced back to at least the late 1980s and its conceptual antecedents much further, but its present usage is relatively recent. Even practitioners charged with technical aspects of cybersecurity did not self-identify as 'cybersecurity' professionals until the 2000s (Denning & Frailey, 2011), when national policy documents also began to use the term. The subsequent rapidity of cybersecurity's rise as concept and practice, and its convergences with other forms of security, has hindered definitional consensus, such that 'no one can agree precisely what cybersecurity means, or requires' (Bambauer, 2012, p. 587). This is regrettable to some but also offers opportunities for productive engagements with cybersecurity that interrogate and contest an unsettled field of policy and practice.

We can offer a broad definition of cybersecurity as 'a means not only of protecting and defending society and its essential information infrastructures but also a way of prosecuting national and international poli-

cies through information-technological means' (Stevens, 2016, p. 11). This highlights cybersecurity's ontological and processual characteristics and its contingent relations with information technologies, particularly the Internet. It recognizes that cybersecurity is not merely defensive, as shown through its attempts to generate political effect through active transnational intervention and engagement. This implies that various theories and methods might be appropriate for exploring cybersecurity but these have yet to attract the attention they perhaps deserve. We have not progressed far beyond the situation noted a decade ago, that cybersecurity studies are oriented to solving policy problems at the expense of theory-building and methodological innovation (Eriksson & Giacomello, 2007, p. 2). Cybersecurity is worthy of such academic work—and there are many excellent such contributions—but few cybersecurity scholars have yet to transcend the 'hectic empiricism' and 'consequent theoretical sterility' afflicting security studies in general (Buzan, 2000, p. 3).

Exceptions to this include an established literature on the securitization of cybersecurity and a growing interest in Science and Technology Studies (STS), each channeling intellectual currents in security studies and International Relations (IR). Securitization studies record the discursive construction of cyber threats and identify tensions between political claims and the objective conditions to which they refer (Conway, 2008; Dunn Cavelty, 2008, 2013; Hansen & Nissenbaum, 2009; Lawson, 2013). This work complements other critical engagements with cybersecurity language, particularly the role of analogies and metaphors in knowledge construction (Betz & Stevens, 2013; Lawson, 2012). STS-inflected studies examine non-discursive facets of cybersecurity, generating sociotechnical analyses of the co-construction of material and immaterial actors in cybersecurity assemblages (Aradau, 2010; Balzacq & Dunn Cavelty, 2016; Stevens, 2016). We should also recognize rich deployments of classical IR theory (Kello, 2017) and theories of risk and governmentality (Barnard-Wills & Ashenden, 2012; Deibert & Rohozinski, 2010; Stevens, 2015). As the contributions to this thematic issue signal, there is further scope for expanding how we understand cybersecurity's many conceptual and empirical manifestations.

3. New Directions in Theory and Methods

McCarthy (2018) addresses one of the core problematics of the field, asking whose interests cybersecurity serves. The article explores public-private partnerships (PPPs), a common form of organization seeking to balance private critical infrastructure ownership with the state's responsibility to provide cybersecurity as a public good. Extant discussions of PPPs assume binary distinctions—public/private, state/market—that obscure power relations. McCarthy's PPPs are reproductive of a liberal order that constructs these binaries in the interests of the few, thereby undercutting the narrative of cybersecurity as a public good. Rather, they should be understood as a means of entrenching the privatization of political power. This illuminates the roles of the private sector in infrastructure design and ownership, its warping effects on cybersecurity provision and political decision-making, and the utility of critical materialism to examining the proper role of cybersecurity in democratic contexts.

Collier (2018) and Dunn Cavelty (2018) illustrate the relevance of STS concepts and methods to cybersecurity. Like McCarthy (2018), Collier (2018) describes the porous nature of the boundaries between conventional binaries like local/global and employs assemblage thinking to sketch the multiplicity of actors and interests competing and combining in cybersecurity. Importantly, this article demonstrates how these assemblages shift over time, creating hybrid and contingent structures that generate new forms of action and actors. Dunn Cavelty (2018) uses bibliometric data to discern two main clusters in the cybersecurity literature: a technical focus on cybersecurity as a means to fix 'broken' objects and a social-scientific perspective that diagnoses the perceived misuse of technological artefacts as a problem to be solved by external intervention. Dunn Cavelty submits that actor-network theory can bridge this gap by describing the relations between technical and sociopolitical objects. Tracing these linkages exposes how cybersecurity knowledge is formed in practice.

Articles by Shires (2018) and Coles-Kemp, Ashenden and O'Hara (2018) articulate a commitment to investigate sociological sites of cybersecurity. Through participant observation of cybersecurity conferences, Shires (2018) introduces the notion of 'ritual' space-time performativity of expertise. Systematized rituals of organization and presentation reproduce commercial logics while creating an illusion of neutral cybersecurity knowledge, a double move Shires identifies elsewhere in cybersecurity. This explains key features of cybersecurity actors' self-identities and disciplinary epistemology, while establishing the potential of ethnography for excavating meaning from situated cybersecurity practices. Similarly, Coles-Kemp et al. (2018) undertook community research to show how institutional decisions on cybersecurity technology design obscure digital service-users' needs and desires. This establishes that cybersecurity measures must develop community trust by design, rather than increasing citizen's insecurity and thereby failing to achieve collective security gains. This is a significant corrective to conventional readings of cybersecurity as a 'top-down' venture by commercial and political elites.

Valeriano and Maness (2018) and Gomez and Villar (2018) bring quantitative methods to bear on established cybersecurity problems. Valeriano and Maness (2018) report on a long-term project to gather data on international cyber conflict, through which to test hypotheses of state actions and intentions. Contrary to received wisdom, for example, they find that states are restrained in their use of offensive cyber capabilities, which explains the historical dearth of escalatory incidents. The authors

point towards the fertile use of data-sets in cybersecurity research and recommend avenues for establishing data integrity and reliability. Gomez and Villar (2018) account for feelings of 'dread' that accompany the types of assumptions about cyber threats disputed by Valeriano and Maness (2018). From experimental data they find that imperfect information and lack of experience elevate actors' levels of uncertainty and likelihood of developing fearful reactions to cyber threats. The authors propose several ways in which embracing 'ecological rationality' can improve individual and collective decision-making.

The final article (Whyte, 2018) raises a number of epistemological challenges for cybersecurity research as seen through the lens of the philosophy of (social) scientific enquiry. Many of these might be ameliorated by adopting a cross-community 'monism' that prioritizes consistency of terms of reference, yet encourages diversity within a discrete research program. Whyte outlines a capacity-building agenda to improve community cooperation and research standards and his article constitutes a progressive call for solidarity within cybersecurity studies.

4. Conclusion

Each of the articles in this issue offers something provocative and innovative for future cybersecurity research. Together, they offer new or revised methods of data collection and theoretical frameworks that assist in interrogating cybersecurity as an assemblage of sociotechnical practices and politics. We look forward to scholars engaging with this collection and to working with us to deliver on the promises of its individual and collective proposals.

Acknowledgements

The Academic Editor and authors extend their sincere thanks to the reviewers for their comments and suggestions, and to Rodrigo Gomes Quintas da Silva and the *Politics and Governance* team for bringing this issue to publication.

Conflict of Interests

The author declares no conflict of interests.

References

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491–514.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–198.

Bambauer, D. E. (2012). Conundrum. *Minnesota Law Review*, *96*(2), 584–674.

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space & Culture*, *15*(2), 110–123.

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

Buzan, B. (2000). 'Change and insecurity' reconsidered. In S. Croft & T. Terriff (Eds.), *Critical reflections on security and change* (pp. 1–17). Abingdon: Routledge.

Coles-Kemp, L., Ashenden, D., & O'Hara, K. (2018). Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance*, *6*(2), 41–48.

Collier, J. (2018). Cybersecurity assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, *6*(2), 13–21.

Conway, M. (2008). Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *Securing 'the homeland': Critical infrastructure, risk and (in)security* (pp. 109–129). Abingdon: Routledge.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32.

Denning, P. J., & Frailey, D. J. (2011). Who are we—now? *Communications of the ACM*, *54*(6), 25–27.

Dunn Cavelty, M. (2008). *Cyber-security and threat politics: U.S. efforts to secure the information age*. Abingdon: Routledge.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Dunn Cavelty, M. (2018). Cybersecurity research meets Science and Technology Studies. *Politics and Governance*, *6*(2), 22–30.

Eriksson, J., & Giacomello, G. (2007). Introduction: Closing the gap between International Relations theory and studies of digital-age security. In J. Eriksson & G. Giacomello (Eds.), *International relations and security in the digital age* (pp. 1–28). Abingdon: Routledge.

Gomez, M. A. N., & Villar, E. B. J. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*, *6*(2), 61–72.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.

Lawson, S. (2012). Putting the 'war' in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, *17*(7). doi:10.5210/fm.v17i7.3848

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

McCarthy, D. R. (2018). Privatising political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12.

Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*, *6*(2), 31–40.

Stevens, T. (2015). Security and surveillance in virtual worlds: Who is watching the warlocks and why? *International Political Sociology*, *9*(3), 230–247.

Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge: Cambridge University Press.

Valeriano, B., & Maness, R. (2018). How we stopped worrying about cyber doom and started collecting data. *Politics and Governance*, *6*(2), 49–60.

Whyte, C. (2018). Crossing the digital divide: Monism, dualism and the reason collective action is critical for cyber theory production. *Politics & Governance*, *6*(2), 73–82.

About the Author

Tim Stevens is Lecturer in Global Security at King's College London. His research addresses cybersecurity politics, cyber strategy, technology and world politics, and time and temporality in International Relations. He is the author of *Cyber Security and the Politics of Time* (Cambridge University Press, 2016) and co-author of *Cyberspace and the State* (Routledge, 2011). His work has appeared in journals including *Contemporary Security Policy*, *International Political Sociology*, *International Politics*, *Millennium: Journal of International Studies and Security Dialogue*.

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*.

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 13–21
DOI: 10.17645/pag.v6i2.1324

Article

Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision

Jamie Collier [1,2]

[1] Department of Politics and International Relations, University of Oxford, Oxford, OX1 3UQ, UK;
E-Mail: jamie.collier@cybersecurity.ox.ac.uk
[2] Centre for Doctoral Training in Cyber Security, University of Oxford, Oxford, OX1 3PR, UK

Submitted: 23 December 2017 | Accepted: 28 February 2018 | Published: 11 June 2018

Abstract
In the context of globalisation and privatisation, an emerging body of literature has applied the concept of an 'assemblage' to international relations and security studies. This article will argue that an assemblage framework provides the best means for understanding the complex configuration of cyber security actors, given that contemporary cyber security practices do not conform to the traditional public-private and global-local distinctions used in security studies and International Relations literature. With the configuration of cyber security actors, and the relationships between them in constant flux, an assemblage framework provides a means for understanding the contested, dynamic and diachronic nature of contemporary cyber security provision. While the concept of security assemblages is favoured in this article, the process and context in which the term has traditionally been used cannot be blindly imposed on the issue of cyber security. This article will therefore propose a different model of how cyber security assemblages have developed and explain the implications this has on contemporary security dynamics.

Keywords
assemblages; cyber security; private security; state power

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

Cyber security is provided by a complex configuration of actors and institutions (Choucri, 2012). Non-state and non-traditional actors sit at the forefront of contemporary cyber security challenges: multinational corporations, hacktivist groups, intergovernmental organisations, and volunteer networks all provide (or threaten) security in some important way. Whether it be the historically prominent role of private actors in the development and growth of cyber-related industries, or the low barriers to entry, non-traditional actors have developed meaningful capabilities (Nye, 2011, pp. 113–151). As this phenomenon has emerged, the traditional distinctions used to capture international politics are becoming hazy: the lines between what is public and private, between what is global and local, are waning. If the Weberian notion of the state, whereby states possess a monopoly on the legitimate use of force and defence, has ever existed, its application to cyber security is increasingly limited. Cyber security, therefore, requires refreshed thinking.

The proliferation of security actors leads to important questions for international politics. The fragmentation of security provision has meant that states cannot take their traditional standing as the primary security provider in the international system for granted. Government actors may find not only their capabilities, but also their legitimacy as a security actor fundamentally questioned. The flight of power away from state structures has produced what Lucas Kello calls a 'sovereignty gap' where private sector firms and individuals can no longer take their government's ability to protect them for granted as they might have done in the face of other threats (Kello, 2017, pp. 160–162). Cyber security is of-

ten provided by a network of actors. Here, existing International Relations (IR) theories, concepts and paradigms provide useful tools in understanding the emerging models of security provision and their implications for international politics. Current academic literature has already addressed many of the relationships between actors that are central to cyber security provision, including public-private partnerships, (Carr, 2016; Dunn Cavelty, 2015; Dunn Cavelty & Suter, 2009) the role of civilian-led groups (Ottis, 2012; Sheldon & McReynolds, 2015; Suciu, 2015; Toomesaar & Ottis, 2010) and states' use of proxies (Collier, 2017; Maurer, 2015, 2018; Rattray & Healey, 2011; Schmitt & Vihul, 2014).

The diffuse model of security provision observed in many cyber security contexts lends itself naturally to theories and concepts that accommodate actors other than the state. This is not particularly novel or controversial within IR literature. Concepts such as actor-network theory and the military-industrial complex have helped to articulate such a world view where state institutions work alongside other actors (Balzacq & Dunn Cavelty, 2016). These concepts would therefore represent a natural home of sorts within the IR tradition for understanding contemporary cyber security provision.

Yet, the challenges associated with interpreting and understanding cyber security provision go beyond just the proliferation of security actors. The emergence of various cyber security actors has led to significant disruption that requires further consideration. Various actors compete for power and ownership of cyber security issues. First-order questions of what aspects of cyber security are 'public' or 'private' are still being contested and defined (Egloff, 2017). The incentive structures of different security actors often clash rather than converge (Carr, 2016). As state actors further develop, processes of securitisation often follow (Hansen & Nissenbaum, 2009). As defence institutions become increasingly interested in cyber security, the issue becomes further militarised, creating an atmosphere of insecurity and tension in the international system (Dunn Cavelty, 2012).

Further, the implications of such a proliferation of security actors cannot necessarily be captured with uniform theories and trends. In truth, various simultaneous and yet seemingly contradictory trends coexist, often unhappily. States are simultaneously undermining and being undermined by private actors. Private actors may compete against states while working directly with them in separate contexts. For example, whilst Apple has publicly challenged the UK governments stance on encryption and privacy (Hern, 2015), the US technology firm also works alongside the UK intelligence community with the UK signals intelligence agency, Government Communications Headquarters (GCHQ), providing Apple with information about vulnerabilities in their products (Cox, 2016).

Given the above, simply acknowledging the proliferation of security actors is not enough. Studying its implications, however, represents the altogether more interesting question. An emerging body of literature that applies the concept of an 'assemblage' to IR and security studies provides a useful first step. The security assemblage concept is one able to articulate the empirical realities and ongoing challenges of contemporary cyber security challenges. Section two proceeds to define the term and discuss how it relates to cyber security. Section three then develops this concept further by suggesting how the formation of cyber security actors and structures is different to the contexts in which the concept of a security assemblage has typically been deployed. Section four then presents concluding arguments and considers the practical applications of the assemblage term.

2. Cyber Security Assemblages

Refreshed thinking is required to better understand the provision of cyber security and the configuration of cyber security actors. Here, the term cyber security is defined as the security of the environment formed by physical and non-physical components and characterised by the use of computers and other networked devices. Cyber security actors, by definition, provide security in some capacity. Yet this does not mean that all actors strive to achieve a single, unitary concept of security. The prevalence of private actors means that cyber security is often provided by actors who prioritise other commercial objectives over security. Encryption disputes between the US government and technology firms show that different actors have altogether different motivations.

This makes the study of the different cyber security providers, and how they interact with one another essential. The concept of global cyber security assemblages provides a conceptual anchor that provides a means for further understanding these issues. The term provides a more appropriate concept for understanding contemporary cyber security contexts when compared to more traditional frameworks. The security assemblage term refers to new hybrid structures that are often simultaneously public and private, global and local. The use of the term is part of an emerging body of scholarship within IR literature that seeks to empirically assess complex structures where a range of different global and local, public and private security agents, interact, cooperate and compete to produce new institutions, practices and forms of security governance that cannot be captured neatly though the boundaries of nation states (Abrahamsen & Williams, 2011; Williams, 2016).

The assemblage concept therefore moves away from the traditional centre of the nation-state to multi-layered, networked configurations that are able to accommodate a range of entities including (inter)governmental, para-governmental, nongovernmental, and private organisations (Voelkner, 2013). The boundaries of an assemblage can be drawn in alternative ways to the traditional contours of national borders. They can be drawn to examine the provision of security within a territory but can also be used to examine security or

governance contexts that are inherently international. The issue of internet governance, for example, comprises a global assemblage of actors, albeit one dominated by US actors (Carr, 2014). Perhaps the most defining characteristic of the assemblage concept is therefore an accommodation of the forces of globalisation and a scepticism of rigid borders and distinctions. Of course, much of the above relates closely to other terms including actor network theory; indeed, the difference between the terms is one of emphasis, rather than kind (Acuto & Curtis, 2014) with the similarities and differences between the two concepts discussed in greater detail elsewhere (Acuto & Curtis, 2014; Müller & Schurr, 2016).

For the purposes of understanding cyber security provision, it is the notion of assembly and disassembly—where actors relinquish, transfer and develop capacities and functions—that is central to the added value of the assemblage concept. As security functions emerge and are captured by either public or private actors, actors assemble greater capabilities and responsibilities. As private actors increasingly take on strategic, ethical, and foreign-policy alignment issues that were previously outside their purview, they are assembling into more political actors. Conversely, as aspects of cyber security are increasingly regulated and managed by states, other aspects of private actors' capabilities and responsibilities are disassembling. Contemporary cyber security practices are replete with these instances of assembly and disassembly. Assemblage thinking therefore pays attention to the instability of security networks. While cyber security is provided by a vast array of actors, assemblage thinking also highlights the contestation related to the roles and responsibilities of security actors. In light of emerging and shifting actors, the point is not to demonstrate that states are stronger or weaker. Rather, the intention is to examine the complex configuration of actors that maintain contingent and multifaceted relationships with each other (relationships that cannot be captured by static and often state-centric theories). Cyber security is replete with global and local, public and private agents whose relationships are deeply competitive as well as cooperative, conflictual, and at times coordinated. While the concept of a security assemblage has been applied to cyber security in previous literature (Stevens, 2012, 2016, pp. 181–186), the argument for why and how the concept should be used and applied to cyber security remains underdeveloped—an imbalance this article hopes to correct.

These hybrid structures are clearly observed through contemporary examples with the cyber security of critical national infrastructure (CNI) in the UK a case in point. The vast majority of CNI is owned and managed by corporations—itself a broad church that includes a variety of actor types including not-for-profit community owned private limited firms, regional and UK-based firms, multinational firms (National Grid operates in both the US and UK for example, probing traditional global-local distinctions) and state-owned or quasi-state owned firms (the now approved Hinkley Point nuclear plant will be owned and managed by a combination of French-state majority owned EDF energy and Chinese state-owned China General Nuclear Power Corporation) (Ward, Pickard, & Stothard, 2016). As a collective, these corporations cannot neatly be categorised as 'private' given the variety of entities including the presence of both partially and fully state-owned entities. Corporations provide cyber security alongside a range of government departments, including GCHQ and its subsidiary, the National Cyber Security Centre (NCSC); the Cabinet Office, the various government departments that are largely responsible for infrastructure related to their department and related institutions such as the Centre for the Protection of National Infrastructure (Collier, 2016). All of these government entities have their own identities, agendas and motivations—a reality that means that 'the government' is not necessarily a coherent entity at all. Adding to the plethora of actors are various international organisations and multilateral bodies. Various actors work together within this cyber security assemblage, often in unusual ways. With Chinese-based firm Huawei providing communication equipment for CNI organisations, GCHQ employees will routinely monitor, take apart and inspect the equipment supplied (due to security concerns) at a centre that is itself funded by Huawei (Rifkind, 2013; Rosenzweig, 2013).

An assemblage approach also considers the normative agendas behind the traditional categories and distinctions used in IR literature. Pursuing assemblage thinking means paying attention to the relationships between a variety of actors and the forces that impel them to act in the way they do (Lisle, 2013). The process of assemblage formation is not neutral but deeply political. Different actors have clashing views on what aspects of cyber security should be 'public' or 'private' as well as where the boundaries of these distinctions lie. Returning to the UK example, the UK 2016 Cyber Security Strategy declared that market based solutions to cyber security have 'not produced the required pace and scale of change', meaning that 'Government has to lead the way and intervene more directly by bringing its influence and resources to bear' in a move that overtly seeks to increase the government's cyber security purview (HM Government, 2016). On the other hand, governments have also sought to relinquish both their authority and responsibility of cyber security issues within other contexts in order to avoid the backlash of security failings (Carr, 2016). This is also observed in recent US encryption disputes that reflect broader political disagreements about the agency afforded to different actors. Law enforcement organisations' interests in accessing intelligence on devices clash with technology firms who instead seek to protect their customers' data from government access, (albeit while simultaneously selling user data to other businesses and using it themselves for the purposes of targeted advertisements). Various government entities compete with each other for ownership of cyber secu-

rity and the tax revenue that accompanies the issue. Alternative visions of cyber security are proposed within such intra-governmental competition—the issue may be framed through a military, business or criminal prism depending on the government entity that seeks to capture the issue. These tensions are mirrored at the international level where various multilateral organisations compete for relevance on the issue including the North Atlantic Treaty Organization (NATO); the United Nations (UN) through the Group of Governmental Experts on Information Security; The European Union Agency for Network and Information Security (ENISA); the International Telecommunication Union (ITU); etc. It is this notion of contestation that further distinguishes an assemblage approach from other theoretical lenses that merely acknowledge the importance of units other than states or the increasingly blurry lines that exist between different types of actors.

3. The Cyber Security Assemblage Process

The arguments and theoretical developments of previous assemblage literature provides a rich intellectual backdrop in which the concept of a global cyber security assemblage can be developed. Assemblage thinking owes its intellectual roots to Gilles Deleuze and Felix Guattari's book that developed an ontology that includes assemblages as a core entity in light of the development of a number of concepts, including 'open systems, complexity, emerging and non-linear dynamics' in the global system (Deleuze & Guattari, 1987). For Deleuze and Guattari, an assemblage is a number of disparate and heterogeneous elements convoked together into a single discernible formation that displays some form of consistency and regularity while remaining open to transformative change, either through the addition or subtraction of elements, or the reorganisation of the relations between elements (Deleuze & Guattari, 1987). Manuel DeLanda subsequently developed the concept to develop a comprehensive theory of assemblages that challenges existing social analyses—often focused at either the individual or societal level (DeLanda, 2002, 2006, 2010).

Assemblages were subsequently considered in an IR and security studies context. Saskia Sassen has pushed back against the focus of globalisation literature on the withdrawal from the state in areas such as the economy as it often ignores the way states actively participate in setting up new structures. In short, globalisation is not a matter of outside private forcers eroding state power and sovereignty; instead, it is a process entwined with a restructuring of institutions and power relations through practices such as privatisation and regulation. Sassen used the assemblage term to articulate how globalisation has led to a new world order that challenges state-centric ontologies. The assemblage process described by Sassen involves three steps. First, a process of state disassembly occurs with traditional state functions taken up by private actors. This first shift therefore involves the transformation of the national state through the denationalisation or privatisation of national authorities and policy agendas (Sassen, 2008). Second, private actors develop new capacities that allow them to act at a global level. For Sassen, this primarily came through a new normative capacity, where private power is increasingly recognised as legitimate and accepted in the international system (Sassen, 2008). Third, a process of reassembly occurs where new actors and capabilities become part of global assemblages that are embedded in national settings but operate at a global scale (Sassen, 2008; Williams, 2016).

Although state-centric ontologies may no longer be coherent for Sassen in the context of globalisation and privatisation, they do at least represent an appropriate starting point in her analysis. States certainly played a decisive role in the formation of cyberspace. Yet, it is not the case that a process of state disassembly has occurred, where many cyber security functions that were once the purview of states have now been taken up by private actors. Instead, many cyber security functions have emerged over time as the internet and networked technologies have become increasingly integral to society. From a theoretical perspective, this means that while security assemblages provide an ideal lens for examining cyber security issues, Sassen's three-part assemblage process does not represent an accurate representation of the development of cyber security actors. Cyber security provision represents a curious counter-example to the ongoing trend of states outsourcing security and military functions to the private sector. In these other areas of security, traditional state functions are increasingly outsourced to contractors (McFate, 2014; Mumford, 2013; Singer, 2008). In a cyber security context, by contrast, states have, if anything, expanded their security role and acquired new functions—often challenging private sector governance in the process. It must therefore be acknowledged that the formation of cyber security assemblages contain their own idiosyncrasies.

Rather than Sassen's three-shift account, a five-shift process of assemblage formation is a more appropriate representation of the formation of assemblages in a cyber security context and is outlined below. Note, rather than to provide a comprehensive history of events, the objective here is to explain how various actors have developed and come together in the context of cyber security. The five shifts outlined below are therefore overlapping and not necessarily perfectly linear. Moreover, with 'cyber' such a broad catch-all term that in fact comprises a number of separate processes (including encryption disputes, disinformation campaigns, and internet governance), clearly not all issues that sit within the concept have developed in the same way (Shires & Smeets, 2017). The following five shifts therefore represent a broad generalisation, rather than a precise account of specific cyber security issues.

3.1. One: Development of Underpinning Technologies

The starting point for contemporary cyber security challenges does not begin with a coherent Weberian state model. To understand the starting point of contemporary cyber security challenges, it is necessary to understand the development of the two key technologies that underpin it: computers and computer networks.

It is difficult to confidently declare when the first computer was built, given the range of classifications. The reality is that a gradual process of incremental technological developments eventually led to the computers used today. For example, the first programmable computer was created by German Konrad Zuse in his parents' living room between 1936 and 1938; the Turing Machine, which became the foundation for theories about computing and computers, was first proposed by Alan Turing in 1936; and the Electronic Numerical Integrator and Calculator, which was the first electronic computer used for general purposes, was invented by John Presper Eckert and John Mauchly at the University of Pennsylvania in 1946.

The emergence of computer networks has a more coherent history. The first paper on switching theory was published in 1961 and by the late 1960s, plans of the ARPANET were being developed. By 1969, a Network Measurement Center at UCLA was selected to be the first node on the ARPANET and the first host computer was connected. Further design choices that have shaped the internet in its current form continued to be made into the 1970s.

For both the creation of computers and the internet, a number of actors were integral. Indeed, the starting point of computers and computer networks was an assemblage of different actors in its own right: academia was at the forefront in many of the decisive developments, yet both states and private sector firms also played vital roles.

3.2. Two: Development of the Private Sector

While initially an academic and military pursuit, commercial incentives drove the subsequent development of computers and computer networks. As APRANET was decommissioned in 1990, the obvious market opportunities of the technology led to an influx of private sector firms who were willing to invest significantly in research and development. This was seen most clearly in the US, where several US computer manufacturers, software vendors and internet service providers began to develop capabilities at a global level. Firms such as IBM, Microsoft and Apple grew rapidly during this shift.

These private developments have grown cyberspace exponentially, making it an integral part of society. With this growth, cyber security has become an increasingly important issue. With many of today's cyber security concerns emerging as a result of the private sector driven growth of networks, it is private actors, who have often been at the forefront of cyber security challenges.

Through their growth, private actors have also taken on a greater political role. Microsoft, for example, has created an international diplomacy team that participates actively in international fora in order to lobby the technology firm's perspective to policymakers from around the world. Google has likewise become involved in various political issues, ranging from protecting the identities of protestors (Halliday, 2012), to developing sophisticated measures to steer potential ISIS recruits away from the terrorist cell (Greenberg, 2016). Yet, whilst political, ethical and security challenges are thrust upon private actors, this does not mean they are always embraced or anticipated. Social media platforms, for example, have come under increasing criticism for failing to deal with disinformation campaigns. While many private actors are undoubtedly now political actors in a cyber security context, this does not, however, mean that they are necessarily competent in such a capacity.

3.3. Three: State Realisation

Although states played an integral role in the formation of the internet and the development of networks, governments on the whole have responded slowly to the cyber security challenges that have emerged as the private sector-led growth of cyberspace has developed since the 1990s (with certain military and intelligence agencies an exception). As computers and networks have become increasingly integral to modern life, states have gradually woken up to the importance of developing their own cyber security capabilities and are starting to invest significantly in the issue. The variety of government objectives has naturally led to divergence in the sort of developments that states have invested in. Authoritarian regimes have developed technology and infrastructure that prevents dissent and political protest (Deibert, 2013). Conversely, Western democracies have invested heavily in cyber security programs: the UK Government has significantly increased its cyber security spending to £1.9 billion in the period 2016–2021 (HM Government, 2016) while The Pentagon has requested $34.7 billion in cyber security funding between 2017 and 2021 (Capaccio, 2016).

3.4. Four: Emerging Hybridity and Contestation

Computers and computer networks, have always comprised an assemblage of actors that includes academia, governments, private sector firms and advocacy groups. These assemblages have become increasingly complex over time with a marked increase in the number of actors involved. The result is the emergence of increasingly hybrid structures—assemblages that embed a range of actors and transcend traditional global-local and public-private distinctions. For example, information sharing partnerships also exist with active participation from both corporations and government entities (NCSC, 2016). Such security arrangements are neither clearly public

or private security but instead an amalgamation of the two—one captured more coherently through an assemblage lens. The network of computer emergency response teams (CERT) also collaborate through the Forum of Incident Response and Security Teams (FIRST) network that combines national and international as well as public and private CERTS. At a more active level, hacker groups will assist and work with government actors in conducting offensive activities. Although these activities are often state-directed, hacker groups also operate independently—often representing a government's interests without explicit instruction or direction from government actors (Suciu, 2015). Such relationships have been presented as state-proxy relationships (Maurer, 2018) that, by definition, imply a certain binary relationship between two actors. However, an assemblage framework that accommodates what are often looser hybrid structures and naturally affords a greater agency to non-state actors provides a more coherent concept for capturing this empirical reality.

As these cyber security assemblages have grown and become more complex, they have also represented an increasing source of tension. Security assemblages are not necessarily harmonious or stable structures. Assemblages are often marked by competition and struggles for power and influence with different actors appealing to conflicting visions of what should be 'public' and 'private'. The history of cyber security related issues is replete with examples of these tensions. The state is a key protagonist in the vast majority of these disputes, becoming increasingly assertive and willing to challenge established private sector norms. The growth in their capabilities has therefore proved a notable source of tension and instability.

3.5. Five: Generativity

If the previous shift described the further development and growth of hybrid structures, comprised of a range of pre-existing actors, then the process of generativity points to the emergence of altogether new actors and processes.

Generativity, first espoused by Jonathan Zittrain, refers to the way in which the malleable nature of digital technologies (such as the internet) allows them to serve a variety of purposes, potentially providing a platform for innovation that may not have even been foreseen by their creators (Zittrain, 2006). Most computers are designed to be able to run software that is not written by the computer manufacturer or operating system publisher, thereby enabling a computer to be used for a range of processes that it was not initially designed for. For example, while Twitter was launched in 2006, computers built before this time would nevertheless be able to run the service provided they had an internet connection and internet browser.

The generative process goes beyond adaptations to hardware and software: it also leads to the emergence of altogether new actors and processes. The outbreak of the WannaCry ransomware worm provides a clear example of these other forms of generativity. Take a moment to consider the strange trajectory of events which led up to the WannaCry ransomware outbreak. First, the US National Security Agency (NSA) developed a number of exploit tools to be used for intelligence gathering and offensive cyber operations (Burgess, 2017). These vulnerabilities were then leaked by The Shadow Brokers (whose identity and intentions remain unverified) (Goodin, 2017), before going on to being used as part of the WannaCry ransomware deployed by North Korea (Volz, 2017). Here, a number of previously separate processes have become embedded: the NSA's development of cyber tools for intelligence gathering and offensive cyber operations led to both the development of a group that leaked these tools before a separate global breakout of ransomware.

Taking the response to malware for example, hardware and software vendors initially tried to protect their own products and services. Yet, it did not take long for an anti-virus industry to form (McAleavey, 2011). The assemblage of actors and processes involved with malware has expanded further still, including white-hat hackers, bug bounties and crypto-markets that illegally sell malware tools. Some of these emerging actors and processes will have further knock-on effects: the emergence of online illegal malware market will create new government police and cybercrime units. Cybersecurity is replete with examples of these sort of generative cascades that creates unstable processes where the implications of an emerging technology, in terms of its impact on the development and emergence of both actors and processes, is highly uncertain.

This five-shift model of security assemblage has implications for security provision today. While states were involved since the beginning of cyber security assemblage processes, they have significantly developed their political role and capabilities in the last decade. Throughout the emergence and development of cyber security assemblages, private actors have therefore enjoyed a significant degree of agency. The more recent further emergence of government actors therefore explains many of the tensions observed today. Whether it is encryption disputes, the increasing regulation of cyber security issues, or the knowledge of vulnerabilities that government actors withhold, states increasingly challenge, disrupt and often undermine the norms and practices that have previously been established amongst private actors. Government actors often 'argue through the past' (Stevens, 2016) evoking, for example, historical analogies regarding their previous ability to access the data of criminals and terrorist suspects through wiretaps in an attempt to make normative claims and justify why they should be able to access encrypted data. Here, states play on their broadly-perceived legitimacy within other security issues in the past to justify an expanded role in the context of cyber security in the future. As private ac-

tors have developed with relatively minimal state involvement since the 1990s, as the state now enters this space further, their previous lack of involvement makes their increasingly active role and their legitimacy as a security actor controversial and increasingly contested.

The diachronic nature of cyber security assemblages is therefore critical. The above analysis highlights the dynamic and highly unstable nature of cyber security assemblages. This constant to-and-froing of cyber security providers, as their power, roles and responsibilities shift, stands as a perennial feature in the development of cyber security assemblages. It remains unclear what aspects of cyber security will eventually be 'public' or 'private'. These contestations are therefore largely unresolved. Flat analyses of cyber security that neglect these ongoing processes therefore miss crucial components regarding the nature of contemporary security provision.

4. Conclusion

This article has introduced a framework for how the assemblage concept can be applied to cyber security. Yet specific cyber security issues have their own unique features—the dynamics of a US encryption assemblage are rather different to an international internet governance assemblage for example. Moving forward, the concept has greater utility when applied to specific case studies. Here, it can be used to examine the issues outlined above, with focus on how security actors interact and with consideration towards power relations, incentive structures and the practices that embed actors together.

The cyber security assemblage concept goes beyond merely recognising the importance of non-state actors or the interdependence between different actors. Crucially, the concept unearths and captures processes that are essential to contemporary cyber security challenges—the current disputes over what should be 'public' and 'private', the presence of contradictory trends as different security actors cooperate and compete with each other simultaneously, a consideration of the diachronic nature of cyber security provision, and the emerging hybridity of cyber security practices that cannot be neatly accommodated within traditional theoretical paradigms.

Thinking with assemblages is useful for understanding the security implications of particular configurations of actors. Discussions of cyber security have become lopsided. Analysis within security studies literature has focused primarily on issues including attribution, deterrence, and offence-defence balance with the dynamics between security actors often neglected. Yet, when considering the relationships between actors—the extent to which mutual understandings of 'public' and 'private' are settled or disputed, or whether there are clashing incentives between actors—these are issues that have fundamental implications towards the nature of security.

Whilst the arguments within this article are largely theoretical, the benefits of an assemblage approach also lie in its practical application. In a security environment where issues such as the use of contractors and diverse supply-chains present security concerns, understanding the network of security actors and how actors relate to one another is important. Thinking with assemblages can be used to understand shifts in actor's capabilities. As public and private actors seek to expand their remit, the assemblage framework provides a lens for capturing processes such as securitisation that present very real threats to individuals. Viewing the growth of private sector actors through an assemblage paradigm brings attention to the nascent challenges they face. As technology firms expand, their purview has increased exponentially as they are confronted with strategic, ethical and foreign-policy alignment challenges. Here, an assemblage approach brings attention to the profoundly political nature of many of these private firms.

There may also be useful comparative insights. Cyber security assemblages, however they are drawn, contrast starkly within different contexts. This provides insight into the different strategic challenges each government faces. Taking the US for example, the incentive structures of private actors often run contrary to the interests of the US government in relation to issues including encryption. A US cyber security assemblage is therefore characterised largely by disputes and friction between public and private actors. A Chinese cyber security assemblage, by contrast, contains a much greater level of harmony between different security actors. Such a comparison, therefore helps policymakers understand the challenges they face, and crucially the relative characteristics of the assemblages that they operate in.

Often underestimated, challenges related to security provision are critical to cyber security. The configuration of security actors, and how actors relate to one another, have fundamental implications for the nature of cyber security. The discipline of IR has much to offer in developing a fuller understanding of these issues. Thinking with assemblages provides a promising framework for advancing such an endeavour.

Acknowledgements

The author is grateful to the thoughts and comments provided by Nazli Choucri, Lucas Kello and Lucie Kadlekova. The author would also like to thank the three anonymous reviewers who engaged with an earlier draft of the article.

Conflict of Interests

The author declares no conflict of interests.

References

Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state*. Cambridge: Cambridge University Press.

Acuto, M., & Curtis, S. (2014). Assemblage thinking

and international relations. In M. Acuto & S. Curtis (Eds.), *Reassembling international theory: Assemblage thinking and international relations* (pp. 1–15). London: Palgrave Macmillan.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber security. *European Journal of International Security*, *1*(2), 176–198.

Burgess, M. (2017). Everything you need to know about EternalBlue—The NSA exploit linked to Petya. *Wired*. Retrieved from http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch

Capaccio, A. (2016). Pentagon seeks $35 billion to beef up cybersecurity over 5 years. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2016-02-29/pentagon-seeks-35-billion-to-beef-up-cybersecurity-over-5-years

Carr, M. (2014). Power plays in global internet governance. *Millennium*, *43*(2), 640–659.

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

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Collier, J. (2016). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. In M. Taddeo & L. Glorioso (Eds.), *Ethics and policies for cyber operations* (pp. 187–212). Cham: Springer.

Collier, J. (2017). Proxy actors in the cyber domain: Implications for state strategy. *St Antony's International Review*, *13*(1), 25–47.

Cox, J. (2016). GCHQ Has disclosed over 20 vulnerabilities this year, including ones in iOS. *Motherboard*. Retireved from http://motherboard.vice.com/read/gchq-vulnerabilities-mozilla-apple

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. Toronto: McClelland & Stewart.

DeLanda, M. (2002). *Intensive science and virtual philosophy*. London: Continuum.

DeLanda, M. (2006). *A new philosophy of society: Assemblage theory and social complexity*. London: Continuum.

DeLanda, M. (2010). *Deleuze: History and science*. New York, NY: Atropos.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia*. London: University of Minnesota Press.

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th international conference on cyber conflict* (pp. 141–153). Tallinn: NATO CCDCOE.

Dunn Cavelty, M. (2015). Cyber-security and private actors. In R. Abrahamsen & A. Leande (Eds.), *Routledge handbook of private security studies* (pp. 65–71). Abingdon: Routledge.

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.

Egloff, F. (2017). Cybersecurity and the age of privateering. In G. Perkovich & A. E. Levite (Eds.), *Understanding cyber conflict: Fourteen analogies* (pp. 231–247). Washington DC: Georgetown University Press.

Goodin, D. (2017). NSA-leaking shadow brokers just dumped its most damaging release yet. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet

Greenberg, A. (2016). Google's clever plan to stop aspiring ISIS recruits. *Wired*. Retrieved from https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits

Halliday, J. (2012). Google introduces face-blurring to protect protesters on YouTube. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2012/jul/19/face-blurring-technology-youtube-protestors

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Hern, A. (2015). Apple calls on UK government to scale back snoopers charter. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill

HM Government. (2016). *National cyber security strategy 2016–2021*. London: HM Government.

Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.

Lisle, D. (2013). Energising the international. In M. Acuto & S. Curtis (Eds.), *Reassembling international theory* (pp. 67–74). London: Palgrave Macmillan.

Maurer, T. (2015). Cyber proxies and the crisis in Ukraine. In K Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (pp. 79–86). Tallinn: NATO CCDCOE.

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge: Cambridge University Press.

McAleavey, K. (2011). The birth of the antivirus industry. *Infosec Island*. Retrieved from http://www.infosecisland.com/blogview/15068-The-Birth-of-the-Antivirus-Industry.html

McFate, S. (2014). *The modern mercenary*. New York, NY: Oxford University Press.

Müller, M., & Schurr, C. (2016). Assemblage thinking and actor-network theory: Conjunctions, disjunctions, cross-fertilisations. *Transactions*, *41*(3), 217–229.

Mumford, A. (2013). *Proxy warfare*. Cambridge: Polity.

National Cyber Security Centre. (2016). *Cyber security information sharing partnership (CISP)*. Retrieved from https://www.ncsc.gov.uk/cisp

Nye, J. S., Jr. (2011). *The future of power*. New York, NY: PublicAffairs.

Ottis, R. (2012). *Lessons identified in the development of volunteer cyber defence units in Estonia and Latvia*. Tallinn: NATO CCDCOE.

Rattray, G. J., & Healey, J. (2011). Non-state actors and cyber conflict. In K. M. Lord & T. Sharp (Eds.), *Americas cyber future security and prosperity in the information age* (pp. 65–86). Washington, DC: Center for a New American Security.

Rifkind, M. (Ed.). (2013). *Foreign involvement in the critical national infrastructure: The implications for national security*. London: Intelligence and Security Committee.

Rosenzweig, P. (2013). The United Kingdom and Huawei. *Lawfare*. Retrieved from https://www.lawfareblog.com/united-kingdom-and-huawei

Sassen, S. (2008). *Territory, authority and rights: From medieval to global assemblages*. Princeton, NJ: Princeton University Press.

Schmitt, M. N., & Vihul, L. (2014). Proxy wars in cyberspace: The evolving international law of attribution. *Fletcher Security Review*, *1*(2), 53–72.

Sheldon, R., & McReynolds, J. (2015). Civil-military integration and cybersecurity: A study of Chinese information warfare militias. In J. R Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cyber security* (pp. 188–222). New York, NY: Oxford University Press.

Shires, J., & Smeets, M. (2017). The word cyber now means everything—And nothing at all. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_lost_all_meaning.html

Singer, P. W. (2008). *Corporate warriors: The rise of the privatized military industry*. Ithaca, NY: Cornell University Press.

Stevens, T. (2012). Norms, epistemic communities and the global cyber security assemblage. *E-International Relations*. Retrieved from http://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage

Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge: Cambridge University Press.

Suciu, P. (2015). How hackers work like a PAC. *Fortune*. Retrieved from http://fortune.com/2015/08/31/how-hackers-work-like-a-pac

Toomesaar, K., & Ottis, R. (2010). From pitchforks to laptops: Volunteers in cyber conflicts. In C. Czosseck & K. Podins (Eds.), *Conference on cyber conflict* (pp. 97–109). Tallinn: NATO CCDCOE.

Voelkner, N. (2013). Tracing human security assemblages. In M. B. Salter & C. E. Mutlu (Eds.), *Research methods in critical security studies* (pp. 203–206). Abingdon: Routledge.

Volz, D. (2017). U.S. blames North Korea for 'WannaCry' cyber attack. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

Ward, A., Pickard, J., & Stothard, M. (2016). Hinkley go-ahead after 'national security' safeguards. *Financial Times*. Retrieved from https://www.ft.com/content/0cde26b6-7b66-11e6-b837-eb4b4333ee43

Williams, M. C. (2016). Global security assemblages. In R. Abrahamsen & A. Leande (Eds.), *Routledge handbook of private security studies* (pp. 131–139). Abingdon: Routledge.

Zittrain, J. (2006). The generative internet. *Harvard Law Review*, *119*(7), 1974–2040.

About the Author

Jamie Collier is a Cyber Security DPhil Candidate based at the Department of Politics and International Relations, and the Centre for Doctoral Training in Cyber Security, University of Oxford. Within Oxford, Jamie is a Research Affiliate with the Centre for Technology and Global Affairs, and a Research Associate with the Changing Character of War Programme. Jamie was based in the US as a Cyber Security Fulbright Scholar at the Massachusetts Institute of Technology during 2017. Jamie also works with Oxford Analytica on cyber security issues and has previous work experience with the NATO Cooperative Cyber Defence Centre of Excellence and PwC India.

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 22–30
DOI: 10.17645/pag.v6i2.1385

Article

Cybersecurity Research Meets Science and Technology Studies

Myriam Dunn Cavelty

Center for Security Studies, ETH Zürich, 8092 Zürich, Switzerland; E-Mail: dunn@sipo.gess.ethz.ch

Submitted: 26 January 2018 | Accepted: 18 April 2018 | Published: 11 June 2018

Abstract
This article sets out to show how different understandings of technology as suggested by Science and Technology Studies (STS) help reveal different political facets of cybersecurity. Using cybersecurity research as empirical site, it is shown that two separate ways of understanding cybertechnologies are prevalent in society. The primary one sees cybertechnologies as apolitical, flawed, material objects that need to be fixed in order to create more security; the other understands them as mere political tools in the hands of social actors without considering technological (im)possibilities. This article suggests a focus on a third understanding to bridge the uneasy gap between the two others: technology defined as an embodiment of societal knowledge. The article posits that in line with that, the study of cyberpolitics would benefit from two innovations: a focus on cybersecurity as social practice—enacted and stabilized through the circulation of knowledge about vulnerabilities—and a focus on the practices employed in the discovery, exploitation and removal of those vulnerabilities.

Keywords
actor-network theory; cybersecurity; cyberwar; science and technology studies; sociology of knowledge

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

Cybersecurity is an important matter in (inter)national politics. But what makes it a *political* issue? Is it not the case that cybersecurity sensitivities arise primarily due to the continued proliferation of digital *technologies* in many aspects of human life? More specifically, if we were to take away the technologies, would the issues not be solved?

Of course, to claim that cybersecurity is predominantly about technology does not do the issue justice, not least because there is ample research both recognizing and focusing upon the human aspect of the security equation (Furnell & Clarke, 2012; Lebek, Uffen, Neumann, Hohler, & Breiter, 2014). Despite this human aspect, this article will proceed from the claim: cybersecurity is about technology. To clarify, as science and technology studies (STS) purport, "technology" means more than is implied by the common usage of the term (Bijker, Hughes, & Pinch, 1987). To make the statement less provocative and more analytically meaningful, this article sets out to show how *three different conceptualisations* of technology can help reveal different facets of cybersecurity as a technopolitical issue. Though there are attempts to bridge the gap between STS and international relations literature more generally (McCarthy, 2016), the STS perspective has not as yet been fruitfully applied to the study of cybersecurity politics.

Following Bijker (2006) the first of the three understandings is *material*: it frames technologies as static artefacts, i.e., "things". The second of Bijker's understandings links technology to social activities: it refers to the interactive relationship between technological objects and humans. The third—and perhaps least familiar—perspective understands technology according to its etymological roots in Ancient Greek, as *techne* and *logos*. *Techne* means art, skill, craft, or the way, manner, or means by which a thing is gained. *Logos* means word, the utterance by which inward thought is expressed, a saying, or an expression. This third perspective thus refers to the discourse around "what people know as well as about what they do with" technology (Bijker, 2006, p. 682).

Technologies in this view are embodiments of societal knowledge, sites where power relations can be seen in operation as they shape and coordinate the behaviour of social actors (Behrent, 2013, p. 57; also Foucault, 1981).

Broadly speaking, STS focusses on the simultaneous shaping of scientific knowledge, technological artefacts and societal matters (cf. Jasanoff, 2005). For cybersecurity, science is an interesting empirical field from which to learn more about the dominant and less dominant ways of thinking about the issue. Empirically, this article uses biometric data to show how the different perspectives of technology play out more concretely. To help understand dominant views of technology *across* disciplines without falling prey to a disciplinary bias, the article turns to scientific output as documented in two prominent scientific databases—World of Science (WoS) and Scopus.[1] In contrast to disciplinary literature reviews (for example, Ebert & Maurer, 2017), the quantitative nature of bibliometrics "provides a certain sense of objectivity for descriptive purposes" (Martinez-Gomez, 2015, p. 209), which of course does not absolve us from interpreting the results carefully in the appropriate context.[2]

The article has three main sections, one for each of Bijker's ways of understanding technology matched to cybersecurity research. What the bibliometric analysis shows is that the first perspective is by far the most dominant. In this "techno-objectivist" view, cybertechnologies are seen as broken "objects" that need to be fixed to produce more security. Political forces are not considered, even though they clearly pre-shape the research environment. The second view, which is marginalized in comparison, is "politico-subjectivist". Cybersecurity is read within pre-existing frameworks of political theories and assumptions. By focusing on cybertechnologies as tools of power in the hands of social actors, analyses often lose sight of technological materiality and idiosyncrasies, which leads to unsatisfactory conclusions.

In contrast to the first two, the third understanding of technology is not visible in the research output. Given that this thematic issue is looking for "innovative approaches to the study of global cybersecurity governance" within the broad field of political science, the article suggests how it could be used to bridge the gap between technical and social inquiries. It is suggested that political scientists can study cybersecurity in innovative ways by looking at how knowledge around the core of cybersecurity—(computer) "vulnerabilities" and their exploitation—is gained within social relations and how such knowledge is related to social and political processes of sense-making and power.

2. Dominant View: Cybersecurity as "Fixing Broken Objects"

WoS and Scopus differ in the way they classify documents into research areas. However, in both databases the field of computer science tops the lists of research areas (WoS: 72%/Scopus: 61%), followed by engineering (WoS: 36%/Scopus: 40%).[3] Though disciplinary categorization comes with its own challenges, this trend is still indicative of the background of the professionals who produce the most cybersecurity research and where the intellectual home of cybersecurity sits.

Though the absolute number of citations varies between the two databases, which leads to different overall rankings, eight of the top ten most cited articles are the same in WoS and Scopus (see Table 1 for top three, matched across both databases).[4] A fact which leaves little doubt as to the area of highest interest, *all* of the Top 10 cited articles in both databases focus on smart grids and/or SCADA (Supervisory Control and Data Acquisition) systems, a category of software application used in many industrial processes to better control equipment and conditions. The majority of these Top 10 articles were published in journals run by the *Institute of Electrical and Electronics Engineers* (IEEE), the largest existing professional association for technical professionals. All the articles are relatively recent, focus on conceptual clarifications, define the new challenges of "cyber-physical systems", offer some classification for different

Table 1. The three most cited cybersecurity publications in both databases (in October 2017).

Title	Journal	Published in
A Reliability Perspective of the Smart Grid (Moslehi & Kumar, 2010)	IEEE Transaction on Smart Grid	2010
A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges (Yan, Qian, Sharif, & Tipper, 2013)	IEEE Communications Surveys And Tutorials	2013
Cyber-Physical System Security for the Electric Power Grid (Sridhar, Hahn, & Govindarasu, 2012)	Proceedings of the IEEE	2012

[1] Google Scholar does not offer the same services of analysis and data extraction at the moment and was therefore not used due to the impossibility to compare the data. On the differences between the databases, see Mongeon and Hus (2016).
[2] Data was considered up to the end of 2016.
[3] Multiple categories per entry are allowed.
[4] The usual method to identify publications with the most influence is to look at their number of citations. There are plenty of well-known issues with such an approach (Archambault, Vignola-Gagné, Côté, Larivière, & Gingras, 2006; Leydesdorff, 1989), but it can suffice here as an indicator of importance in the larger field.

aspects of smart grid security, and describe some of the solutions, with emphasis on risk management methodologies and future research needs.

A qualitative reading of the top 10 cited articles reveals that the reason for studying cybersecurity issues stems from a set of larger, uncontested technological trends including autonomous systems as well as cloud and high performance computing. The level of risk is considered to be on the rise because of progressive digitalization. Through the connection of the virtual realm with the real world in "cyber-physical systems", scenarios involving more severe damage are possible, the most serious being a sustained and large-scale power outage with potentially catastrophic consequences. These scenarios are not new. On the contrary, they have always been very strong fear mobilizers in the related policy debate (Conway, 2008). However, recent technological developments (*opportunity*) coupled with reports of rising skills of malicious actors (*capabilities*) make these scenarios seem more likely now than they ever were.

"Vulnerabilities", exploitable flaws in code or design of hardware or software, are the focal point of this type of research. In the field of IT-Security, vulnerabilities are defined as weaknesses or flaws in hardware or software products that allow an attacker with sufficient capabilities to compromise the integrity, availability, or confidentiality of a resource (cf. Bowen, Hash, & Wilson, 2006). The type of security that is sought is a combination of these three IT-security goals—if only one is compromised, the system's overall security is compromised. Integrity refers to the trustworthiness of a resource: it is compromised if silent modification without authorization occurs. Availability is compromised if an appropriate user is denied access to a resource. Confidentiality is compromised if somebody gains access to information that she should not have had access to. The main aim of research is to develop better cyberincident prevention, protection and detection capabilities on the one hand and more "resilient" systems and infrastructures, signifying timely recovery of functionality if under duress due to an attack, on the other. The causes of the insecurity are of little interest—fixing them is the priority.

From this perspective, data is like a raw material, the "blood" of cyberspace, that which circulates through the arteries (the information infrastructure). Security here is security *of* cyberspace—the protection of the body and the blood. Cybertechnologies are mere objects to be acted upon. Ultimately, we are looking at the practice of fixing flawed, inanimate "things" to the greater benefit of all. This way of thinking is instrumental for sustaining a specific kind of a-political materiality, which is an underlying condition for security and protection practices, but is also reproduced through them (Aradau, 2010). Political practices or borders are secondary: all things share the same vulnerabilities and everybody will profit equally from fixing them. Consequently, cybersecurity is entirely positive in its overall connotation. The focus is on developing usable "tools and techniques" to improve the overall level of IT-security. Future research is geared towards developing marketable solutions that will create a larger benefit for society through a) ensuring trust in cybertechnologies and b) economic growth through innovation in the IT (security) market.

This dominant understanding of cybertechnologies manages to sidestep politics almost completely, and yet is quite obviously very much in its grip. Two data-driven observations support this claim (see Figure 1). First, cybersecurity research output sees an almost exponential

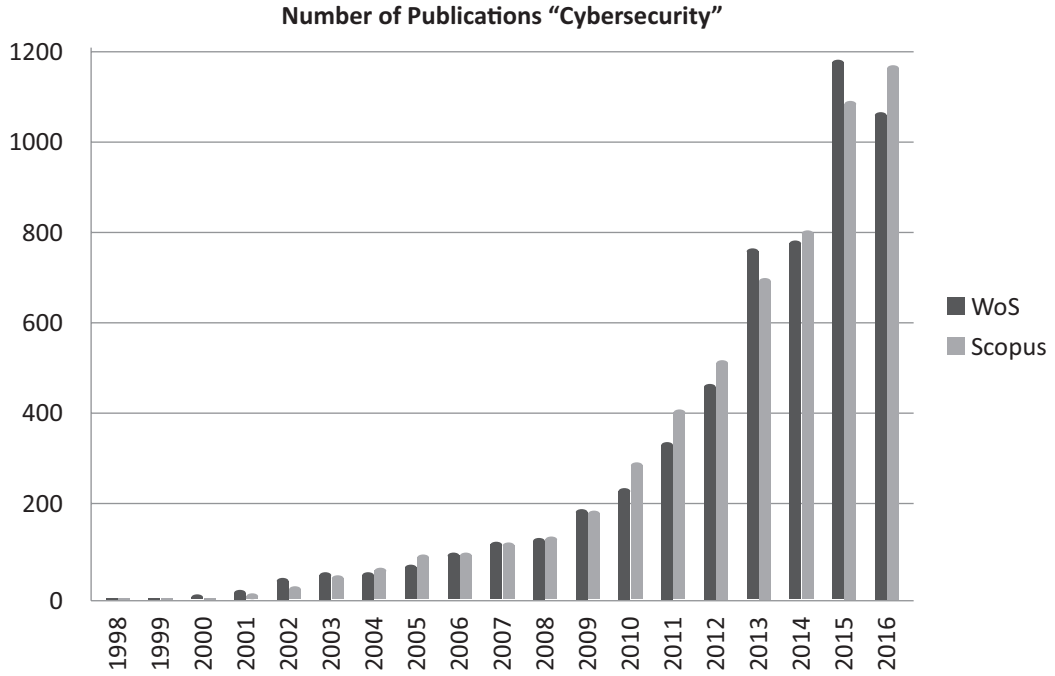

Figure 1. Number of published items per year with Topic "Cybersecurity" (WoS and Scopus).

growth rate. From 2012 to 2014, the number of scientific products almost doubled, with another steep increase in 2015. Even if we can only speculate about why 2012 is the watershed year, we can observe that the steep increase in cybersecurity-related publications around 2012 mirrors the time political attention shifted to highly sophisticated and targeted attacks (epitomized by Stuxnet). They were regarded as indicators for the rising capabilities and political willingness of state actors to use cyberspace for strategic goals (Farwell & Rohozinski, 2011; Langner, 2011). Beyond the question whether there is an *objective* increase in willingness and skill for cyberattacks among political actors, the focus of research on SCADA-systems (as targeted by Stuxnet) and on the infrastructure considered the most "critical" for society (electricity) is intertwined with political interests and sensibilities.

Second, cybersecurity was non-existent as a research topic before 2002, which mirrors observations elsewhere that the term came into existence and gained widespread traction in the policy field only around the year 2000 (Dunn Cavelty & Suter, 2012). Though the details of this dynamic remain unclear, one observer convincingly calls it "attributable to a combination of military influence, marketing hype and societal acceptance" (Rout, 2015). The choice of researchers to use the label "cybersecurity" for their research (rather than Internet security or information security) also occurs against a specific political background. Literature that focuses on the diplomatic difficulties of coming to any international agreements about "cybersecurity" has pointed out that the term is favoured primarily by Western states. In a clear move to disassociate from the Western understanding, Russia and China in particular like to use the term "Information Security" (Giles & Hagestad, 2013). Indeed, in both databases, the US tops the list of the Top 10 countries where cybersecurity research originates by a large margin (WoS: 63%/Scopus: 75%). However, for the search term "Information Security", China leads the ranking before the US (WoS: China 25%, US 11%/ Scopus: China 23%, US 18%).

3. Secondary View: Social Interactions with and through Cybertechnologies

The second conceptualization of technology is focused on the interactions between technology and social actors. As the empirical research reveals, this view is predominantly found in the category "social sciences".[5] Scopus has "social sciences" as a lump category on third place, with 18%. WoS lists 31% of its cybersecurity records in "social sciences", which is the third largest category after "science and technology" and "technology". Overall, this type of research is far less prevalent than the first type (cybersecurity as fixing broken things). Even though there was also a quantitative increase of research around 2010, there is a growing gap between computer sciences and engineering approaches and social sciences research (Figure 2).

Top cited research in the social sciences[6] is much more diverse than the dominant (computer science) view. A reading of the articles reveals two main focal points. The first is an interest in organizational and managerial aspects of cybersecurity, such as "information

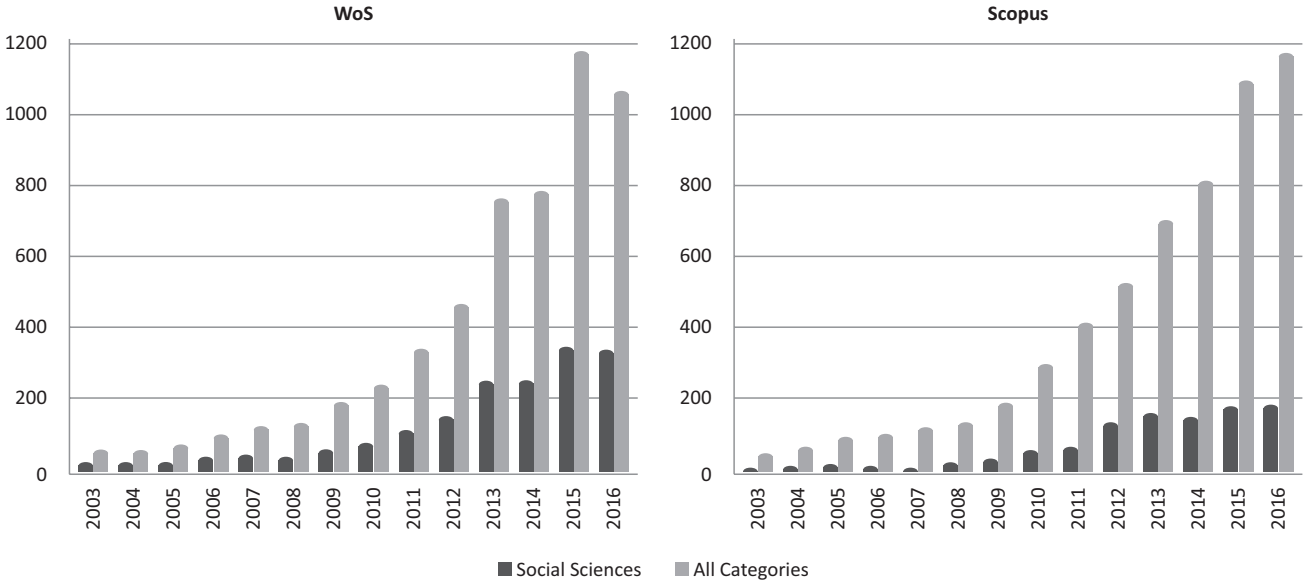

Figure 2. Output of Social Science Research vs. General Cybersecurity Research, both WoS (left) and Scopus (right).

[5] Importantly: this is a database category and does not mean to say that only social scientists work on these issues. In fact, most publications are classified into several different such categories.

[6] For each publication, multiple research areas can be chosen. Therefore, some of the top 10 papers in the social sciences category overlap with the general top 10 papers. After reducing the sample to "pure" social science, 1,220 entries remain in WoS and 497 documents in Scopus.

sharing" between state and private actors (the top cited article in both databases is Gal-Or & Chose, 2005) or the combination of technology with human and organizational factors (cf. Arce, 2003). The second focal point is on cyberwar and related political violence phenomena, which is closer to the core interest of this article. After filtering the results for publications in the "international relations" category, cyberwar and other threat forms dominate in the top cited publications (see Table 2).

Again, the 10 top ranked publications were read for a more thorough understanding of how cybersecurity is viewed. The focus shifts from the inbuilt insecurity of cybertechnologies to their intentional (mis)use by different social actors (and the political processes or concepts this challenges or triggers). The research questions vary depending on the meta-theoretical stance of the authors, leading to a treatment of cybersecurity either as an "objective" problem that calls for different (political) solutions (this is the dominant view) or as a "subjective" construction where different threat perceptions are linked to political outcomes that are critically reflected (this is the less dominant view).

Cybertechnologies become abstract tools of power ("black boxes" in STS jargon) with which to threaten objects and services of value to the state and society in peacetime and during conflict. If threats are considered, there is also an inward-looking focus on vulnerabilities, yet these vulnerabilities are no longer (just) the vulnerabilities in machines, but higher-level, abstract vulnerabilities of the entire society. In a dominant part of the literature, cybertechnologies shape the familiar "realist" conception of inter-state security in an anarchical system. Since these technologies create vulnerabilities that can have detrimental effects on society, more or less traditional "threat" actors and their willingness to do harm come into focus. This way, cybertechnologies gain traction as tools or even "weapons" for disruption and insecurity in the hands of political actors, often states.

Because a link is established to the abstract notion of "national security", states are frequently the actors called upon to re-establish control over the misuse of cybertechnologies through international norms, often by looking to lessons from previous security issues and solutions, like nuclear deterrence. This strong disciplinary "pull" is also visible in the way established approaches to studying political violence are "imposed" on cybersecurity topics. For example, the framing of cyberincidents as cyber*attacks* helps to study cybersecurity through the discipline's core concepts like political violence. Traditional conflict researchers aim to look at the effect of cybertechnologies as part of the toolset in foreign policy and conflict using quantitative methods (exemplary: Valeriano & Maness, 2014). The uncertainties surrounding cyberincidents or the question of what even qualifies as a cyberincident and for what reasons become secondary.

From this perspective, cybertechnologies are treated like any other tool of power projection and coercion and their effects are read in pre-established and familiar categories of political interaction. Technological knowledge has little value for such analyses. In fact, *homo homini lupus* (man is wolf to man) is one of the most important reasons for why cybersecurity has become an issue to study—though, arguably, of marginalized importance in the larger field when considering the minimal coverage in the top ranked political science journals.[7] However, the separation between technical and political knowledge has repercussions for this type of research. For example, the means of achieving security in the anarchical international system are international norms (DeNardis, 2014; Finnmore & Hollis, 2016), one of the core issues the discipline of international relations is interested in. When looking at (the lack of) clear norms for state behaviour in cyberspace solely through the political lens, two important details are missed. First, norms formation in this field is currently happening through explorative "cyberattacks", whereby political actors are using techni-

Table 2. The three most cited cybersecurity publications, filtered for "international relations".

Title	WOS Rank	Scopus Rank	Journal	Published in
Cyber War Will Not Take Place (Rid, 2012)	1	1	*Journal of Strategic Studies 35*(1), 5–32	2012
Digital Disaster, Cyber Security, and The Copenhagen School (Hansen & Nissenbaum, 2009)	2	2	*International Studies Quarterly 53*(4), 1155–1175	2009
Cybersecurity and Threat Politics (Dunn Cavelty, 2008)	3		Book, Routledge	2008
Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War (Liff, 2012)		3	*Journal of Strategic Studies 35*(3), 401–428	2012

[7] As an indication that cybersecurity is a fringe topic in the larger discipline, only one of the top three political science/international relations journals has published articles on cybersecurity (*International Organization*, 0 articles; *World Politics*, 0 articles; *International Security*, 8 articles). Overall, the observation that cybersecurity research in political science is a marginalized topic that communicates relatively little with more general international relations theory and research still hold true today (Eriksson & Giacomello, 2006).

cal means to elicit political reactions and to try out where the "red lines" are. Without a close reading of the technological (im)possibilities shaping these activities, understanding them properly in connection with norms formation processes is difficult. Second, the different communities involved in cybersecurity research and practices have very different understandings of what "security" means and implies. In the second (politico-subjective) perspective, it concerns not only security *of* cyberspace, but also a more abstract form of security that is influenced by activities *in* cyberspace (cf. DeNardis, 2012). Whereas the first is a limited notion of security closely related to technical logics, the second is not. Furthermore, the security *of* cyberspace and security *by* (*or through*) cyberspace are often diametrically opposed. That becomes apparent when we bring computer vulnerabilities back into the analysis: a strategically exploitable cyberspace wants to have vulnerabilities through which to achieve one's goals. A stable and secure cyberspace should have as little as possible. Without understanding the interactions between the two images, finding good solutions will remain elusive.

4. Cybersecurity as "Knowledge about Vulnerabilities"

Even though both the view of cybersecurity based on material vulnerabilities and the socio-political view are interconnected at the very least through their common interest in what both call "cybersecurity", the overlap between the two spheres of research is small. While the first focuses on improving technologies and governing processes without considering the larger context that shapes research questions, the second loses sight of cybertechnologies as a material underpinning of political action. The third perspective—that which sees technology as embodiment of societal knowledge—can help to bridge this gap by analytically combining technical knowledge with political knowledge. Furthermore, it comes with an interesting focus on social practices, much in line with and speaking to the practice turn in critical security studies (Bueger & Gadinger, 2014).

Importantly, neither the technical nor the political lens should be given precedence over the other, at least analytically speaking. Rather, the socio-political determines the technical, and the technical determines the socio-political and both spheres should always be considered as closely intertwined. As an example, consider the limits to the "interpretative flexibility" of cybertechnologies. "Interpretative flexibility" is a term from STS used to highlight that the interpretations and uses of any technology vary across time and between different groups (Woolgar, 1991, p. 30). However, the underlying material insecurity of cybertechnologies is not open to social interpretation. There *are* vulnerabilities that can be exploited by malicious software (malware) or through social engineering (the manipulation of human psychology). On the other hand, knowledge of these vulnerabilities combined with the right capabilities allows certain actions in specific contexts, but are restricted by the characteristic of the vulnerability and its technical environment.

Vulnerabilities (broadly understood) offer themselves as interesting concept around which cybersecurity practices converge.[8] More concretely, the third perspective invites us to focus on cybersecurity as social practice, enacted and stabilized through the circulation of knowledge about vulnerabilities. An approach from STS well suited to study these practices is *Actor Network Theory* (ANT) (Balzacq & Dunn Cavelty, 2016). ANT, better understood as "a way of thinking" instead of a coherent theory, prominently develops a generalized ontological symmetry between human and non-human entities. Both are equally involved in relational productive activities without giving one precedence over the other (Latour, 1994; Preda, 1999). Of interest is the circulation of different "objects"[9] and the structures of relations ("networks" in ANT jargon) that these objects activate. Among other things, ANT scholars are interested in understanding how social practices emerge, how they spread and how they become normalized. They are also interested in the moments such routines break down. These moments are called *depunctualization* because they interrupt the normalized and unproblematic workings of stable networks (Latour, 1999), thereby revealing their inner working to the interested analyst (cf. Best & Walters, 2013, p. 346).

Characteristically, vulnerabilities become visible once their exploitation creates an effect in a machine (the depunctualization). In a first instance, such effects affect the machine that runs the software, and potentially various other processes supported by that machine. However, depending on the type and context of these technical effects, they may be translated into political consequences. In this process, the following questions—among others—are of interest: what kind of incidents become visible and why? Why do some make it into the news, while others remain obscure or potentially invisible? Who has the authority to make claims about cyberincidents and why? In what form is this knowledge made available? Are there conflicting accounts? Do they endure or does one set of interpretations become "the truth"? How does knowledge about vulnerabilities travel between and across different boundaries and with what effects? In what ways is knowledge about vulnerabilities and their exploitation used to make political attributions? In what ways is this knowledge mobilized for political action?

Since space is scarce, a brief example must suffice here. The blockbuster malware "Stuxnet" is chosen;

[8] As a side-note, the concept could also serve for a study on "boundary objects". In STS literature, "boundary objects" operate as mediators in the coordination process between different communities of practice (originally: Star & Griesemer, 1989).

[9] Importantly, an object is not a material thing, but simply something people or other objects "act toward and with. Its materiality derives from action" (Star, 2010, p. 603).

since there is already a large amount of common knowledge about this worm, the added benefit of the proposed approach should become more easily apparent. In the phase immediately after depunctualization, a lot can be learned about power and authority and different practices of knowledge gathering specific to the tech community from observing knowledge claims about vulnerabilities and the incident. In Stuxnet's case, there were several instances of depunctualization, visible to different communities at different times (for more details, see Balzacq & Dunn Cavelty, 2016, p. 17–19). In July 2010 security blogger Brian Krebs broke the news about Stuxnet, causing a very high interest among tech-oriented news media (Krebs, 2010). Several other security researchers added facets of knowledge afterwards. The pieces were finally assembled by Ralph Langner, a German security researcher, who first claimed that Stuxnet was a precision weapon targeting specific facilities and that significant insider knowledge was required for the creation of this worm (Langner, 2010). That made the classification of this malware as "weapon" possible and gave this program particular weight in the discourse.

As soon as several unusual aspects about the malware became public knowledge, attempts to "attribute" the malware began to dominate the discussion. This is a second phase after depunctualization that reveals the interplay between the technical and the political. In November 2010, Langner claimed that the culprit was most likely Israel, the US, Germany or Russia (Zeiter, 2011)—using the *cui bono* logic (to whose benefit) as a basis for this statement. Alternative interpretations existed at the time, but they did not manage to convince a larger audience. Not long after, it became accepted knowledge that Stuxnet was launched by the US and Israel. Debates about this attribution continued among security experts for a time, until a detailed report in the New York Times in June 2012 took an authoritative stance on the attribution question. In this article, David E. Sanger, claiming access to government sources, explained how Stuxnet was programmed and released as a collaborative effect between American and Israeli intelligence services (Sanger, 2012). This explanation has since established itself as the "truth" because the technical expertise was aligned with and influenced by political reasoning.

Of course, we cannot expect access to the inner workings of intelligence agencies and the knowledge creation processes happening there. Nevertheless, public statements by political actors about vulnerabilities and cyberincidents are available and can be studied as part of the larger picture. In the case of Stuxnet, because the US was accepted as the likely culprit, the reaction of its "allies" were twofold. On the one hand, many states updated their cybersecurity strategies. On the other hand, they started investing in cybercapabilities for both their military and their intelligence agencies, in turn creating new possibilities for security-relevant practices. While such reactions can be explained by pointing to the "security dilemma", the actual practices of security actors in cyberspace can only be understood when we take into account the technical possibilities. Finally, returning to the point made above about emerging "norms" of behaviour in cyberspace, rules are shaped by practices and practices are guided by political interests. In cyberspace, practices always have a link to technologies. Ultimately, understanding the behaviour of involved actors means understanding social practices as shaped and restrained by technological (im)possibilities.

5. Conclusion

Though it is true that without (insecure) technology we would not have a cybersecurity issue, these issues also cannot be solved through technical means alone. In addition, though it is impossible to understand the evolution of cybersecurity as a policy issue without telling it as a history shaped by digital technologies and their (mis)use, we cannot understand why it is considered one of the top security political challenges of our time without also understanding why and how digital technologies have been used in social and political contexts. Indeed, technological realities and social practices are closely intertwined.

This article used scientific research as an empirical basis to gain an understanding of how cybersecurity is viewed and then matched it to three views of technology discussed in STS. Two dominant perspectives were identified. The first sees cybersecurity as the practice of fixing broken objects and the second sees cybertechnologies as tools to further political goals. With relatively little overlap between them, the first view neglects social construction and meaning-making processes whereas the second focuses too much on preconceived notions of politics and security, with too little knowledge of how the materiality of the artefacts constrains their use. What we therefore need for innovative cybersecurity research is to combine both perspectives at the intersection between the technical and the social to the greater benefit of both communities. At this intersection, as argued in this article, lies knowledge (and non-knowledge) about vulnerabilities. Therefore, to bridge the two spheres of research, we need to study how knowledge about vulnerabilities is created, disseminated and transformed into political (and other) effects.

Acknowledgements

I would like to thank the three anonymous reviewers and the academic editor for their very helpful comments and my Cybersecurity Team at the Center for Security Studies, ETH Zürich for the many fruitful discussions over coffee and lunch and in the corridors. Special thanks to Robert Dewar for proofreading and editing.

Conflict of Interests

The author declares no conflict of interests.

References

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *43*(2), 491–514.

Arce, I. (2003). The weakest link revisited. *IEEE Security & Privacy*, *1*(2), 172–176.

Archambault, É., Vignola-Gagné, É., Côté, G., Larivière, V., & Gingras, Y. (2006). Benchmarking scientific output in the social sciences and humanities: The limits of existing databases. *Scientometrics*, *68*(3), 329–342.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–198.

Behrent, M. C. (2013). Foucault and technology. *History and Technology*, *29*(1), 54–104.

Best, J., & Walters, W. (2013). Translating the sociology of translation. *International Political Sociology*, *7*(3), 345–349.

Bijker, W. E. (2006). Why and how technology matters. In R. E. Goodin & C. Tilly (Eds.), *The Oxford handbook of contextual political analysis* (pp. 681–706). Oxford: Oxford University Press.

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (1987). *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers*. Gaithersburg: National Institute of Standards and Technology (NIST).

Bueger, C., & Gadinger, F. (2014). *International practice theory: New perspectives*. Basingstoke: Palgrave Macmillan.

Conway, M. (2008). Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. In M. Dunn Cavelty & K. S. Kristensen (Eds). *Securing 'the homeland': Critical infrastructure, risk and (in)security* (pp. 109–129). London: Routledge.

DeNardis, L. (2012). Hidden levers of internet control. *Information, Communication & Society*, *15*(5), 720–738.

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Dunn Cavelty, M., & Suter, M. (2012). The art of CIIP strategy: Taking stock of content and processes. In J. Lopez, R. Setola, & S.D. Wolthusen (Eds.), *Critical infrastructure protection: Information infrastructure models, analysis, and defense* (pp. 15–38). Berlin: Springer.

Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge.

Ebert, H., & Maurer, T. (2017). Cyber security. *Oxford Bibliographies*. Retrieved from http://oxfordbibliographiesonline.com/view/document/obo-9780199743292/obo-9780199743292-0196.xml?

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review*, *27*(3), 221–244.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of cyber war. *Survival*, *53*(1), 23–40.

Finnmore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*, *110*(3), 425–479.

Foucault, M. (1981). *The history of sexuality* (Vol. 1). Harmondsworth: Penguin.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988.

Gal-Or, E., & Chose, A. (2005). The Economic incentives for sharing security information. *Information Systems Research*, *16*(2), 186–208.

Giles, K., & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *Proceedings of the 5th international conference on cyber conflict* (pp. 1–17). Tallinn: CCD COE Publications.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Jasanoff, S. (2005). *Designs on nature: Science and democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.

Krebs, B. (2010, July 10). Experts warn of new windows shortcut flaw. *Krebs on Security*. Retrieved from www.krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw

Langner, R. (2010, September 10). *Stuxnet logbook, Sep 16 2010, 1200 hours mesz*. Retrieved from www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49–51.

Latour, B. (1994). Pragmatogonies: A mythical account of how humans and non-humans swap properties. *American Behavioral Scientist*, *37*(6), 791–808.

Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Cambridge, MA: Harvard University Press.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breiter, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092.

Leydesdorff, L. (1989). The relation between qualitative theory and scientometric methods in science and technology studies. *Scientometrics*, *15*(5/6), 333–347.

Liff, A. P. (2012). Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401–428.

Martínez-Gómez, A. (2015). Bibliometrics as a tool to

map uncharted territory: A study on non-professional interpreting. *Perspectives*, *23*(2), 205–222.
McCarthy, D. R. (2016). *Technology and world politics: An introduction*. London: Routledge.
Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics*, *106*(1), 213–228.
Moslehi, K., & Kumar, R. (2010). A reliability perspective of the Smart Grid. *IEEE Transactions on Smart Grid*, *1*(1), 57–64.
Preda, A. (1999). The turn to things: Arguments for a sociological theory of things. *The Sociological Quarterly*, *40*(2), 347–366.
Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32.
Rout, D. (2015). Developing a common understanding of cybersecurity. *ISACA Journal*, 6. Retrieved from https://www.isaca.org/Journal/archives/2015/volume-6/Pages/developing-a-common-understanding-of-cybersecurity.aspx
Sanger, D. E. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. Retrieved from www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2
Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224.
Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, "Translations" and boundary objects: Amateurs and professionals in Berkeley's museum of vertebrate zoology, 1907–39. *Social Studies of Science*, *19*(3), 387–420.
Star, S. L. (2010). This is not a boundary object: Reflections on the origin of a concept. *Science, Technology & Human Values*, *35*(5), 601–617.
Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists 2001–11. *Journal of Peace Research*, *51*(3), 347–360.
Woolgar, S. (1991). The turn to technology in social studies of science. *Science, Technolgy & Human Values*, *16*(1), 20–50.
Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys and Tutorials*, *15*(1), 5–20.
Zeiter, K. (2011, November 7). Stuxnet timeline shows correlation among events. *Wired*. Retrieved from www.wired.com/2011/07/stuxnet-timeline

About the Author

Myriam Dunn Cavelty is a senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS), ETH Zürich. She was a visiting fellow at the Watson Institute for International Studies (Brown University) in 2007 and Fellow at the stiftung neue verantwortung in Berlin, Germany 2010–2011. Her research focuses on the politics of risk and uncertainty in security politics and changing conceptions of (inter-)national security due to cyber issues.

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 31–40
DOI: 10.17645/pag.v6i2.1329

Article

Enacting Expertise: Ritual and Risk in Cybersecurity

James Shires

Department of Politics and International Relations, University of Oxford, Oxford, OX1 3UQ, UK;
E-Mail: james.shires@politics.ox.ac.uk

Submitted: 29 December 2017 | Accepted: 12 February 2018 | Published: 11 June 2018

Abstract
This article applies the concept of ritual to cybersecurity expertise, beginning with the cybersecurity "skills gap": the perceived lack of suitably qualified professionals necessary to tackle contemporary cybersecurity challenges. It proposes that cybersecurity expertise is best understood as a skilled performance which satisfies decision-makers' demands for risk management. This alternative understanding of cybersecurity expertise enables investigation of the types of performance involved in key events which congregate experts together: cybersecurity conferences. The article makes two key claims, which are empirically based on participant observation of cybersecurity conferences in the Middle East. First, that cybersecurity conferences are ritualized activities which create an expert community across international boundaries despite significant political and social differences. Second, that the ritualized physical separation between disinterested knowledge-sharing and commercial advertisement at these conferences enacts an ideal of "pure" cybersecurity expertise rarely encountered elsewhere, without which the claims to knowledge made by cybersecurity experts would be greatly undermined. The approach taken in this article is thus a new direction for cybersecurity research, with significant implications for other areas of international politics.

Keywords
conference; cybersecurity; expertise; Middle East; performance; skills gap

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

In 1944, the team programming the IBM Mark I, a mammoth computing machine built in the US during WWII to assist military calculations, had a surprising routine:

> When the program was punched into a tape and the moment came to test it, the Mark I crew, as a joke that became a ritual, would pull out a prayer rug, face east, and pray that their work would prove acceptable. (Isaacson, 2015)

This short anecdote suggests that *rituals* exist in technological practices such as cybersecurity, even if most cybersecurity rituals are not as clearly defined as prayer and have little explicit religious content. It also serves as a reminder of the cultural specificity of the Internet's origins, in contrast to its now global reach. Cyberspace is no longer the province only of those who pray towards Mecca satirically, and cybersecurity is a concern across nations, religions and cultures.

This article applies the concept of ritual to the cybersecurity "skills gap": the perceived lack of suitably qualified professionals necessary to tackle contemporary cybersecurity challenges. It draws on theories of expertise in International Relations (IR) to interpret this skills gap not as an objective absence of people or knowledge, but as an ideal socially constructed in tandem with an ever-widening sphere of cybersecurity threats. It proposes that cybersecurity expertise is best understood as *enacted*: as a skilled performance which satisfies decision-makers' demands for risk management. This alternative understanding of cybersecurity expertise as performance enables investigation of the types of

performance at key events which congregate experts together: cybersecurity conferences.

This article makes two key claims, which are empirically based on participant observation of cybersecurity conferences in the Middle East. First, that cybersecurity conferences are ritualized activities which create an expert community across international boundaries despite significant political and social differences. Second, that the ritualized physical separation between disinterested knowledge-sharing and commercial advertisement at these conferences enacts an ideal of "pure" cybersecurity expertise without which claims to knowledge would be greatly undermined.

This article has three main parts. The first introduces the cybersecurity skills gap and offers an alternative interpretation of cybersecurity expertise as performance. The second identifies conferences as a key site for participant observation and details the growth of cybersecurity conferences in the Middle East. The third applies the concept of ritual to these conferences. Following the conclusion, a postscript reflexively considers my role as a participant observer.

2. Cybersecurity Expertise

Cybersecurity experts are in great demand. A survey in 2015 predicted a "shortfall" of 1.5 million "information security professionals" by 2020 ((ISC)^2, 2015), and a year later another survey increased this forecast to a 2 million "shortage" of "cybersecurity professionals" by 2019 (ISACA, 2016). The message of these surveys, which are partly intended to raise awareness and business for those conducting them, is clear: there is a cybersecurity "skills gap", where "cyberattacks are growing, but the talent pool of defenders is not keeping pace" (ISACA, 2016). Current policy responses to this skills gap focus on adapting curricula, creating competitions to demonstrate technical skill, and training staff on-the-job (Vogel, 2016).

These policies are hampered by the unclear content of cybersecurity expertise. Cybersecurity professionals appear to require a vast range of skills from communications, compliance, data analytics and organizational psychology, as well as information technology (IT) (Pironti, 2013). This has led some to conclude that there is "surprisingly little consensus" around the cybersecurity skillset (Wolff, 2016). To counter this issue, the UK government has created a "cybersecurity body of knowledge" or CyBOK programme, which aims to build up a repository of core data for cybersecurity (Ensor, 2017). Like many observers of the lack of clarity in cybersecurity expertise, the creator of this programme attributes the problem solely to the "relative youth" of cybersecurity (Ensor, 2017). This suggests that cybersecurity is merely a "nascent epistemic community" (Stevens, 2012), which has yet to settle on its area of exclusive competence.

However, this narrative of novelty is deceptively simple. Novelty is not an external condition to which cybersecurity experts must respond, but rather a concept of time integral to the field itself. In other words, "the field of cyber security seems pervaded by a profound sense of frustration and disorientation at being trapped in an accelerating present, cut off by history" (Stevens, 2015, p. 93). Attributing the cybersecurity skills gap simply to an increasing rate of technological change—a permanent state of novelty—prevents analysis of the social and political ingredients which constitute cybersecurity as an expert domain.

Instead, contest is at the heart of cybersecurity expertise, which has been repeatedly refigured according to its political context (Barnard-Wills & Ashenden, 2012; Bendrath, 2001; Dunn Cavelty, 2008). Although an influential analysis of the social construction of cybersecurity argues that "cyber security can be seen as 'computer security' plus 'securitization'" (Hansen & Nissenbaum, 2009, p. 13), the suggestion that contest is limited to securitization—the framing of political issues as a security concern—implies that computer security itself is clearly defined. In contrast, others argue that the content of computer security, and how and where it overlaps with or adopts labels of cybersecurity and information security, are themselves key areas of contest (Shires & Smeets, 2017, p. 10).

To understand this contest, I draw on more sophisticated understandings of expertise which have emerged in IR (for overviews see Bueger, 2014; Cross, 2013). Such theories hold that, rather than simply importing expert knowledge from their academic or professional discipline into problems of societal and political importance, experts instead conduct what Seabrooke terms "epistemic arbitrage". This is where experts "mediate between knowledge pools for strategic advantage and, if successful, they can become the 'arbiters' on what knowledge and practices are most influential" (Seabrooke, 2014, p. 1). In cybersecurity, the proliferation of related disciplines allows experts to emphasise some areas over others in their interpretation of what counts as cybersecurity expertise, to "create new markets for their services and to challenge established orders" (Seabrooke, 2014, p. 13). This competitive rug-pulling in turn stretches and reshapes the domain itself, redistributing its increasing social, political and financial capital between software engineers and hardware manufacturers, lawyers, accountants and insurers, psychologists, intelligence professionals and political scientists.

These views of expertise focus not on expert knowledge in a static, codified form, but on expert *practice* and *performance*. In the words of legal scholar David Kennedy:

> Expert knowledge is human knowledge: a blend of conscious, semiconscious and wholly unconscious ideas, full of tensions and contradictions, inhabited by people who have projects and who think, speak and act strategically. Style and role count as much as content. (Kennedy, 2016, p. 278)

Kennedy here combines Seabrooke's view of experts as involved in power struggles, jostling for position and concerned with their individual projects, with an emphasis on how expertise is enacted or performed. To be an expert, one must *act* as an expert. For cybersecurity, this performance does not only include familiarity with Internet networks and computer programs, and the use of specialist tools. Most importantly, it includes the judgement and communication of certain risks, including reputational risk, threats to life and safety, financial risk, and national security. This expert performance has been described by some scholars as that of a "cyber-guru" (Quigley, Burns, & Stallard, 2015), who simplifies and overstates risks to maximise cybersecurity "hype" (Lee & Rid, 2014). Kennedy's view of expertise suggests in contrast that expert performance is essentially flexible, and that a nuanced and complex expression of risk can be more effective than exaggeration. In his words, "the uncertainty and ambivalence of professional knowledge may be the subtle secret of its success" (Kennedy, 2016, p. 10).

Cybersecurity experts learn this performance in several ways. One is to obtain cybersecurity qualifications, many of which claim to be "practical" and "hands-on", explicitly recognising the practice-based nature of expertise. Surveys indicate the popularity of this route; three quarters of respondents to one industry survey claimed that professional certifications are an effective way to demonstrate cybersecurity skills (Intel Security, 2016, p. 13). However, such qualifications suffer from contest over the power to become an 'arbiter' of professional practice, in Seabrooke's terms. As Wolff suggests, the "desire to profit from providing [cybersecurity] training may lead to too much competition" (Wolff, 2016), with the result that cybersecurity qualifications are of uncertain value. Supporting this view, other surveys indicate that experience is valued above all else: one found that experience was valued more highly than qualifications (UK HMGovernment, 2014, p. 15), and another reported that 93% of respondents thought experience was more important than qualifications (Sundaram, 2017). While all theories of expertise would agree that experience is important, the performance approach gives it an extra dimension. In this view, cybersecurity experience is not just a chance to collect further knowledge, but an apprenticeship in which professionals first mimic and then successfully inhabit the role of expert, pronouncing authoritatively on cybersecurity risks.

We can now reframe the concerns over a cybersecurity "skills gap" with which I began this section. The skills gap stems from a supposed mismatch between the level of risk and the number of cybersecurity experts. However, we can now see that this level of risk is itself the result of a successful performance by those experts. Crucially, cybersecurity risk expands as more knowledge pools are brought to bear on cybersecurity, with ever more additions to the "attack surface" and potential means for illegitimate access. As long as cybersecurity continues to accrue social and political capital, this proliferation of relevant domains will continue, and the required repertoire of the "sufficiently skilled" cybersecurity professional will continue to expand. A gap is the wrong metaphor for this process, as it obscures the connection between expanding expert performance and increasing risk. Instead of focusing on how to 'close the gap', I examine the performances themselves.

3. Cybersecurity Conferences

Cybersecurity expertise is performed in many places, not least in the day-to-day work of cybersecurity professionals. One way of accessing this performance is through participant observation. Participant observation, defined as "immersion in a community, a cohort, a locale, or a cluster of related subject positions" (Schatz, 2009), is closely associated with a commitment to ethnographic modes of research, which "chronicle aspects of lived experience and…place that experience in conversation with prevailing scholarly themes" (Wedeen, 2010). Some scholars have attempted to access a professional cybersecurity environment—security operations centres, or SOCs—using participant observation. These scholars have identified several new aspects of cybersecurity expert performance, including detailed information about workflows and reflections on their perceived status, described as follows:

> SOCs face a constant challenge in in justifying their value to the management. Security monitoring, unlike in any other business, cannot be quantified through profit margins. Nobody notices the value of a SOC as long as there is no major breach. (Sundaramurthy, Case, Truong, Zomlot, & Hoffmann, 2014, p. 49)

This quotation anticipates an underlying tension between financial incentives and cybersecurity expertise to which I will return in the last section. In this section I detail the empirical site of participant observation on which my argument is based. SOCs and other daily professional environments are not the only locations of expert performance, which also occurs at professional conferences. As Howard describes in his study of digital democracy activists, conferences, although "occurring in sterile hotels…still represent key events full of important social interaction" (Howard, 2002, p. 561). Despite this potential, conferences are not a traditional ethnographic site, as they are short, happen infrequently, and move between different geographical locations. This has posed a methodological problem for anthropologists, who have conceptualised conferences and similar phenomena in several ways: as "transitory" sites; as together forming a "multi-site" ethnography, or as forming one geographically discontinuous site (Falzon, 2009, p. 17).

One region where cybersecurity conferences have become a regular occurrence is in the Middle East. Using structured Internet searches, with search terms based

on cybersecurity and cognate terms such as digital or information security, with "Middle East" as an initial guiding qualifier, I identified 165 conferences within these parameters between 2007 and 2016. Larger technology or security conferences that included cybersecurity as a minor topic were excluded. The rise in the frequency of these conferences was significant, from 2 in 2007 to 28 in 2016, as shown in Figure 1. The conferences included some hosted by cybersecurity vendors, others organised by professional events companies, and some with support from governments or international organisations. The average attendance based on media reports was around 200 people, excluding one large outlier (GISEC, with around 4,000 attendees). In numerical terms, this trend is not especially surprising. The increase in Middle East cybersecurity conferences could probably be replicated in many areas of the world, as during that decade cybersecurity grew significantly in the global consciousness. However, the geographical grouping of these conferences is not intuitively obvious, in two ways.

First, although these conferences are often labelled expansively, as "Middle East", "Middle East and North Africa" (MENA), or as "Arab Region", these conferences nearly all take place in Egypt and the states of the Gulf Cooperation Council (GCC): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE).[1] This narrower representation within the wider Middle East stems from several political factors. Other countries in the region are the site of severe conflicts, and although the Gulf states above are intimately involved in these conflicts their domestic environments have been relatively unaffected. This stability is connected to commercial incentives for holding the conferences: the GCC states are the richest in the Middle East due to extensive natural resources, and have—to various extents—developed their domestic infrastructure to attract global capital (Held & Ulrichsen, 2011). Cybersecurity concerns in these states are much more similar to the concerns of other wealthy, highly connected states than their immediate neighbours (in comparison, Yemen, the only non-GCC Arab state in the Gulf, has very different Internet issues (Dalek, Deibert, McKune, Gill, & Senft, 2015).

Two other key countries in the Middle East cybersecurity landscape, Iran and Israel, are not represented in the conferences above, for different reasons. Iran is seen by many as a geopolitical rival to Saudi Arabia and has conflicted relationships with other Gulf states. Furthermore, Iran is perceived as a threat to the US, which has a longstanding presence in Egypt and the Gulf, due to its nuclear ambitions, regional influence, and reciprocal hostile cyber activity. Israel, in contrast, is a global cybersecurity hub in its own right, with a strong military-based cybersecurity sector (Behar, 2016) and traditional isolation from the Arab world, although covert cooperation exists in various cybersecurity-related areas (Caspit, 2016; Donaghy, 2015; Marczak & Scott-Railton, 2016). In sum, the narrowed definition of Middle East cybersecurity therefore stems not only from domestic characteristics and commercial incentives, but also wider international relations in the region.

However, this grouping of conferences is also surprisingly inclusive, as Egypt and the GCC states have substantial differences which affect their cybersecurity posture. Egypt does not have the same financial advantages due to a large population and relative lack of natural resources, although it also has an outsized military and security sector and commensurate budgets. The Arab Spring was experienced very differently, with Egypt un-

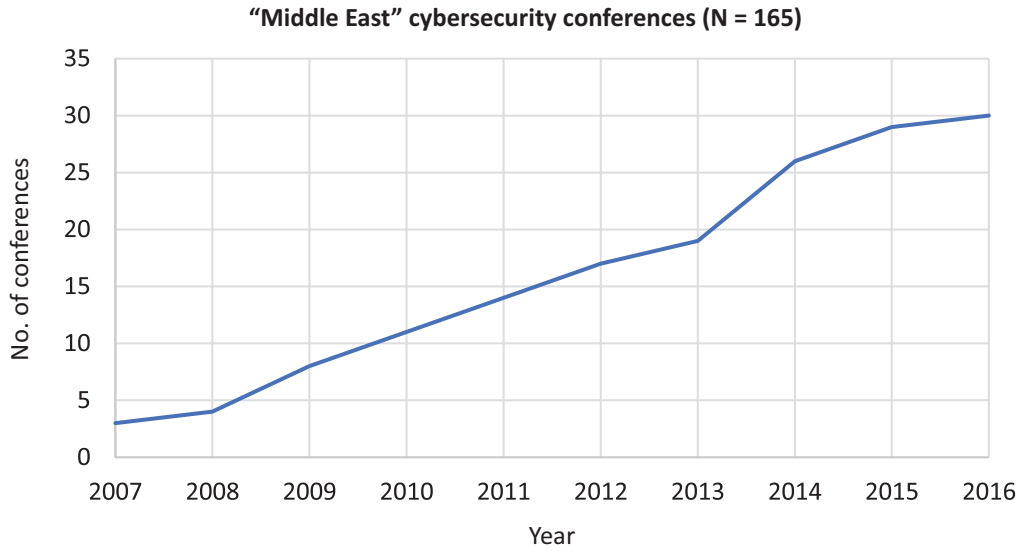

Figure 1. "Middle East" cybersecurity conferences.

[1] The exception was the MENA Information Security conference 2011 in Amman, Jordan. For further discussion about the scope of this term, see Bonine, Amanat and Gasper (2011).

dergoing repeated changes of government and the GCC cooperating in repression against activists (Matthiesen, 2013). While Egypt has broader issues with Internet adoption, and has taken more drastic Internet policies than the GCC—the Egyptian government resorted to a complete severance of Internet connections following the January 2011 revolution—the GCC states have incorporated restrictions on the public sphere in keeping with a cautious approach to new communications technologies due to their potential political effects (Shires, in press). Finally, there are significant political rifts within the GCC, exacerbated since the Qatar crisis in June 2017, leading to a "quartet" of Egypt, Bahrain, Saudi Arabia and the UAE separating from the other three states.

Given these diverse regional factors, the spread of conferences across Egypt and the GCC states is not intuitive and creates a "site" for ethnographic observation in cybersecurity stretching across and between other socio-political divides. I conducted participant observation at seven cybersecurity conferences in the region, summarised in Table 1. These conferences were chosen due to the length of time held, the range of organizing bodies and topic, and more prosaic research characteristics such as budget and time constraints. At these conferences, I repeatedly met the same community of conference speakers, and the same companies and government organizations, which suggests that these conferences constitute a unique regional space in which to perform cybersecurity expertise.

This personal observation of a distinctive cybersecurity community is supported by a wider analysis of conference speakers. I created a dataset of all invited speakers at the 165 cybersecurity conferences in the region, based on a range of open sources including conference programmes and surrounding media. This dataset identified which conference series were attended by each speaker and the number of conferences within each series attended by that speaker. Of the total number of speakers (1,177), only 96 (8%) had spoken at more than three conferences *and* across more than one conference series (and these had often spoken at many more). This indicates that although many individuals participate as speakers at these cybersecurity conferences, a relatively small number do so consistently over time and are recognised as cybersecurity experts by several conference organisers.[2] In the next section, I use the concept of ritual to explore the conference performances of this expert community in more detail.

4. Ritualized Conferences

Cybersecurity conferences are highly ritualized activities. Ritual was originally a term for the script used to instruct religious practices or rites, but has become commonly used to refer to religious practices themselves (Stewart & Strathern, 2014). However, many anthropologists argue that a fundamental distinction between religious and secular is unhelpful in the analysis of rituals (Grimes,

Table 1. Middle East cybersecurity conferences attended.

Name	Location	Date attended	Years held (to date)	Organizing body
ITU Arab Region Cybersecurity Summit	Sharm El Sheikh	October 2016	2014–2017	Egypt National Telecommunications Regulatory Authority (NTRA), International Telecommunications Union (ITU)
FIRST Middle East	Sharm El Sheikh	November 2016	2016	Egyptian NTRA, FIRST (non-profit association of CERTs)
Cairo Security Camp	Cairo	November 2016	2010–2017	Bluekaizen (cybersecurity company)
RSA MENA	Abu Dhabi	November 2016	2012–2017 (others in Qatar and Saudi Arabia)	RSA (cybersecurity and events company)
Cybersecurity for Critical Assets MENA	Dubai	November 2016	2015–2016	Qatalyst Global (cybersecurity events company)
Middle East Cybersecurity	Riyadh	April 2017	2015–2017	Nispana (events company)
ITU Arab Region Cybersecurity Summit	Muscat	November 2017	As above	Oman Information Technology Authority (ITA), ITU

[2] A further step in this analysis would compare this attendance to other regions or other countries in the region such as Iran or Israel. Although space constraints prevent such an analysis here, conversations with the "super-speakers" identified above suggest that they rarely if ever participate in conferences in those two countries.

2006). Instead, we can see all activities as lying on a scale of ritualization with several dimensions, including formalism, disciplined invariance, rule-governance, and symbolism (Bell, 2009, p. 138). Highly ritualized activities possess these characteristics in greater intensity or quantity than the surrounding environment, and these characteristics are often found together, in a mutually reinforcing manner.

The ritualization of cybersecurity conferences is facilitated by their physical and temporal organization, which follows a standard pattern for business conferences. The cybersecurity conferences I attended all had a central presentation room for "keynote" speakers, as well as several breakout rooms for smaller-scale discussions, with scheduling governed by several written and unwritten rules: printed schedules, food and drink requirements, unexpected absences, and the importance of the speaker. There was a separate area for marketing stands by cybersecurity companies, who paid for spaces. Some companies paid for higher levels of sponsorship, in return for a keynote slot and branding on presentations, notes, and conference paraphernalia such as lanyards, which serve as constant symbolic reminders of their contribution. This overall format is largely due to what Bell terms 'disciplined invariance'—i.e., deliberate repetition—created by the logistical and financial assemblage behind the conference. Although the conferences themselves were often hosted by a national government organization involved in cybersecurity, the organization of the conference was outsourced to events companies who imprint standard formats onto the cybersecurity community (following Rappaport's formulation of the conditions of ritual, conferences are largely "encoded by other than performers"; Rappaport, 1999, p. 32). As such, these conferences are ritualized in the sense that they are more rule-governed, invariant, and formalised than the day-to-day work of cybersecurity professionals.

To understand how this ritualization enhances the performance of cybersecurity expertise, we can compare cybersecurity conferences to similar cases. In a closely related context, the concept of ritual has been used to argue that "hacker" conferences embody a particular "lifeworld", which is brought into being through hackers spending short, intense periods of time together focusing on their common passion (Coleman, 2010). However, in her participant observation Coleman also detected differences in the "moral economy" of conferences:

> The differences between the American Psychiatric Association annual meetings, where doctors are dressed in suits and mill about during the day at San Francisco's Moscone Center, retiring individually in the evening to a luxury San Francisco high-rise hotel after a nice dinner, and the outdoor festival held by European hackers, where bodies are clothed in tee-shirts and shorts (if that), and many participants can be found sleeping together under the stars of the night, are difficult to deny. (Coleman, 2010, p. 67)

Despite their similar content to the hacker conferences described by Coleman—malware analysis, details of vulnerabilities, stories of famous hacks, and so on—cybersecurity conferences appear to have as much in common with the drab medical gatherings to which she juxtaposes the hackers' "ritual celebration". The cybersecurity conferences I attended were held in luxury hotels, with high-quality food and drink available throughout. Formal dress was required (Figure 2). As is the case for cybersecurity and technology sectors more generally, there were far more men than women at these

Figure 2. Arab Region Cybersecurity Summit 2017 (Source: Author's own photo).

conferences, and only 4 of the 96 frequent speakers (4%) identified in Part 3 were women.[3] Although the post-conference recreational activities occasionally resembled hacker conferences more closely—for example, poetry recitation on a trip to the beach—there was just as much "milling about". If cybersecurity conferences create a lifeworld, it is not that of the hacker.

Given these differences, another comparison may be useful. Scholars have also conducted participant observation at trade fairs for security products (defence technologies, policing equipment, surveillance, and so on). These fairs have a shared genealogy with the cybersecurity conferences I attended, in that some cybersecurity conferences in the Middle East are offshoots of larger defence and security fairs, and defence companies are central figures in the cybersecurity market. In an analysis of a long-running trade fair in the UK, Alexander argues that "these spaces are pivotal in the dissemination, propagation, and reformulation of changing attitudes towards security" (Alexander, 2014, p. 18), as they underpin the "logic of a particular mind-set regarding what it means to consume security as a commodity" (Alexander, 2014).

Although cybersecurity conferences also involve the sharing of a security mind-set, Alexander's description of security fairs as hotspots for the "intensive exchange of knowledge [and] new ideas" only partly resonates with my participant observation. Although cybersecurity conference programs are full of talks on professional topics, most delegates spend little time listening to them. Other than the keynote speeches, which are well attended partly due to greater interest and partly greater enforcement from the conference organizers, there is ample opportunity to spend time at trade stalls, refreshment places, in hotel lobbies or (if the heat permits) outside at lengthy cigarette breaks. Panel discussions often elicit few questions and little audience participation. When delegates are in the audience, most of their time is spent on devices; sometimes working, but also as an instinctive response to what is almost downtime. Networking is a large part of these conferences, but they also offer a space to relax, to catch up on work, and to spend time away from the desk.

Given the unclear attention paid by conference attendees to formal methods of disseminating knowledge, I use ritual theorists' focus on space (e.g. Turner, 1977), to show how the shared format of these conferences shapes the performance of expertise. The fundamental division in this physical space is between the outer layer of company-branded booths and the inner layer of presentation rooms; in other words, between a space for commerce (the trade stands) and a space for knowledge (the central auditorium and breakout rooms). Speakers conform to this ritual division in their on-stage performance, disclaiming any "sales pitch" when delivering talks, even about their product, although this is often undermined by the company copyright of their slides. The conference space is therefore an explicit acknowledgement and simultaneous separation of both the myriad commercial incentives for conference organizers, hosts, speakers, and attendees at the outer layer, *and* their claims to possess an independent and unbiased expert knowledge at the inner layer.

The separation of knowledge and commerce shapes cybersecurity expertise in two ways, enhanced by the formalism and invariance identified above. First, this separation expresses an ideal version of cybersecurity expertise. Despite the competitive political and commercial struggles between individuals and organizations that exist in any expert domain, this separation creates a guiding principle or myth of "pure" cybersecurity knowledge, untainted by these struggles, which encourages the formation of the discipline itself as a new area of disinterested inquiry. Second, this physical separation inscribes the ability to alter their performance between these spaces—to shift repertoire—as a core skill for cybersecurity experts. The same people deliver their independent expert judgement on stage, and then an unashamedly partisan view of their superior product after returning to their booth. I do not mean to imply that either is incorrect, or that to do both is necessarily hypocritical, but that this duality is imposed by the separation of the conference space itself. Cybersecurity expertise is thus not just the successful performance of risk management, but one which is essentially flexible, with several registers and the capacity for context-based improvisation.

This physical separation and performative disconnect between knowledge and commerce suggests that cybersecurity expertise does not match either close comparison above: it is neither an explicit commodification of security nor a liberated hacker's lifeworld. Instead, the heart of cybersecurity expertise is the simultaneous embrace of an underlying commercial logic *and* the ideal of a neutral judgement of new technological risks. This double movement exists elsewhere in cybersecurity: in the contest over cybersecurity qualifications, in the challenges of cybersecurity public-private partnerships (Carr, 2016), and the rise of the "cyber-industrial complex" (Deibert & Rohozinski, 2011). However, conferences, as ritualized occasions for the performance of expertise *to other experts*, uniquely equip cybersecurity professionals with the repertoire incorporating this double movement, and so are key sites for the production of cybersecurity expertise more broadly.

5. Conclusion

This article has completed three tasks. First, it reoriented discussions around cybersecurity expertise, often

[3] This may be changing: conversations at these conferences suggest that around half of citizens training in cybersecurity in the smaller Gulf states are female (themselves a small proportion of cybersecurity professionals overall, due to the overwhelmingly male expatriate technology community). These simple gender proportions do not accurately portray the complexities of gender performance (both masculinities and femininities) in cybersecurity in the region, which deserve a separate study.

expressed as a skills gap, towards a conception of expertise as successful performance. Cybersecurity expertise should not be thought of as a gap to be closed, because the requirements for successful performance grow together with the widening of the domain. Second, it identified cybersecurity conferences as key sites of expert performance and used the example of cybersecurity conferences in the Middle East to show how such conferences bring together a diverse community across international divisions. Third, it analysed these conferences as ritualized activities, which physically separate commercial transactions and knowledge production in a way which makes possible the emergence of cybersecurity expertise itself as a body of knowledge.

The main limitation of this article is that, due to space constraints, it has focused only on the spatial performance of expertise in the overall conference environment. Further work would distinguish more finely between the different genealogies of cybersecurity professionals (defence, intelligence, IT, engineering, and so on), and would track the effect of this professional "habitus" on cybersecurity worldviews, analysing not just commercial underpinnings but also wider threat construction. A related limitation is that this article relies on personal observation of expert performance (albeit informed by extensive interaction with the expert community) but does not investigate the perception of this performance by experts themselves, or otherwise provide a space for their voices. Further work, drawing explicitly on interviews and conference discourse, would correct this imbalance and provide a more comprehensive picture of cybersecurity expert performance.

This investigation has several implications for other areas of IR. First, it provides a performance-based interpretation of the dynamics of a growing arena of knowledge which could be applied to other skilled domains in international politics. Second, it provides an empirical treatment of cybersecurity conferences in the Middle East, which crosses familiar boundaries and offers a new reading of regional dynamics with implications outside cybersecurity. Finally, it underlines the importance of ritual in analysing the dynamics of international behaviour, especially conferences and conference-like events, which are frequent occurrences in international politics on topics ranging from peace negotiations to climate change treaties. Some of the ritualized characteristics noted here may appear, with similar symbolism, in these other areas.

Postscript

In this postscript, I briefly reflect on my participation in the cybersecurity conferences above. Reflexive analysis of my own epistemological, moral, and other commitments is a key aspect of participant observation. This is especially important as I use the concept of ritual, which imputes significance to an activity which may not be expressed or recognised by other participants. In this analysis, I attempted to avoid two related pitfalls. The first is an assumption of superiority: that the interpretation offered here is somehow truer, better, or more accurate than an "inside" interpretation. The second is a refusal of symmetry. As Latour notes, ritual and its associated concepts are often reserved for those who are assumed not to be "Modern" and are not applied symmetrically to Modern practices (Latour, 2010).

To counter these pitfalls, the analysis above is an intervention in a conversation not only with other academics, but with conference participants as well, to be judged and critiqued on both levels. Furthermore, cybersecurity professionals, as highly qualified graduates of advanced engineering and scientific courses, are as Modern in Latour's sense, if not more so, than any social scientist who works with and alongside them. Consequently, my methods and conclusion are as open to critique by them as much as their epistemological stance is questioned by this article.

Although the empirical site is the Middle East, rather than the "West", I do not mean to imply homogeneity. This community includes people from across the world, with varied religious, political, and social backgrounds. Countries of origin for speakers include South Korea, Singapore, China, Europe and the US, and conference attendees with a more permanent presence in the region include expatriate workers from South Asia and Europe, as well as immigrants within the region itself (notably Egyptian nationals throughout the GCC, due to proximity and attractive market conditions). While some religious and cultural formulations are nearly always present (such as religious introductions to formal speech used instinctively by many Muslims and sometimes attempted sympathetically by non-Muslim presenters), there are as many moments which present a different set of cultural and linguistic associations and hierarchies, such as native Arabic speakers who find it easier to switch into English to present on technical cybersecurity topics.

Nonetheless, my own profile as a white male and a native English speaker with working Arabic proficiency was important. I was quickly put into specific categories—consultant, guest speaker—by my interlocutors, and treated in a way which would have changed had my gender, ethnicity, or language been different. I wore a badge accurately describing me as a member of the University of Oxford, which also had a significant impact on my reception. As a recognisable label with extensive social and academic associations, "Oxford" both increased my acceptance and made it suspicious: as one interlocutor mentioned, pointing out Oxford University's connection to the UK intelligence community, "they don't know who you are, you come from a country with a bad history in these things, they don't know what you will do with the information".

Acknowledgments

I thank the UK Economic Social Research Council and the University of Oxford for funding this research, and the

members of the Cyber Studies Programme and Centre for Technology and Global Affairs at the University of Oxford for their stimulating conversations on the issues in this article.

Conflict of Interests

The author declares no conflict of interests.

References

(ISC)^2. (2015, April 17). *Workforce shortfall due to hiring difficulties despite rising salaries, increased budgets and high job satisfaction rate. (ISC)^2*. Retrieved from http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html

Alexander, J. (2014). *Promoting security imaginaries: An analysis of the market for everyday security solutions* (Doctoral dissertation). University of Manchester. Manchester, UK.

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), 110–123.

Behar, R. (2016, May 11). Inside Israel's secret startup machine. *Forbes*. Retrieved from https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#6c3400ca1a51

Bell, C. (2009). *Ritual: Perspectives and dimensions, revised edition*. New York, NY: Oxford University Press.

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

Bonine, M. E., Amanat, A., & Gasper, M. E. (Eds.). (2011). *Is there a Middle East? The evolution of a geopolitical concept*. Stanford, CA: Stanford University Press.

Bueger, C. (2014). From expert communities to epistemic arrangements: Situating expertise in International Relations. In M. Mayer, M. Carpes, & R. Knoblich (Eds.), *The global politics of science and technology* (Vol. 1, pp. 39–54). Heidelberg: Springer Verlag GmbH.

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

Caspit, B. (2016, February 29). The Israeli–Egyptian love affair. *The Washington PAC*. Retrieved from http://www.washingtonpac.com/Articles%20of%20Interest/israeli_egyptian_love_affair.htm

Coleman, G. (2010). The hacker conference: A ritual condensation and celebration of a lifeworld. *Anthropological Quarterly*, *83*(1), 47–72.

Cross, M. K. D. (2013). Rethinking epistemic communities twenty years later. *Review of International Studies*, *39*(1), 137–160.

Dalek, J., Deibert, R. J., McKune, S., Gill, P., & Senft, A. (2015, October 21). Information controls during military operations: The case of Yemen. *Citizen Lab*. Retrieved from https://citizenlab.ca/2015/10/information-controls-military-operations-yemen

Deibert, R. J., & Rohozinski, R. (2011, March 28). The new cyber military-industrial complex. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990

Donaghy, R. (2015, February 28). Falcon eye: The Israeli-installed mass civil surveillance system of Abu Dhabi. *Middle East Eye*. Retrieved from http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769

Dunn Cavelty, M. (2008). *Cyber-security and threat politics*. London and New York, NY: Routledge.

Ensor, C. (2017, July 26). Building the cyber security body of knowledge. *National Cyber Security Centre*. Retrieved from https://www.ncsc.gov.uk/blog-post/building-cyber-security-body-knowledge-0

Falzon, M.-A. (Ed.). (2009). *Multi-sited ethnography: Theory, praxis and locality in contemporary research*. Farnham and Burlington, VT: Routledge.

Grimes, R. L. (2006). *Rite out of place: Ritual, media, and the arts*. Oxford and New York, NY: Oxford University Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Held, D., & Ulrichsen, K. (Eds.). (2011). *The transformation of the Gulf: Politics, economics and the global order*. Abingdon, Oxon, and New York, NY: Routledge.

Howard, P. N. (2002). Network ethnography and the hypermedia organization: New media, new organizations, new methods. *New Media & Society*, *4*(4), 550–574.

Intel Security. (2016). *Hacking the skills shortage: A study of the international shortage in cybersecurity skills*. Washington, DC: Centre for Strategic and International Studies.

Isaacson, W. (2015). *Innovators: How a group of inventors, hackers, geniuses and geeks created the digital revolution*. New York, NY: Simon & Schuster.

ISACA. (2016, January). *2016 cybersecurity skills gap. Cybersecurity nexus*. Retrieved from https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

Kennedy, D. (2016). *A world of struggle: How power, law, and expertise shape global political economy*. Princeton, NJ: Princeton University Press.

Latour, B. (2010). *On the modern cult of the factish gods*. Durham NC, and London: Duke University Press Books.

Lee, R. M., & Rid, T. (2014). OMG cyber! *The RUSI Journal*, *159*(5), 4–12.

Marczak, B., & Scott-Railton, J. (2016, August 24). The million dollar dissident: NSO group's iPhone Zero-days used against a UAE human rights defender. *Citizen Lab*. Retrieved from https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae

Matthiesen, T. (2013). *Sectarian Gulf: Bahrain, Saudi Arabia and the Arab Spring that wasn't*. Stanford, CA: Stanford University Press.

Pironti, J. (2013, January 15). The changing role of security professionals. *Info Security*. Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-changing-role-of-security-professionals

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber gurus'. *Government Information Quarterly*, *32*(2), 108–117.

Rappaport, R. A. (1999). *Ritual and religion in the making of humanity*. Cambridge: Cambridge University Press.

Schatz, E. (Ed.). (2009). *Political ethnography: What immersion contributes to the study of power*. Chicago, IL, and London: University of Chicago Press.

Seabrooke, L. (2014). Epistemic arbitrage: Transnational professional knowledge in action. *Journal of Professions and Organization*, *1*(1), 49–64.

Shires, J. (in press). Cybersecurity governance in the GCC. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity governance*. Hoboken, NJ: Wiley-Blackwell.

Shires, J., & Smeets, M. (2017, December). *Contesting 'cyber'*. Washington, DC: New America Foundation.

Stevens, T. (2012, March 27). Norms, epistemic communities and the global cyber security assemblage. *E-International Relations*. Retrieved from http://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage

Stevens, T. (2015). *Cyber security and the politics of time*. Cambridge: Cambridge University Press.

Stewart, P. J., & Strathern, A. (2014). *Ritual: Key concepts in religion*. London and New York, NY: Bloomsbury Academic.

Sundaram, A. (2017, March 20). Security certifications are useless, right? *Info Security*. Retrieved from https://www.infosecurity-magazine.com/news-features/security-certifications-useless

Sundaramurthy, S. C., Case, J., Truong, T., Zomlot, L., & Hoffmann, M. (2014). A tale of three security operation centers. In R. Biddle & B. Chu (Eds.), *Proceedings of the 2014 ACM workshop on security information workers* (pp. 43–50). New York, NY: ACM.

Turner, V. (1977). Variations on a theme of liminality. In S. F. Moore & B. G. Myerhoff (Eds.), *Secular ritual* (pp. 36–52). Assen: Van Gorcum.

UK HMGovernment. (2014). *Cyber security skills: Business perspectives and government's next steps*. London: Department for Business Innovation and Skills.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46.

Wedeen, L. (2010). Reflections on ethnographic work in political science. *Annual Review of Political Science*, *13*(1), 255–272.

Wolff, J. (2016, April 14). Why computer science programs don't require cybersecurity classes. *Slate*. Retrieved from http://www.slate.com/articles/technology/future_tense/2016/04/why_computer_science_programs_don_t_require_cybersecurity_classes.html

About the Author

James Shires is a DPhil candidate in International Relations and a Research Affiliate at the Centre for Technology and Global Affairs, at the Department of Politics and International Relations, University of Oxford. He has an MSc in Global Governance and Public Policy from Birkbeck College, University of London, a BA in Philosophy from the University of Cambridge.

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 41–48
DOI: 10.17645/pag.v6i2.1333

Article

Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen

Lizzie Coles-Kemp [1,*], Debi Ashenden [2] and Kieron O'Hara [3]

[1] Information Security Group, Royal Holloway University of London, Egham, TW20 0EX, UK;
E-Mail: lizzie.coles-kemp@rhul.ac.uk
[2] School of Computing, University of Portsmouth, Portsmouth, PO1 2UP, UK; E-Mail: debi.ashenden@port.ac.uk
[3] Electronics & Computer Science, University of Southampton, Southampton, SO17 1BJ, UK; E-Mail: kmo@ecs.soton.ac.uk

* Corresponding author

Submitted: 30 December 2017 | Accepted: 7 March 2018 | Published: 11 June 2018

Abstract
Assumptions are made by government and technology providers about the power relationships that shape the use of technological security controls and the norms under which technology usage occurs. We present a case study carried out in the North East of England that examined how a community might work together using a digital information sharing platform to respond to the pressures of welfare policy change. We describe an inductive consideration of this highly local case study before reviewing it in the light of broader security theory. By taking this approach we problematise the tendency of the state to focus on the security of technology at the expense of the security of the citizen. From insights gained from the case study and the subsequent literature review, we conclude that there are three main absences not addressed by the current designs of cybersecurity architectures. These are absences of: consensus as to whose security is being addressed, evidence of equivalence between the mechanisms that control behaviour, and two-way legibility. We argue that by addressing these absences the foundations of trust and collaboration can be built which are necessary for effective cybersecurity. Our consideration of the case study within the context of sovereignty indicates that the design of the cybersecurity architecture and its concomitant service design has a significant bearing on the social contract between citizen and state. By taking this novel perspective new directions emerge for the understanding of the effectiveness of cybersecurity technologies.

Keywords
cybersecurity; cyberspace; power; social contract; sovereignty

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

Assumptions are made by government and technology providers about the power relationships that shape the use of technological security controls, and about the norms under which technology usage occurs. These assumptions are coloured by notions of sovereignty and the importance of not only protecting boundaries (including national borders) in whatever space they manifest themselves (digital or otherwise) but also in demonstrating the exclusive control that legitimizes the existence and the authority of the state. In this article, we present a case study that examined how a community might work together using a digital information sharing platform to respond to the pressures of welfare policy change. Insights gained from this case study cast light on the relationships between the security of the digital infrastructure and the security of the people using that infrastructure *as they perceive it*. Contrary to the typical start point for the security of such a platform, which

might best be described as controls to protect the data and the technologies, the community start point was to build networks of trust and collaboration into which the digital sharing technologies could be productively deployed. Our conclusions are that whereas theories of security focus on the relationships between the political, the social, the economic and the technological, the application of cybersecurity controls is often focused on the technical or physical protection of the digital infrastructure, thereby missing the social part of the sociotechnical security system.

The case study leads us to question the sufficiency of the security focus on the protection of the data and the digital technologies, turning to security theory, stemming from Hobbes and also the work of Mark Neocleous (2008), for possible explanations of the apparent gap between the state's use of cybersecurity technologies and the security needs of citizens. Cybersecurity research focuses primarily on the "cyber" part of "cybersecurity", with the unfortunate consequence that the security concerns of the citizen are literally invisible to it. We argue that by locating cybersecurity issues within a broader security literature that takes into account the need to respond to human *insecurities*, new directions emerge for the understanding of the effectiveness of cybersecurity technologies. When, on the other hand, we neglect the citizen-centric view, the security implications of digital service delivery are obscured.

From the case study insights and the subsequent literature review, we conclude that there are three main absences not addressed by the current designs of cybersecurity architectures. We argue that by addressing these absences, the foundations of trust and collaboration can be built which are necessary for effective cybersecurity:

- *Lack of consensus as to whose security is being addressed:* in order for security to work to the public benefit, it is apparent that citizens need to feel secure as a result of its operation. If they do not, then they take security into their own hands, which might increase their local security at the cost of undermining their ability to cooperate with outsiders. Therefore, concentrating on the security and well-being of its citizens is also for the benefit of the state;
- *Lack of evidence of equivalence between the mechanisms that control behaviour:* we argue that when designing a digital service, a control is not independent of the medium used to implement it and a change in medium changes some of the qualities of the control, leading to changes in its effectiveness. For example, when we replace socially-based controls with technology we lose a whole layer of communicative structures when certain options are simply "greyed out" online;
- *One-way legibility:* the state has a need to make the citizen readable by its standardised processes (Scott, 1998) but no corresponding imperative to make itself or its systems legible to the citizen. However, it is apparent that this lack of legibility makes the citizen feel insecure—particularly when the citizen feels that the state views it as the threat.

We first present an inductive consideration of a highly local case study. Whilst such a case study does not of course allow us to generalise the findings, it does compel us to problematise the focus on the security of the technology at the expense of the security of the citizen. We will then consider the contribution that theorising about social, economic and political security can make to the design of cybersecurity technologies.

2. A Community Information Sharing Platform: A Case Study

Our case study took place in the North East of England, in a community suffering the effects of long-term unemployment and degrading social, physical and political infrastructure. Researchers and an arts organisation, Proboscis, worked together to support a community group in the design of an information sharing system that would help their community respond to challenges associated with welfare change.

The community group wanted to develop a system of information sharing that used digital technologies to enhance their capabilities to respond to welfare system changes and provide community support for job seeking, debt management, housing and tenancy advice and benefit claiming. The research team wanted to observe how such a community might design this type of information sharing system as a means to better understand individual and community securities. The research centred on two questions: (i) Which everyday issues become most pressing due to changes in welfare rules and the move to digital welfare delivery? (ii) How might communities work together to alleviate those pressures?

When designing the case study, researchers wanted to develop an empowering space in which participants could reflect on and design for the types of support that would help them and where the interactions between the research team and participants were transparent. Accordingly, the research design was grounded in participatory design principles (e.g. Coles-Kemp & Ashenden, 2012; Vines, Clarke, Wright, McCarthy, & Olivier, 2013) that encouraged participants to co-design the research questions, to influence the design of the data gathering methods and to actively reflect on and contribute to the presentation of the research findings. Following the community participatory engagement principles set out by Coles-Kemp and Ashenden (2012), the research took place in a community centre which was a familiar space for the participants, the research focus was shaped in partnership with the participants, the data gathering methods were adapted to fit with the participant groups and, to nurture a sense of empowerment and agency,

participants were encouraged to consider community responses to the issues identified. Such an anthropologically informed design approach is particularly appropriate for design projects that produce outputs that are to be embedded and sustained within community practices. The case study acted as a provocation for us as researchers by encouraging us to think about security theory in relation to the use of technological cybersecurity controls.

Five focus groups were carried out each with between 4 and 8 participants. In the initial group, the participants were asked to articulate the range of economic, emotional and administrative pressures that they experienced as part of everyday life. Such pressures shed light on the conditions under which interaction with state services might occur and the challenges such pressures present for conformant use of digital state services. In line with participatory design philosophy, the research method used in this initial session was a simple storytelling method which encouraged participants to describe the pressures experienced in different scenarios. The second focus group further deepened the researchers' understanding of these pressures using story telling together with an icon-library to help participants build up a visual and lexical vocabulary of pressures and their responses. For the third focus group, story sheets were developed that were used to systematically capture the pressures, the needs for information sharing and possible community responses. This enabled a wider, more systematic gathering of the issues and ideas for potential community responses and support. The fourth and fifth focus groups used a refined version of this story gathering process until the principles for community support had been developed. The focus groups were recorded, transcripts produced and analysed using thematic analysis before the results were then presented to the wider community for consultation.

2.1. Results and Discussion

The strongest theme to emerge from the data analysis was that of citizen insecurity and precarity. The data illustrated the ways in which the interactions with the welfare systems generated feelings of insecurity for the individual. For example, participants felt that they were not able to question or negotiate with the system and yet experienced heavy penalties for making errors. As one participant pointed out, "If you are underpaid, you don't get it back. If you are overpaid they expect you to pay it back". Participants highlighted that the problems they experienced were due to the complexity of the system and the constant rolling programme of changes. The data from the first focus group showed that participants experienced many such pressures on a day-to-day basis that were exacerbated by the mechanisms used to interact with the system. At the same time, finding ways to work outside the system was also difficult. As another participant commented, "The self-help route is fraught with problems". This insight led us to reflect on how interaction with systems connects to an individual's feelings of security and insecurity that operate at a deeper level than is assumed by the presence (or absence) of technical security controls.

Analysis of the transcripts from the first and second focus groups demonstrated how technology is conceptualised as being interwoven with human social networks and does not operate as a replacement for them. This socio-technological enmeshing connects security technologies to the human networks in which they operate, such that as one participant commented, "It was better when you could see someone face to face. It was better when you could phone for an appointment". Not only was technology not seen as a viable alternative for human interaction, these focus groups highlighted that human networks help to overcome the fear of engaging, as one participant confessed that when reporting to a change in status it, "took me nearly 18 months to phone the Council". This led us to think about in what ways the design of a system that operates within human social networks might increase trust and confidence in working with that system.

Analysis of the data from the first two focus groups shows that receiving understandable information about welfare changes from trusted sources was an important means of reducing anxieties, thereby increasing the feeling of security. For these participants, the information you share and how you use it depends on your values and morals as well as your individual circumstances. As one participant said, "it's a lot to do with your priorities". This is an element that digital service design fails to make allowances for—individuals have different priorities in their lives and therefore have different positions on what constitutes security. One participant in the third focus group told the following story of how she had recently lost her job: "The senior that was on, didn't like us because she was me ex's wife. She hated us and grassed us up for everything. But I should have grassed her up first because she was drinking on the job….But you cannot do that". This story highlights that values and morals shape what information is shared, and how it is used. Yet digital services assume an "idealised", "abstract" or "model" individual interacting with systems and such abstractions often lack ecological validity—a "cultural disconnect" in which system designers illegitimately assume that system users share similar characteristics to a dominant social type, able, for example, to manage passwords, absorb complex instructions and adapt easily to change (King & Crewe, 2013). In such models attitudes and behaviours appear predictable and the state assumes that it understands, and can make sense of, its citizens. This insight led us to think about the importance of different types of legibility and how the design of systems needs to be able to adjust to different patterns of information sharing and protection.

2.2. Trust Rather Than Protection: A New Start Point for Security Design

Whilst a Government cybersecurity response is more likely to encompass access control and surveillance, this case study indicates that a community approach is more likely to focus on trust points, crowdsourced trust recommendations and the collaborative use of the community's own resources to dispel abusive behaviour. This understanding of how communities work might well be possessed by those tasked with local delivery of systems, but is typically lacking in the higher echelons of policymakers and system designers, a phenomenon which has been called "operational disconnect" (King & Crewe, 2013).

The types of trust discussed during the study were many and varied, including trust in the quality of the information, trust in the individuals providing the information, trust that the information exchange will help their circumstances and trust that personal details would be kept private. The participants showed that trust in the quality of the information can be engendered through knowledge champions who are seen as having specialist knowledge and are validated through recommendations, through their jobs in related areas, as well as through their track record in providing specialist advice. Trust in the quality of information was further engendered by peer review of information shared within the community.

In the later focus groups, concern for the security and safety of community members who were information providers emerged as a dominant theme. These concerns included liability if the information turned out to be incorrect and concerns for the safety of the provider if they gave information that involved local intelligence about community activities. Of particular concern was information shared about loan sharks and unhelpful or abusive staff who provided state or state-endorsed support. A further concern was the potential for individuals to use the information that was provided to them to defraud the state or other institutions. The third, fourth and fifth focus groups focused on ideas of information sharing to better support each other in responding to the pressures articulated. During this process, several key security concerns were identified: trust in the quality of the information, the safety of the information providers and the potential for manipulation or abuse of the information provided.

These security concerns focus on the close proximal relationships in everyday life. These concerns contrast sharply with the more conventional cybersecurity systems' protection approach that focuses on attackers misusing the system. It suggests an approach to protect citizens who suffer as a result of the lack of information, the flow of false information, the misrouting of information by those who want to abuse the network and the pressures inherent within the context of use. To address these latter concerns, the start point is trust and collaboration rather than a control architecture to protect against attackers and malicious activities.

Our case study insights led us to conclude that a community approach to security might focus on trust points, crowdsourced trust recommendations and the use of the community's own resources to dispel abusive behaviour. From our analysis of focus group data and a comparison of the community response with the typical state approaches to technological control, we focused our attention on the theoretical underpinnings of a security design that speaks to the three absences of security consensus, control equivalence and two-way legibility that we identified above. We conclude that such principles have the potential to encourage a collective notion of cybersecurity and engender positive buy-in and active engagement from citizens, facilitating a genuinely sociotechnical cybersecurity system. We conclude that in the digital by default era, trust between state and citizen is in large part built by developing a cybersecurity model that can (i) adjust to the security needs of the citizen, (ii) that provides a more comprehensive range of security qualities and (iii) is legible to the citizen. We explore these three principles below.

3. The First Absence: The Security of the Citizen

The insights from the case study reflect that security requirements are often conflicting, culturally and morally constructed and both individualistic and communal. To explore how a cybersecurity model might better reflect this, we need to look at the roots of modern conceptualisations of sovereignty. The modern security community theorises sovereignty of cyberspace along the lines of the pioneering conceptualisation of Thomas Hobbes (1588–1679), which still underpins both liberal and conservative theorising of the nature of the state. In particular, Hobbes suggested that sovereignty, to be effective and legitimate, needed to take a particular form, and fulfil particular functions: it was contractual, and co-constructed with (though not co-constituted by) the citizens. People would rationally seek wider protection than they could provide for themselves by surrendering their rights of self-protection to a more powerful sovereign which could protect a community from outsiders and the members of the community from each other, therefore promoting cooperation, trust and other forms of social behaviour. It follows that, if people feel unprotected by the state, then it is reasonable and rational for them to seek protection elsewhere. "The end of obedience is protection" (Hobbes, 1996, p. 152), and therefore if obedience to the state does not give you protection, (i) protection needs to be found elsewhere, and (ii) the duty of obedience evaporates.

We argue that as the state withdraws from in-person contact to digitally-mediated interaction and as digital technology facilitates the types of communication and collaboration that can make possible the diversification of wealth production and gives citizens the option to move between modes of wealth production and social orders, the security relationship between the citizen and

the state needs to be re-negotiated. Such re-negotiation is necessary in the first place because the assets that citizens wish to be secured may not be the same as those identified by the state (or large organisations). Secondly, citizens may value particular types of behaviour or interaction which may be hindered or even prevented by security measures, and which may therefore prompt the use of workarounds which undermine those measures even in their own terms. Because of the co-constructed nature of Hobbesian sovereignty, these are serious problems, because citizens' acceptance of the legitimacy of the sovereign (i.e. in the modern world, the state) depends crucially on their own perceptions that it serves their security needs. It follows that if the sovereign opts to define the types of security it will provide on the winner-takes-all model, it must either persuade citizens that these are the types of security they value, or sacrifice legitimacy. If it fails to engage with the citizenry upon matters of security, then it has to expect the citizenry to have an antagonistic attitude, resulting in the only option being to rule by force, treating its own citizens as the enemy. The insights from the case study indicate that an alternative means of overcoming this potential for antagonistic outcome is to situate Digital by Default (DBD) services within existing networks and embed the services through a more robust security control equivalence and through system legibility, thus both increasing trust and creating spaces in which conflicts and differences can be resolved.

4. The Second Absence: Equivalent Methods of Control

The case study data indicate many frustrations with the control mechanisms deployed in the various state systems. For the citizenry to align with the state's model of security, the controls have to afford security to the citizen. Yeung (2011) talks about the bond of trust between the state and the community it governs pointing out that, "small erosions may lead to its long-term degradation" (p. 25). One of the reasons that trust may erode is that the principles of control and the related principles of security remain the same but the mechanisms for operationalising them differ. Digital controls do not necessarily carry the same signals of trustworthiness, legitimacy, openness to negotiation, and ability to reconcile different interpretations of security within a single transaction as socially-grounded forms of the same control principle.

Lessig's (1999) socioeconomic theory of behaviour constraint argues that regulation (in the widest sense) can happen through four mechanisms—the law, social norms, economic incentives and architecture. Taking this view, digital technology and sovereignty have been game-changers for the state. Previously, the state had monopoly control only over the law, and so that was its main interface for citizen control. Now, it can alter the *architecture* of its interactions with the citizen in order to make certain behaviours more likely while ruling others out (and it can also gather the data to evaluate and refine its strategies in real time). It follows that it can achieve its goals stealthily by adjusting the architecture of interaction, rather than by commanding and punishing; this is the basis of 'nudge' philosophy (Thaler & Sunstein, 2008).

This theory has much plausibility, but it has intentionally or otherwise led to the fallacious corollary, that, because control can be exercised through any one of these four mechanisms, the mechanisms are *interchangeable* for a given piece of control (Hildebrandt, 2015). In other words, if some type of behaviour is prevented through, say, a legal restriction, the control mechanism can be changed to, say, a constraint on the digital architecture, while leaving everything else untouched. Indeed, one of the myths underpinning the DBD strategy for citizen-state interaction is that the easiest way to do this is through techno-regulation which Yeung defines as a reliance on embedding regulation in technology design rather than relying on the law to regulate. Yet this is fallacious for two reasons that are relevant to our own inquiry.

First, the four mechanisms have very different properties. Techno-regulation uses the architecture of systems to enforce control. Yeung (2011) suggests that, "it is the action-forcing character of techno-regulation that makes it a particularly powerful form of control" (p. 4) and goes on to make the point that this way of regulating human activity in cyberspace has negative "implications for liberty, autonomy and responsibility". Compare the use of law to constrain behaviour with the use of architecture. Law has three properties that digital architecture does not have. Firstly, one can disobey the law. There are consequences if one does, but one can (and people often do). This is an important source of freedom—consider civil disobedience—which is not replicated by a technical architecture. Secondly, law can be challenged within the law; one can take one's case to higher courts. Architecture does not admit legitimate challenge (although it can be illegitimately hacked). Thirdly, law needs a certain legitimacy to operate—it is at least in part created, in a democracy, by a legislature that can be voted out by the citizens it binds. Software (even open source), on the other hand, is created by small expert cliques accountable to no-one but themselves. Economic incentives can also be subsumed by the architecture of a digital system. In our case study, participants gave examples of how failure to engage with the system on its own terms resulted in financial punishment by being underpaid or overpaid and then expected to pay it back.

The case study indicates that citizens can choose not to engage with these incentives and may well prefer informal economic activities that are outside the control of the state and bypass the digital system. Some of the social norms that sit around these informal economic activities emerge from our focus group community. Not only does each of these constraint mechanisms have different properties but the state is more likely to focus on hard controls such as the law, architecture of the system and economic incentives rather than attempt to tackle

social norms and yet this mechanism emerged from the case study as the most important factor in developing trust and security through protection of the community and its members. In other words, when we switch focus from the security of digital or financial assets to the kinds of security that matter to the citizen, we see that the hard constraints are more likely to produce insecurity than security, and consequently that the ideal of a co-constructed sociotechnical security architecture in this context fractures into a set of government controls designed to counter community resistance.

The second reason is that the nature of the constraints in question is more complex than Lessig's simple picture suggests. Perhaps most importantly, pre-DBD, the citizen might have spent time talking to a representative of the state who almost unconsciously performed the vital communicative function of explaining the assumed responsibilities of the citizen. This is a very rich interaction of the citizen with not only a monolithic state, but its human representatives and also various other actors in the same society. The digital architecture wishes most of this away, and replaces it with an input/output function where the claimant identifies himself in terms meaningless to him, but that the state recognises (e.g. a biometric or a password), and then transfers resources once it has verified entitlement. No conversation, explanation or human interaction is needed from the architecture's point of view. This is not merely a change in interaction style but a removal of fundamental and necessary qualities of security control. By contrast, the case study reflects the importance of communication, interaction and the negotiation of responsibilities that are preconditions to the successful operation of a system.

5. The Third Absence: Legibility of the State to the Citizen

The illegibility of the state systems appears as a clear source of mistrust for our focus group participants. The technologies of cybersecurity are built on a particular type of mathematical abstraction away from the everyday, "embodied situated experience" (Cohen, 2007, p. 213) of individuals, reducing visibility of the fluidity that digital technologies both enable and encourage (Bauman, 2013). However, reducing its visibility does not remove it. Scott (1998) has described the processes by which the state reduces complexity, by rendering its citizens and their lifeworlds legible to administrative order. This goes against typical living practices that are legible for citizens, that are local, interested, contextual and historically specific (Scott, 1998) and that make sense in the particular circumstances of citizens' lives. For the state to intervene effectively, either to appropriate resources, to control behaviour, or to manipulate behaviour, it has to abstract away from all these factors to produce national, homogeneous, uniform standards. State simplification produces descriptions of communities that are usually: (i) related only to the state's interests (in taxing, providing services, providing security, etc.), (ii) written facts, numerical or verbal, (iii) static facts, snapshots rather than ongoing processes, (iv) aggregate facts about groups and averages, rather than about individuals per se, and (v) standardised, based on categories that bracket citizens together, no matter how unique their circumstances (Scott, 1998).

In the end, such an understanding engenders incentives for people to abridge their own practice in order to be legible by the state—for instance, an unemployed person on welfare might be better off working casually in the informal economy, but the state recognises only the possibility of formal employment or enforced idleness. Its rules are crafted on this assumption, giving the welfare claimant the choice of forfeiting payments or foregoing informal work. If she forfeits her welfare entitlement, the social safety net is removed from under her, but if she claims welfare and foregoes informal employment she is unable to use her contacts and local knowledge (her social capital) to help support her and her dependents, and work that would benefit the local community is left undone. The state, with its imperative to abstract and simplify, ends up with individuals simplifying their own behaviour deliberately to become legible to the state.

Note also that some commitment to transparency (e.g. the provision of open data) may be necessary for legibility, but cannot be sufficient. Government transparency can only help when what is revealed to citizens is legible to them. A data set in the Resource Description Framework from data.gov.uk will not in itself accomplish this. As our case study insights indicate, rich engagement, and a willingness to discuss and explain, will be of far greater value.

6. Discussion and Conclusion

Sovereignty is the ability of a state to maintain the exclusive power and authority to govern itself, for example by maintaining control of, and managing, citizens within, its borders. Neocleous (2008) argues that social security is an important aspect of this imperative for the state. An effective cybersecurity deployment is essential if the state is to maintain its exclusive authority and a secure DBD policy further bolsters this. Franzese (2009) suggests that sovereignty in cyberspace depends on a state receiving external recognition of its authority and ability to, "exert some measure of control over its own cyberspace" (p. 9), and such authority is under heavy challenge at the time of writing. In the UK, the importance of such recognition to the establishment of sovereignty is encapsulated in the Government aspiration to make the UK the safest place to do business online (UK Government, 2016). Achieving this aim establishes sovereignty in two ways, firstly, through other countries and global businesses engaging in online business with the UK thereby demonstrating their confidence in the control UK Government has over its cyberspace and secondly, through delivering secure Government services to

its citizens, again demonstrating that the Government has the ability to manage its citizens in cyberspace.

Sovereign capability in cyberspace is complex and contested and the projection of sovereignty is demonstrated, at least in part, through state activities around cybersecurity. As Lessig (1999) points out, "real-space sovereigns" (p. 198) will respond to the threat of cyberspace by attempting to ensure that their regulatory power encompasses virtual spaces, and, by framing cyberspace as a spatial domain analogous to land, sea and air (Murphy, 2010), will conceptualise the control and management of cyberspace through cybersecurity. This Westphalian model is traditionally framed as being threatened by hacking causing the disruption of democratic processes by foreign powers, and by attempts to copy or take control of data assets of UK businesses and individuals. However, our case study gives us cause to reflect that civil disobedience stemming from the undermining of the social contract between citizen and state is also a potential significant threat to domestic sovereignty. In the era of DBD, civil disobedience can result in non-compliance with cybersecurity controls and rejection of social policies and programmes as the citizen feels forced to focus on their own security at the expense of making positive and creative contributions to the state.

Neocleous (2008) makes a powerful argument for social security to be considered an integral part of a nation's security policy as its function is the maintenance of social and economic order. If considered from this perspective, cybersecurity technologies of passwords, file permissions, encryption and firewalls are digital means of fulfilling this mission of order and containment. These security technologies are core to DBD and embody a particular security philosophy. The case study participants, however, focus on a different security mission, of mutual support and information sharing. This mission addresses the challenges of human insecurities rather than the frailties of a system of order and rendering legible. These security missions are not mutually exclusive, but each responds to a different type of insecurity.

In the context of Neocleous' argument about domestic containment (2008), DBD makes cyberspace central to the question of domestic sovereignty and this makes cybersecurity and its control framework a central part of domestic policy initiatives. The current security model for DBD focuses on the protection of the data and the technology with the assumption that this will also provide security for the citizen. By contrast, our case study shows that the start point for an individual's security is not protection but trust.

Acknowledgements

We'd like to thank the participants who gave their time, creativity and energy to the work of the focus groups. We'd like to thank Proboscis for their support and creative input to the case study. Coles-Kemp's contribution was funded by EPSRC grant ESSfES: Everyday Safety-Security for Everyday Services (grant number EP/N02561X/1). O'Hara's contribution was partially funded by EPSRC grant SOCIAM: The Theory and Practice of Social Machines (grant no. EP/J017728/2).

Conflict of Interests

The authors declare no conflict of interests.

References

Bauman, Z. (2013). *Liquid modernity*. New Jersey, NJ: John Wiley & Sons.

Cohen, J. E. (2007). Cyberspace as/and space. *Columbia Law Review*, *107*, 210–256.

Coles-Kemp, L., & Ashenden, D. (2012). Community-centric engagement: Lessons learned from privacy awareness intervention design. In S. Faily, I. Fléchais, & L. Coles-Kemp (Eds.), *Proceedings of HCI 2012 the 26th BCS conference on human computer interaction* (pp. 1–4). Retrieved from https://ewic.bcs.org/content/ConWebDoc/48813

Franzese, P. W. (2009). Sovereignty in cyberspace: Can it exist? *Air Force Law Review*, *64*, 1–42.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Cheltenham: Edward Elgar Publishing.

Hobbes, T. (1996). *Leviathan*. Cambridge: Cambridge University Press.

King, A., & Crewe, I. (2013). *The blunders of our governments*. London: Oneworld Publications.

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

Murphy, M. (2010, July 1). Cyberwar: War in the fifth domain. *Economist*. Retrieved from http://www.economist.com/node/16478792

Neocleous, M. (2008). *Critique of security*. Edinburgh: Edinburgh University Press.

Scott, J. C. (1998). *Seeing like a State: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.

Thaler, R. H., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New York, NY: Penguin.

UK Government. (2016). *UK National cyber security strategy 2016–2021*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Vines, J., Clarke, R., Wright, P., McCarthy, J., & Olivier, P. (2013). Configuring participation: On how we involve people in design. In S. Bødker, S. Brewster, P. Baudisch, M. Beaudouin-Lafon, & W. E. Mackay (Eds.), *Proceedings of the SIGCHI ACM conference on human factors in computing systems* (pp. 429–438). Paris: ACM.

Yeung, K., (2011). Can we employ design-based regulation while avoiding brave new world? *Law, Innovation and Technology*, *3*(1), 1–29.

About the Authors

Lizzie Coles-Kemp is Professor of Information Security at Royal Holloway University of London. She is a qualitative researcher who uses creative engagement methods to explore everyday practices of information production, protection, circulation, curation and consumption within and between communities. Lizzie's focus is the intersections between relational security practices and technological security and she specialises in public and community service design and consumption. She is currently an EPSRC research fellow with a research programme in everyday security.

Debi Ashenden is Professor of Cyber Security in the School of Computing at the University of Portsmouth. She is also the Programme Director for Protective Security & Risk at the Centre for Research & Evidence for Security Threats (CREST). Debi's research interests are in the social and behavioural aspects of cyber security—particularly in finding ways of "patching with people" rather than technology. She focuses on building security dialogues between communities.

Kieron O'Hara is an associate professor in electronics and computer science at the University of Southampton, and visiting professor in law at the University of Winchester. His interests are the political implications of technology, particularly the World Wide Web, AI and big data, with a focus on privacy, trust, openness and ethics. His book *The Anonymisation Decision-Making Framework* (co-written with Mark Elliot, Elaine Mackey and Caroline Tudor) is a practical guide to data anonymisation.

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 49–60
DOI: 10.17645/pag.v6i2.1368

Article

How We Stopped Worrying about Cyber Doom and Started Collecting Data

Brandon Valeriano [1,*] and Ryan C. Maness [2]

[1] Donald Bren Chair of Armed Politics, Marine Corps University, Quantico, VA 22134, USA; E-Mail: drbvaler@gmail.com
[2] Defense Analysis Department, Naval Postgraduate School, Monterey, CA 93943, USA; E-Mail: rmaness@nps.edu

* Corresponding author

Submitted: 17 January 2017 | Accepted: 12 March 2018 | Published: 11 June 2018

Abstract
Moderate and measured takes on cyber security threats are swamped by the recent flood of research and policy positions in the cyber research field offering hyperbolic perspectives based on limited observations. This skewed perspective suggests constant cyber disasters that are confronting humanity constantly. The general tone of the debate argues that cyber war is already upon us and our future will only witness more cyber doom. However, these hyperbolic perspectives are being countered by empirical investigations that produce the opposite of what is to be expected. It is generally observed that limited cyber engagements throughout the geopolitical system are the dominant form of interaction. Our task here is to offer a different path forward. We first posit what can be known about cyber security interactions with data as well as what cannot. Where is the water's edge in cyber security research? We then examine the known works in the field that utilize data and evidence to examine cyber security processes. Finally, we conclude with an offering of what types of studies need to be done in the future to move the field forward, away from the prognostication and generalizations so typical in the discourse in this constantly changing and growing field.

Keywords
cyber conflict; cyber security; cyber strategy; data collection; quantitative methods

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. The Challenge of Cyber Security Threat Data

Beginning in 2014, various news organizations began reporting on a particular cyber security firm, Norse Corporation, and their active cyber threat map (Walker, 2015). *Mashable* noted in 2016 that "the global cyber war is raging on, and this mesmerizing map shows just how serious it has become" (Gallucci, 2016). The map is dynamic, colorful, and gets the point across quickly, a criterion for any decent visualization of data. As late of August 2017, the Defense Intelligence Agency (DIA) tweeted out a link and photo of the threat maps suggesting it represented ongoing cyber-attacks (DIA, 2017). Yet this map is not a very clear representation of any real threats that nation-states face on a daily basis.

Unfortunately, the Norse cyber threat map does not represent active threat data, but attacks, likely by bots, on preset honeypots. Honeypots are a method of providing data on fake targets to either distract the opposition from the real targets or to deter an aggressor from attacking in the first place (Gartzke & Lindsay, 2015). While sometimes a useful method to gather threat intelligence if presented a sleight of hand for an attractive target, honeypots as reported in popular discourse are not exactly an accurate representation of the cyber threat landscape. In this case, the goal was to demonstrate the ability to track global attacks to gain interest in the company and promote its capabilities.

Nearly all active threat maps either present data tracking honeypots and various bot networks that are de-

void of human agency, simply presenting what is in fact fake data. Active representation of the threat landscape is the goal, but the reality is that the picture of the cyber security threat landscape we currently have is incomplete, misleading, or outright fake.

High profile data breaches have been consuming media narratives for at least a decade. With each act of cyber disruption or espionage, pundits as well as government officials and several academics declare that cyberwarfare is upon us, is the future of warfare, and it is only a matter of time before a "Cyber Pearl Harbor" wreaks havoc on the American homeland (Gurdus, 2016). With this new revolution in military affairs, the battlefield, according to some, is forever changed and the next big war could very well be a cyberwar (Clarke & Knake, 2010; Kello, 2013). Politicians, pundits, and practitioners have jumped on this doomsday narrative and have promoted cyber arms races, offensive advantage, and deterrence strategies to stay one step ahead of would be adversaries in order to prevent them from infiltrating networks out of fear of massive retaliation. These revolutionists point to acts such as Stuxnet, Shamoon, Sony, and the Office of Personal Management (OPM) hack as the new norm of conflict between states, and that the US is losing ground with every tolerated cyber-attack on American networks.

This illustration points out the need for reliable collected data on cyber incidents between entities to challenge threat inflation. Empirical evidence and inferences with data from the academic community can help serve policy makers in constructing policies that help in developing proper normative behavior from states.

The challenge of collecting cyber security data runs right up against the difficult reality of collecting information on active threat interactions in real time. The process is difficult, complicated, and prone to error, but not impossible. Researchers need to be clear that there is an imperative to collect data on all forms of conflict and no domain presents easy opportunities for data collection. Scholars and activists alike are still trying to sort through casualty data in Syria (Black, 2016). Human Rights Watch (2017) data is likely prone to reporting bias reflected by an increased interest in human rights abuses through time.

The impediment for cyber security can be considered even more challenging. While interest in cyber security interactions is increasing, bringing with it elevated reporting of cyber breaches, there remains a greater problem. In a domain thought to be mostly secret, how do you collect data on what most of the population assumes is uncollectable and mainly classified? Why even seek to overcome this challenge, given the high degree of difficulty? In this article, we will review why the need to collect data on cyber security interactions, how the process can be conducted and is not only possible but happening, highlight ongoing attempts to empirically assess the cyber security complex.

2. The Need for Cyber Security Data

Moderate and measured takes on cyber security issues that intersect with policy and international relations issues can be out of place amongst the recent flood of research and policy positions in the cyber conflict and security field. The general tone of the debate suggests that cyber war is here, it is our present, and it will be our future. One gets millions of hits if "Cyber Pearl Harbor" is Googled (Lawson & Middleton, 2016). The basic assumption is that our future military, diplomatic, and economic history will involve the use of computers as the main avenue of attack and defense because these technologies are not only transformative, but also cheap and easy.

Cyber strategies and tactics are like any other technological development. At first, new technologies suggest immense possibilities and promise to give states an edge, yet the reality is that technological advances rarely change the face of the battlefield, either in the diplomatic, economic, or military realm. New technologies can be used to defeat specific threats or defenses, such as the tank helping break the stalemate of the trenches in World War I; but are often limited in other contexts. Tanks need to be supported by infantry and logistical teams constantly supplying fuel or towing the machines, limiting their effectiveness and reach. cyber strategies will be no different, and they will be just another important piece in the arsenal but not game-changing on their own.

Claims of revolutionary importance are easy to make, and persuasive given certain examples, but there are always countering examples. Vasquez (1991) makes the case that nuclear weapons were not responsible for the long peace during the Cold War, rather the lack of direct territorial disputes between rivals limited devastating war. The important point is that no one example or story tells the complete picture, and for that we need evidence and data to support much of the theory and practice.

Data-focused research can make an important and lasting statement. By looking at the complete landscape of interactions, we can leverage a different view of the evidence and data. No longer does one attack stand out, but the total picture emerges and in cyber security it is a picture of a restrained international system developing a norm against the use of cyber weaponry (Valeriano & Maness, 2015).

We do offer one key caveat. Our focus is mainly on nation-state interactions because they are discussed as the most devastating and dangerous. In reality, collecting data on cyber-crime or digital attacks of civil society is just as important, but ignored in the field. We hope refocus the debate a bit here and help scholars rethink the domain regarding the nation-state seeking to move towards a more holistic view of cyber security as an everyday security issue. By moving beyond the dramatic examples of Stuxnet and the Sony Hack, we can expand the range of possibilities but also expose the limitations inherent in new technologies. These caveats are critical when theorizing about the future use of cyber weaponry.

3. Reality Is a Social Construction

There have been many challenges to the utility of data in international relations. Hedley Bull (1966) long ago argued that data-based analysis was tortuous and inelegant. He also maintained that nothing in data-based examination goes beyond what can be deduced using conventional wisdom. J. David Singer (1969) challenged this presentation as being naïve about the utility and purpose of data. There is a limitation on our ability to understand the world without taking a total snapshot of interactions to make predictions, understand patterns, and examine how outliers may alter our perceptions of interactions. Data can illuminate counterintuitive patterns not readily apparent to the qualitative observer.

Insights from postmodern and critical scholars are imperative to our task. If reality is basically what we make of it (Berger & Luckmann, 1991), what happens when the perspective we construct to deal with nascent threats is divorced from reality? While data and evidence will never be value free, an insight offered by critical theory, it also offers a more nuanced approach to the issue than selecting the obvious cases for examination and extrapolating from outliers. We must start somewhere; the postmodern project is a reaction to the behavioral turn in the social sciences. The cyber security field has to yet to even start its behavioral moment but seems to have started with the suggestion that collecting data is impossible (Kello, 2013).

As Vasquez (1998, p. 218) points out, language and conceptual frameworks are prone to self-fulfilling prophecies. If we allow the language we use to construct how we view security challenges, we likely will miss key developments in the field. Social science is not value-free, but this does not mean that it must be data-free in order to reflect the true state of nature. Language without the consideration of data and evidence will often be empty and akin to Norse's threat map, which is an imperfect and often a misrepresented vision of reality.

Using social science methods can improve the practice of cyber security. "Science is not simply a useful tool, but a practice that creates a mode of life that consciously destroys other ways of thinking and living" (Vasquez, 1998, p. 219). Without encouraging the perspective that data adds to the cyber security debate, we might accept observations as truth when in fact they merely reflect a skewed sample that is not reflective of actual patterns and practice. To encourage better behavior in cyberspace, to stop gross abuses, and to predict future events, we must move beyond biased and constrained samples offered by observational logic that cannot move beyond description and theoretical logic.

For Vasquez (1998), "good" empirical theories should be accurate, falsifiable, have explanatory power, be progressive, be consistent with what is known in other areas, yet also be parsimonious. Theories must pass reasonable tests of fact first. The process of progress inherent in a social science enterprise starts with the collection and analysis of data. Once data is collected, positions and theories can be challenged and falsified in light of evidence. We then can move towards explaining the past, present and future based on the data processes that we observe now.

The key addition of Lakatos (1970) is that for a theory to be progressive, it must obtain more empirical content than the prior theory and generate new and interesting questions. Without a foundation of theory, data and logic, we have no bias on which to proceed with knowledge based inquiries. Cyber security theory is empty without a firm foundation of fact that then pushes us to explore new directions.

Of course, data is always biased by the unit collecting the data and interpreting the evidence. However, this is also a strength of data, others can come along and use it for their own ends and expand upon the original intent of the data to build different perspectives. The basic point is that we need to stop engaging important policy questions through prognostication that would be more suitable on a 2am television advertisement. Political scientists and policymakers should not be fortune tellers who make guesses about the future without reference to what we already know. We have evidence from the recent past and emerging contemporary situation, so we must use it to engage critical policy questions.

4. What We Can and Cannot Know from Data

It is thought that most cyber strategies and events are secret, but this is not entirely true. Much of what happens in cyberspace is the definition of overt—by interacting with external networks, threat actors make their presence known. Attackers may try to mask their origins, but language traits, common techniques and malware, and motive as well as historical context can give us a great deal of information about who is attacking whom. For example, near the beginning of the 2018 Winter Olympic Games in Pyeong Chang, South Korea, the International Olympic Committee (IOC) was hacked and subsequently stolen emails from the organization were released to the public (Matsakis, 2018). Forensic analysis attributes this operation to the Russian Federation, which was the primary culprit from the beginning, as the country had been banned from competition for the games for a massive doping scandal that Moscow vehemently denies guilt to this day. Feeling cheated, the APT 28 Russian hacking group FancyBear, the same group responsible for attacking Democratic Party networks during the 2016 US presidential election, enacted their revenge in the digital realm.

Covert action is "the effort of one government to influence politics, opinions, and events in another state through means that are not attributable to the sponsoring state" (Anderson, 1998, p. 423). Yet in cyber security, the attribution problem is often overstated, what is beyond our ability is constructing real-time data that can be used to charge culprits in the act based on domestic le-

gal standards. Observing malicious cyber behavior is possible but delineating responsibly in a legal sense is quite difficult. Measuring ongoing infiltrations, unknown zero-day threats, and attempts at access that fail are difficult if not impossible to observe. Once an operation achieves a certain level of access, inserts malware into the target, and seeks to coerce the opposition, there are clear observable patterns that can be documented.

In short, there is much we can know about the cyber security domain that can be gleamed from observations. Operating in this landscape as if the threats cannot be known, monitored, and predicted betrays the great advances we have made in doing exactly this. What we cannot do is watch ongoing operations as they occur. This is mainly because organizations might not know they are violated till after this happens, as was the case for the OPM hack (Koerner, 2016). Cyber security companies might operate at a level where they promise a great deal of information, but this is likely to be a promise that cannot be kept. There is clearly a great utility in cyber security data, but we must temper expectations and excitement with collaborative analysis and sobered expectations of the utility of these data-based efforts.

In the cyber security field, we witness all sorts of interactions that can be processed into data. Incidents and events, malware and its spread, vulnerabilities, and social media interactions are all critical elements of the cyber security discourse and represent collectable data samples. Yet, the majority of the cyber security field seems to reject the idea that data collection is possible. This is perplexing in the face of calls to reform the vulnerabilities equities process (VEP), or the process by which threats are communicated by the government to private industry (Newman, 2017). Cyber security data is clearly observable and a part of the news cycle for cyber interactions, but it is generally removed from the political, policy, and military discourse.

Unfortunately, some critics and skeptics believe that collecting data on a subject is synonymous with perfect information about a topic. Data producers have never claimed that their data was complete, total, or absent of bias. These attributes are common for all data enterprises. In the social science world, all data collection enterprises will be incomplete or inaccurate in some way. This does not mean that data projects should be scrapped, but that those who use these projects should understand the limits and possibilities inherent in data collection enterprises.

It must also be made clear that are we are generally speaking of cyber security interactions are they pertain to state-based action. Extending this data-based architecture to criminal interactions would require different theories, data collection methods, and processes. Future efforts should seek to move beyond the state towards examining non-state behavior including criminal interactions.

We can only observe what actually happens rather than what was intended to happen, this is one reason to focus on states where malicious action is to be expected and even admitted at times. It is not exactly an interstate crisis if one state tries to attack another state in cyberspace and fails to be noticed. This is an unobserved process, a tree falling in the woods with no one to witness the fall so to speak. Can there really be a coercive impact if one node in the interaction does not even know there was an interaction?

Scholars must be prepared to go to war with the data we have, not the data we wish we had. There are inherent limitations in the data collection process that make data problematic for many reasons but gathering a wide snapshot of interactions is clearly preferable to observing a single interaction and extrapolating from that data point. That is not data analysis but an exercise in guesswork that has no place in the academic or policy enterprise.

5. Other Data-Focused Efforts in Cyber Security so Far

The Department of Homeland Security (DHS) now has an incident reporting feature (DHS, 2018a) and ongoing efforts to collect data (DHS, 2018b). Without this step, we are operating in known environment needlessly wearing a blindfold. Hopefully this will allow the US to become an open and transparent leader for cyber security data, but this also leaves out the rest of the world in terms of sampling, making it a problem to generate a global sample enabled by the targets.

The United Kingdom's National Cyber Security Strategy proposes data driven solutions to the problem but these efforts are typically clouded by a disagreement on methods and evaluation standards rather that starting first with active threat information collection (UK Government, 2016). The US Office of the Director of National Intelligence (ODNI) office offers a standard of evaluation hoping to generate what they deem as a "Cyber Esperanto" method of data evaluation and coding but fails to articulate a standard by which incidents would be collected (Ackerman, 2017). Generally, the focus on evaluating the phases of attacks rather than starting with a macro sweep of the field.

It is strange that the cyber security domain has restricted itself from understanding the basic contours of the conflict dynamics through the analysis of empirical events. To not take this step is a self-defeating strategy that betrays our standard operating procedures in other military and political domains. The first step is to always understand the behavior of the key threat actors in a domain, however in the cyber security field we seem to think that the adversary is inherently unknowable and without a past, this is an unhelpful conjecture. The first step always seems to develop risk management methods to minimize damage without seeking to understand the goals and past actions of the attacker in the first place.

In academia, Healey and Grindal (2013) make clear strides early on to seek to revive the idea of a disciplinary history of cyber conflict and examine as many cases as

possible. Another excellent example is Lindsay's (2015) listing of prominent Chinese cyber espionage cases. The problem is that these examples of macro-case studies are few and far between. With the exception of Karatzogianni (2012) and Middleton (2017), most studies focus on a few prominent cases like Stuxnet, Shamoon, and Sony, at the expense of the typical behavior and strategies that rival countries exhibit in cyberspace.

The plethora of new emerging data sources of information is heartening, but also reinforces key points we make in *Cyber War Versus Cyber Realities* (Valeriano & Maness, 2015). We have observed restraint in cyber interactions. Escalation is rare (Valeriano, Jensen, & Maness, 2018), and most disputes piggyback on previously known foreign policy conflicts and crises that are well established, often connected to territorial disputes. Schneider (2017) demonstrates that even in the context of wargame scenarios, escalation is rare.

Examining the data on cyber incidents, Pytlak and Mitchell (2016) are able to point out that rivalry intensity does not predict which rivals will engage in cyber conflict. Instead the best predictor is the presence of nuclear weapons. While the possibility of escalation in the context of nuclear weapons is troubling, we also know that empirically, nuclear states can push their negotiations to the edge of war and draw back (Beardsley & Asal, 2009). Mauslein (2014) also demonstrates empirically that rival states are less likely to engage in cyber conflict due to escalation risks which counters the early idea that rival states would be primary testing ground for cyber disputes (Valeriano & Maness, 2012).

Understanding the impact of cyber confrontations appears to be the next key challenge. In an examination of 1,841 cyber events from 2013 to 2016 in Ukraine, Kostyuk and Zhukov (2017) demonstrate that cyber actions had no discernible impact on battlefield events. Narrowing down on fighting between 2014 and 2015, the authors find no escalatory patterns in the cyber data, but conventional attacks do result in corresponding reprisals. While this study represents a small selection of battlefield events in Ukraine, there does appear to be a pattern emerging. Evidence from a case study on Syria finds many of the same patterns as in the Ukraine case. Valeriano et al. (2018) produce a macro level view of the impact of cyber strategies suggesting that only 5% of the 192 incidents coded produce a describe change in behavior in the target. What is more important is that these events demonstrate no clear escalatory pattern. Cyber strategies, even intensely invasive ones that seek to degrade networks and systems, neither appear to compel the adversary nor do they produce the escalation risks often hypothesized by scholars such as Buchanan (2016).

The Axelrod and Iliev (2014) formal model is another useful examination of the utility of cyber conflict. They note that actors with a high degree of stealth have a lower likelihood of utilizing a cyber weapon because the utility of the weapon does not decline through time (it is unlikely to be discovered). They also note that gain is a key consideration, a state will only use a cyber weapon if there is a gain to be made. The studies by Valeriano et al. (2018) and Kostyuk and Zhukov (2017) suggest that gains are rare therefore the Axelrod and Iliev (2014) formal model would predict a low instance of cyber conflict when the consideration of effects and gains are added.

A novel investigation produced by Lawson and Middleton (2016) might be a useful example for future scholars looking to collect data on threat perceptions and securitization policies. By examining the threat construction of the term "Cyber Pearl Harbor", the authors are able to delineate the history of the term's use and the key referent objects. They find that 45% of the time, the term is used to describe threats to civilian infrastructure. The authors also demonstrate that the term is only used to discuss actual events 33% of the time with majority of frames being used to discuss imagined or non-actual threats.

6. Expanding Cyber Security Data

Our team has been coding cyber incident data since 2010 and serves as a unique example of how the process of collecting cyber security data and evidence can be done. Our first peer reviewed published work appeared in 2014 in *Journal of Peace Research* (Valeriano & Maness, 2014). In this article we note that cyber conflict is much more restrained than generally understood by popular discourse. Threat inflation is ripe in cyber security, and the real use of cyber tools seems to be to enhance the power of strong states.

The data that Valeriano and Maness (2014, 2015) have built challenges the cyber revolution perspective and does so with the tools of social science, and is a necessary turn given the general tone of the debate. We first determine that a viable data collection method in light of limited resources was to focus on states that are committed interstate rivals (Diehl & Goertz, 2001). This allows us to focus on those actors with an intense history of recent hostilities that should be the most likely users of cyber technology on the battlefield (Maness & Valeriano, 2018).

In our research (Maness & Valeriano, 2016; Maness, Valeriano, & Jensen, 2017; Valeriano & Maness, 2014, 2015), we have been able to marshal a massive amount of evidence that is useful in dissecting the actual trends on the cyber battlefield in a geopolitical context. We demonstrate that while cyber-attacks are increasing in frequency, they are limited in severity, are directly connected to traditional territorial disagreements, and mostly take the shape of espionage and low-level disruptive campaigns rather than outright warfare.

Given this data-based perspective, we question the dynamics of the cyber security debate and offer a countering theory where states are restrained from using more malicious cyber actions due to the limited nature of the weapons, the possibly of blowback, the connection between the digital world and civilian infrastructure, and

the reality that any cyber weapon launched can be replicated and used right back against the attacker. Given all of these perspectives gleamed from the data, we must moderate our views about the transformation that is offered by cyber strategists who stress a more revolutionist tone (Lango, 2016).

Social science clearly matters for contemporary technological policy debates. Absent rigorous methods, much of what is in the field is basically guesswork. Our work really owes an intellectual debt to J. David Singer, who started the effort to quantify war at the University of Michigan with the Correlates of War (COW) project (Small & Singer, 1982). Our project builds on this methodology and uses many of the same coding strategies. We recognize that data is a work in progress and seek to build more and more knowledge through subsequent updates. By gathering the full picture, we can gain the perspective that really matters in these emerging policy debates regarding the cyber battlefield.

The problem with collecting data where it does not exist already are centered around the difficulties that come with starting such an endeavor in the first place. Often it has been claimed that it would be impossible to collect cyber conflict data, as such data would present a skewed picture of the scope of the field. Yet the imagined impossibility of collecting data should never be the barrier in starting such an undertaking, and the only real barrier should be the literal impossibility of collecting such information.

In the process of collecting data on these state-based cyber events, we found that official leaks to the media have been helpful, but more importantly for the cyber security field was the obvious impetus by cyber security firms to demonstrate their ability to identify attacks and release reports forensically accounting for the process behind the attacks. This sort of information was exactly what we were looking for and it continues to be available to this day as the ultimate calling card demonstrating skills and expertise, but also as a source of information in our investigation. We are prudent and recognize that there have been other efforts at empirically-focused cyber security research. We welcome all and every effort since it will allow for the field to seek the overall goal for the accumulation of knowledge around cyber security practices.

Subsequent work in our book *Cyber War Versus Cyber Realities* reinforced these points and added case studies to support our empirical findings. Our next book, *Cyber Strategy*, includes cyber incident data from 2000 to 2014 between rival states. Our cut point is 2014 because the majority of the coding effort was done in 2016 and we are firm in belief that while cyber incidents can be coded, one needs to wait at least a year to make sure the sources, actors, and targets are confidently known.

The main addition in our work is a consideration of the efficacy of cyber actions. Simply, do they work? To that end we have now coded concessions and targets in the data. We also altered the severity coding to account for a wider scale of events. All cyber incidents in the Dyadic Cyber Incident and Dispute (DCID) are dyadic and the countries must be considered rivals, which are states with recent past animosities with each other. For the coding of the variables for all pairs of states added to the dataset (non-state actors or entities can be targets but not initiators as long as they critical to state-based systems, or if the original hack escalates into an international incident in the non-cyber domain), the initiation must come from a government or there must be evidence that an incident or dispute was government sanctioned.

For the target state, the object must be a government entity, either military or non-military; or a private entity that is part of the target state's national security apparatus (power grids, defense contractors, and security companies), an important media organization (fourth estate), or a critical corporation. Third parties are noted and coded as an additional variable in the data.

We are also now including information on cyber strategies, breaking this down into a four-point typology that is mutually exclusive and logically exhaustive.

1. *Disruptions:* which include taking down websites, disrupting online activities, and are usually low cost, low pain incidents such as vandalism or DDoS techniques;

2. *Short-Term Espionage:* gains access that enables a state to leverage critical information for an immediate advantage example; an example being the Russian theft of DNC emails and publicly releasing them in a disinformation campaign during the 2016 US presidential election;

3. *Long-Term Espionage:* seeks to manipulate the decision-calculus of the opposition far into the future through leveraging information gathered during cyber operations to enhance credibility and capability, an example being China's theft of Lockheed Martin's F-35 plans;

4. *Degrade:* attempt physical degradation of a targets' capabilities. Example: US' Stuxnet against Iran; create chaos in a country to invoke a foreign policy response.

The most active dyad in the international system is China and the US. The majority of these incidents between the world's two most powerful states are espionage campaigns. China sees itself as the rising power that is far behind its status quo counterpart, and this could explain the disproportional balance in initiations between the two states (Lindsay, 2015). Most US-initiated attacks against China are counterespionage degradation campaigns to raise the costs of future espionage by China so that they slow or stop these malicious attacks on American intellectual property and government information. US–China cyber relations came to a head as a result of the OPM hack discovery in 2015, where China successfully stole the personal and sensitive information of over 20 million federal employees and contractors. This led to a high-level meeting between Obama and Chinese President Xi Jingping dur-

ing the latter's state visit in September 2015, where the two agreed to halt intellectual property theft from each other. It has been reported that China has drastically reduced its cyber espionage on the US as a result of this agreement, which was a diplomatic victory for the Obama Administration where escalation and arms races have been avoided (FireEye, 2017). It remains to be seen whether this behavior will hold with the new Trump Administration, whose early rhetoric with Beijing has been more bombastic.

The more recent cyber menace for the US has been Russia, where the former Cold War foe has successfully socially engineered attacks on political networks, including the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC), as well as Hillary Clinton's presidential campaign manager John Podesta's email account. The information stolen from these accounts was then strategically released to WikiLeaks (ODNI, 2017), which could have changed enough minds in crucial swing states and possibly was the deciding factor in the victory of Donald Trump in the 2016 US presidential election. The Obama Administration has responded with economic sanctions on high-level Kremlin operatives and has expelled a few dozen diplomats from the US. However, it remains to be seen if the Trump Administration will continue to hold the Russians to account for these acts of espionage and information warfare.

Yet these data breaches could have been easily prevented with basic cyber hygiene practices for those with access to the networks, and the political espionage conducted by Russia is not outside the acceptable behaviors for spy agencies. The blame could easily lie with the Democratic Party for being so vulnerable to outside attack. Before promoting offensive posturing and escalatory retaliatory action, the US needs to get its networks better defended society-wide, and cyber hygiene policies to prevent such easy attacks such as the Russian election hacks would be a good first start. If the US is considering going toe to toe with its cyber adversaries, the defenses of its large attack surface and vulnerable networks need to be shored up significantly.

Dyads not involving the US are overwhelmingly regional rivals, suggesting that adversarial relationships between these states have been ongoing for years (Vasquez, 1993). Rivals who have been managing these relationships for a long time have developed normal relations (Azar, 1972) and given that most of these cyber incidents and disputes launched against each other are disruptions or espionage, the probability that cyber conflict between regional rivals will lead to escalatory tensions remains low.

Breaking down the macro evidence of Valeriano et al. (2018), Table 1 below shows that 87% of all cyber incidents between rival states are either disruptions or espionage. Victims of these acts of cyber malice have not responded in an escalatory fashion in the majority of cases (Maness et al., 2017), indicating that responses have either been proportional via conventional foreign policy tactics, such as targeted economic sanctions, or diplomatic outreach to promote better behavioral patterns have been successful. Evidence for policies of restraint as the future of governance of the international cyber realm are demonstrated, strengthening these modes of behavior for all states in the international system, as championed by the UN's Group of Government Experts (GGE), should be the primary goals of the government of the US and its NATO and EU allies.

Table 1. Cyber incidents by coercive objective.

Coercive Objective	Number (%)
Disruption	70 (36%)
Espionage	97 (51%)
Degradation	25 (13%)
Total	192 (100%)

US deterrence proponents such as former Director of National Intelligence James Clapper have posited that cyber-attacks will get worse "until such times as we create both the substance and psychology of deterrence" (Jones, 2015). This is assuming that cyber incidents will not only grow in number but also in severity, where escalation will be the future if deterrence mechanisms cannot be put into place. This would require developing sophisticated cyber weapons, communicating these capabilities to potential adversaries in the cyber realm, and being willing to follow through with action that may harm civilians, lead to escalatory retaliation, and provide enemies with digital technologies they did not have before the attack. Yet this type of thinking is an enduring one as more high-profile data breaches, usually espionage campaigns or disruptive information operations and rarely physical degradations (Valeriano et al., 2018) continue to proliferate and be misconstrued in popular narratives (Lawson, 2013).

According to the data, offensive posturing and digital arms races that the US may set into motion as policy could be self-defeating policies (Craig & Valeriano, 2016). There are normative modes of behavior from states that have been observable since the turn of the century based on collected empirical data that suggest that cyberspace can be governed from a less escalatory strategy, where restraint mechanisms can be built upon if the US and its transatlantic allies continue to push for stabilizing norms. The question that remains at the time of this writing is whether or not the Trump Administration will continue this process or turn toward the more dangerous deterrent strategy.

Scholars who have looked at past dynamics of cyber conflicts find that there is evidence for restraint from states. Reveron (2012) acknowledges that states have great capabilities in terms of inflicting damage on one another, yet this does not mean that they will. Espionage and disruptions seem to be the majority of state-based

actions, and more coercive degrading techniques such as Stuxnet or Shamoon are exceptions to the rule according to Valeriano et al. (2018). The need for weaponized retaliatory responses and initiating policies that promote this behavior may therefore be premature at this point, according to available evidence.

The key point is the evidence is critical to evaluate the domain. How can policy decisions be made without considering the shape and scope of the environment? Some scholars paint a vastly different picture than those in the discourse and this is spurred on by a careful analysis of empirical evidence.

7. Important Components of any Dataset

Many groups have produced lists of cyber events, the most prominent might be Hackmageddon (2018). The key aspect to understand is that making a list of cyber events is not enough to produce social science inferences or data analyses. So much more is required. The Council on Foreign Relations (CFR) cyber operations tracker covers cyber incidents from the years 2005–2017 (CFR, 2018). It includes incidents that are "suspected" to have state sponsorship plus non-state action. This is a problem for datasets of this kind, as laying blame on a state or group for cyber actions has enormous geopolitical implications. Throwing suspected state-sponsored incidents in with verifiable ones is problematic coding and raises the possibility of retractions at a later date.

For the variable coded as affiliation, which attempts to attribute the group responsible for the cyber incident, 105 cells of this variable are left blank. Furthermore, 37 of these cells either begin with the phrases "believed to be" or "possibly", indicating further uncertainty of who just might be responsible for the cyber incident. This translates to the coders having 74% of their coded incidents being uncertain that the culprit had been a state actor.

In the DCID, we wait at least one calendar year to pass before we begin to code a year. Right now, our latest, version, 1.1 covers all dyadic cyber incidents between rival states from 2000–2014. We are in the process of coding version 1.5, which will include state-initiated incidents from the years 2000–2016. Both collect government initiated cyber action between rival states from the years 2000–2014, which are extracted from the Klein, Goertz and Diehl (2006) dataset on enduring rivals as well as Thompson's (2001) strategic rivalry dataset. Coding efforts are mirrored after the COW project that records conventional conflict dynamics since the Napoleonic Wars (Jones, Bremer, & Singer, 1996). Several variables are coded based on typologies, methods, target types, coercive objectives, and severity levels. Events are coded into cyber incidents and disputes. Incidents are individual events that can last a matter of hours, days, or weeks, depending on method and have specific objectives. The Stuxnet worm is classified as a cyber incident. Disputes are larger campaigns that can contain multiple incidents and are part of a larger strategy. The Olympic Games dispute which contains Stuxnet but also espionage incidents such as Duqu and Flame.

Many cyber incidents can take months to find the proper attribution, especially covert espionage incidents. The analogy of the iceberg is often made with the idea that much what we know about cyber interactions falls below the surface. Instead we argue that at some point, the iceberg flips over and we are able to get a representative sample of the dynamics of all cyber actions. What is unknown is important, but it is also unknowable. For an incident to make it in the DCID, we must have at least two verifiable sources that have given enough confidence to place the blame on a state actor. Sources include government intelligence reports and cyber security forensic reports.

We must be clear that datasets need some things in common to make them useable to the wider community. Every effort to produce a trusted source of cyber security information should contain clear coding rules, independent variables, compatibility with other coding efforts, and reliability checks. Clear coding rules are critical for any social science effort. How does an outside observer know what is coded in the dataset? What is included and what is left out? This is associated with the condition of replication. Can someone come behind your effort and produce something similar? Clear instructions are critical in order to ensure the progression of knowledge, building and reproducing prior work is critical in seek to confirm knowledge.

A dataset cannot simply be a list of events, that is just a list. Independent variables are critical for any data source. This should include location information, characteristics of the unit of observation, issues such as linkages to other events, damage and severity, and a host of other factors that make up what might be a traditional dataset that can be used for analysis. If there is just a list of events, this is just a single variable that would then need to be merged into another source.

The next clear requirement is the compatibility with prior efforts. The whole purpose of data collection efforts being clear and replicable is to ensure that knowledge is moving forward based on some sort of basic consensus. Others should be able to build on your work and push things forward. The data should be compatible with other sources, our cyber events coded in the DCID dataset has country codes, dates, and other events that can be linked and merged to other data efforts. This effort is based on the Correlates of War project (Jones et al., 1996), a long-standing data collection effort and can be fit in with other data research done in the International Relations field. Avoiding trying to reinvent the wheel and respecting the efforts of those that have come before is critical in moving forward towards shared wisdom.

Finally, reliability is likely the most critical aspect of any dataset. Is it reliable in that we are sure that it was coded correctly, absent of as much bias as possible, and others should be able to take the coding rules and agree

with the basic judgements made? Our DCID data was independently checked by three other hired coders at both rounds of data coding. Version 1.1 of the DCID also had a group of 15 military officers go through all the coding of the more subjective elements to ensure that our coding of success, impact, and actors was reliable and could withstand basic measures of intercoder reliability and acceptance of judgement calls made on borderline cases.

Salehyan (2015) has a useful review of the things needed to produce data in the conflict studies field. There are a host of other issues we have not even begun to mention such as source bias, source inclusion, scalability, information extraction, and the challenges of analysis. One such challenge rarely admitted in cyber security is the problem of selection effects (Fearon, 2002). If we are only taking a sample, such as state-based actions reported by the press, or in our case, only actions between rivals, we are only coding a selection of the wider possible universe of cases. This constraint is critical in understanding the implications of the possible analysis done on the data. Selecting which cyber incidents to be examined, whether state-based, cybercrime, or cyber activism, is a critical judgement call that one must make to facilitate analysis, and the coders must be clear about these choices and their implications.

8. Data Investigations of the Future, What Comes Next?

Social science investigations into cyber security interactions are rare to this point. There is much that needs to be done before we can suggest that the field has a strong grasp of cyber security interactions. Instead, speculation substitutes for detailed understanding and this is of limited value given the importance of cyber security challenges. Rigorous surveys of cyber security interactions are rare. While it seems clear that the public and elites regards cyber threats as prime challenges to the security of the state (Stares, 2017), it is unclear just what context is given to the respondents and what background they are operating under when making sweeping judgements about the security challenges states face.

Embedding experiments within surveys is a potential avenue for future research. Kreps and Schneider (2017) demonstrate that public respondents are unlikely to advocate for escalation even under hypothetical situations. Experiments into human behavior in response to cyber security threats is also critical. Utilizing biological samples of stress, a series of studies seem to suggest that the population regards cyber security threats on par with conventional terror threats (Gross, Canetti, & Vashdi, 2016). Cyber security challenges result in elevated stress levels (Gross et al., 2017). What is unclear is if this is an outlier tied to the sample country, Israel, and what conditions might bring down elevated threat frameworks.

Repression is another key area to study in the future. The expectation is that the future of cyber combat will be state on state violence when in reality we observe much more state on individual cyber violence than would be expected (Valeriano, 2016). The challenge is collecting data on cyber repressive events which are akin to human rights violations. Some have made strides examining individual state repressive incidents (Gohdes, 2015), while others have demonstrated that states experiencing DDoS attacks are also likely the victims of internal repression (Asal et al., 2016).

Future datasets will need to expand to investigate non-state actors and internally repressive cyber incidents. We believe this is the critical future of cyber security investigations. Investigating the macro data inherent in cyber processes can help us understand much more about the domain than the conjecture that seems to dominate the field. All these efforts are a work in progress but working in conjunction with other scholars and avoiding duplication is the only way to move forward.

9. Conclusion

Establishing knowledge about the cyber security domain is critical because it is recognized as a Tier 1 security threat. The potential implications of a cyber security disasters and the strategic logic behind the cyber threats makes the utilization of cyber weapons a possible method of interstate competition. The challenge is to understand how much of this perspective is based on threat inflation and how realistic any of these conjectures is in relation to reality.

By undertaking data exploration efforts, we can seek progress forward on critical security questions. There is appears to be a consensus in the field that there is evident restraint in cyberspace despite the potential for conflict. This consensus is supported by the Council of Foreign Relations incident data which locates only 191 incidents from 2005–2017. The DCID data, which is restricted to only rival states, locates 192 incidents from 2000–2014 (Maness et al., 2017). Other supporting investigations find similar limited engagements utilizing cyber methods to alter state to state relationships.

States are the most cyber-capable actors in the international system (Nye, 2011), therefore collecting data on cyber actions enacted by state actors has been our starting point. The next step in our research program is to begin collection of data on non-state actors, which is a much larger universe of cases, but not impossible to collect data and infer implications of the dynamics of cybercrime, cyber terrorism, and cyber hackitivism. Our same methods and procedures, we posit, will uncover these unknowns in the social science realm of cyber conflict and security research.

This is not to say that data is the only way forward in cyber security. Rigorous case study logic that establishes critical casual actions is welcome. Examining wargames and responses in combat scenarios is also important. Formal modeling would be useful in deducing behavioral options and the constraints imposed by institutions. The cyber security field is ripe for more social science-based in-

vestigations, but these must include the direct collaboration of social scientists who have experience in coding data, practitioners who experience the events first hand, and policy-makers who seek to transform the data into actionable events.

Acknowledgments

Thoughts and prayers for the Chicago Bears. We thank our dogs, the US Marine Corps, the US Navy, and Donald Bren. We do not thank Star Wars, Netflix, and Amazon for being too distracting.

Conflict of Interests

The authors declare no conflict of interests.

References

Ackerman, R. (2017, August 1). Creating a common language of cybersecurity. *AFCEA*. Retrieved from https://www.afcea.org/content/creating-common-language-cybersecurity

Anderson, E. (1998). The security dilemma and covert action: The Truman years. *International Journal of Intelligence and CounterIntelligence*, *11*(4), 403–427.

Asal, V., Mauslein, J., Murdie, A., Young, J., Cousins, K., & Bronk, C. (2016). Repression, education, and politically motivated cyberattacks. *Journal of Global Security Studies*, *1*(3), 235–247.

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences*, *111*(4), 1298–1303.

Azar, E. (1972). Conflict escalation and conflict reduction in an international crisis, Suez 1956. *Journal of Conflict Resolution*, *16*(2), 183–201.

Beardsley, K., & Asal, V. (2009). Nuclear weapons as shields. *Conflict Management and Peace Science*, *26*(3), 235–255.

Berger, P., & Luckmann, T. (1991). *The social construction of reality: A treatise in the sociology of knowledge*. London: Penguin.

Black, I. (2016, February 10). Report on Syria conflict finds 11.5% of population killed or injured. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/feb/11/report-on-syria-conflict-finds-115-of-population-killed-or-injured

Buchanan, B. (2016). *The cybersecurity dilemma*. New York, NY: Oxford University Press.

Bull, H. (1966). International theory: The case for a classical approach. *World Politics*, *18*(3), 361–377.

Council on Foreign Relations. (2018). *Cyber operations tracker*. Retrieved from https://www.cfr.org/interactive/cyber-operations

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to National Security and what to do about it*. New York, NY: Harper Collins.

Craig, A., & Valeriano, B. (2016). Conceptualising cyber arms races. In *Cyber conflict (CyCon), 2016 8th international conference on cyber conflict* (pp. 141–158). Piscataway, NJ: IEEE.

Department of Homeland Security. (2018a). *Report cyber incidents*. Retrieved from https://www.dhs.gov/how-do-i/report-cyber-incidents

Department of Homeland Security. (2018b). *Cyber incident data and analysis working group white papers*. Retrieved from https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers

Defense Intelligence Agency. (2017, August 14). *Cyber attacks going on right now* [Tweet]. Retrieved from https://twitter.com/DefenseIntel/status/897106479546851329

Diehl, P., & Goertz, G. (2001). *War and peace in international rivalry*. Ann Arbor, MI: University of Michigan Press.

Fearon, J. (2002). Selection effects and deterrence. *International Interactions*, *28*(1), 5–29.

Fireeye. (2017). *Red line drawn: China recalculates its use of cyber espionage*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

Gallucci, N. (2016, October 21). This mesmerizing map shows what cyberattacks look like. *Mashable*. Retrieved from: http://mashable.com/2016/10/21/norse-map-global-hacking-problem/#isxCIop4N8q3

Gartzke, E., & Lindsay, J. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Gohdes, A. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, *52*(3), 352–367.

Gross, M., Canetti, D., & Vashdi, D. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284–291.

Gross, M., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, *3*(1), 49–58.

Gurdus, E. (2016, December 15). We're headed for a "cyber Pearl Harbor", says Adm James Stavridis. *CNBC*. Retrieved from http://www.cnbc.com/2016/12/15/were-headed-at-a-cyber-pearl-harbor-says-adm-james-stavridis.html

Hackmageddon. (2018). *Cyber attacks statistics*. Retrieved from http://www.hackmageddon.com/category/security/cyber-attacks-statistics

Healey, J., & Grindal, K. (Eds.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Washington, DC: Cyber Conflict Studies Association.

Human Rights Watch. (2017). Syria: Events of 2016 (*World Report 2017*). Retrieved from https://www.hrw.org/world-report/2017/country-chapters/syria

Jones, D., Bremer, S., & Singer, J. D. (1996). Militarized interstate disputes, 1816–1992: Rationale, coding rules, and empirical patterns. *Conflict Management*

and Peace Science, *15*(2), 163–215.

Jones, S. (2015, July 29). Cyber insecurity: West eyes Dr. Strangelove tactics in cyber wars. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/2d23d4c8-35d2-11e5-b05b-b01debd57852.html?siteedition=intl&utm_content=buffere8653&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#axzz3h6sRmLBL

Karatzogianni, A. (2012). Cyberconflict and the future of warfare. In H. Gardner & O. Kobtzeff (Eds), *The Ashgate research companion to war. Origins and prevention* (pp. 491–504). Burlington, VT: Ashgate.

Kello, L. (2013). The meaning of the cyber revolution: Perils in theory and statecraft. *International Security*, *38*(2), 7–40.

Klein, J., Goertz, G., & Diehl, P. (2006). The new rivalry dataset: Procedures and patterns. *Journal of Peace Research*, *43*(3), 331–348.

Koerner, B. (2016, October 23). Inside the cyberattack that shocked the US Government. *Wired*. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government

Kostyuk, N., & Zhukov, Y. (2017). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*. doi:10.1177/0022002717737138

Kreps, S., & Schneider, J. (2017, December). *Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics*. Paper presented at Emerging Technologies and Strategic Stability Conference, Stanford University, Stanford, CA.

Lakatos, I. (1970). Criticism and the growth of knowledge. In I. Lakatos & A. Musgrave (Eds.), *Proceedings of the international colloquium in the philosophy of science, London, 1965, volume 4*. Cambridge: Cambridge University Press.

Lango, H. (2016). Competing academic approaches to cyber security. In K. Friis & J. Ringsmose (Eds.). *Conflict in cyberspace* (pp. 7–26). New York, NY: Routledge.

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Lawson, S., & Middleton, M. (2016, September). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016. Paper presented at Legal and Policy Dimensions of Cybersecurity, George Washington University, Washington, DC.

Lindsay, J. (2015). Introduction: China and cybersecurity: controversy and context. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain* (pp. 1–28). New York, NY: Oxford University Press.

Maness, R., & Valeriano, B. (2018). International cyber conflict and national security. In D. Reveron, N. Gvosdev, & J. Cloud (Eds.), *Oxford handbook on US national security* (pp. 139–158). New York, NY: Oxford University Press.

Maness, R., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces and Society*, *42*(2), 301–323.

Maness, R., Valeriano, B., & Jensen, B. (2017). *The dyadic cyber incident and dispute dataset, version 1.1*. Retrieved from https://drryanmaness.wixsite.com/cyberconflcit/cyber-conflict-dataset

Matsakis, L. (2018, January 10). Hack brief: Russian hackers release apparent IOC emails in wake of Olympics ban. *Wired*. Retrieved from https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails

Mauslein, J. (2014). *Three essays on international cyber threats: Target nation characteristics, international rivalry, and asymmetric information exchange*. (Doctoral dissertation). Kansas State University, Kansas, USA.

Middleton, B. (2017). *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

Newman, l. (2017, November 15). Feds explain their software bug stash-but don't erase concerns. *Wired*. Retrieved from https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns

Nye, J. (2011). *The future of power*. New York, NY: Public Affairs.

Office of the Director of National Intelligence. (2017, January 6). *Assessing Russian activities and intentions in recent US elections*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Pytlak, A., & Mitchell, G. (2016). Power, rivalry and cyber conflict. In K. Friis & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 65–82). New York, NY: Routledge.

Reveron, D. (2012). An introduction to national security and cyberspace. In D. Reveron (Eds), *Cyberspace and national security: Threats, opportunities, and power in a virtual world* (pp. 3–20). Washington, DC: Georgetown University Press.

Salehyan, I. (2015). Best practices in the collection of conflict data. *Journal of Peace Research*, *52*(1), 105–109.

Schneider, J. (2017). *The information revolution and international stability: A multi-article exploration of computing, cyber, and incentives for conflict*. (Doctoral dissertation). The George Washington University, Washington, DC, USA.

Singer, J. D. (1969). The incomplete theorist: Insight without evidence. In K. Knor (Ed.), *Contending approaches to international politics* (pp. 62–86). Princeton; NJ: Princeton University Press.

Small, M., & Singer, J. D. (1982). *Resort to arms: International and civil wars, 1816–1980*. Thousand Oaks, CA: SAGE.

Stares, P. B. (2017). Preventative priorities survey: 2018. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/report/preventive-priorities-survey-2018

?utm_medium=partner&utm_source=atlantic_global&utm_campaign=pps&utm_content=12101

Thompson, W. (2001). Identifying rivals and rivalries in world politics. *International Studies Quarterly*, *45*(4), 557–587.

UK Government. (2016). *National cyber security strategy 2016 to 2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Valeriano, B. (2016). Closing the Internet up: The rise of cyber repression. *Council on Foreign Relations Net Politics*. Retrieved from https://www.cfr.org/blog/closing-internet-rise-cyber-repression

Valeriano, B., & Maness, R. (2012). Persistent enemies and cyber security: The future of rivalry in an age of information warfare. In D. Reveron (Ed.), *Cyberspace and national security: Threats, opportunity and power in a virtual world* (pp. 139–158). Washington DC: Georgetown University Press.

Valeriano, B., & Maness, R. (2014). The dynamics of cyber conflict between rival antagonists, 2001–2011. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York, NY: Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. (2018). *Cyber strategy: The changing character of cyber power and coercion*. New York, NY: Oxford University Press.

Vasquez, J. (1991). The deterrence myth: Nuclear weapons and the prevention of nuclear war. In C. Kegley (Ed.), *The long postwar peace* (pp. 205–223). New York, NY: HarperCollins.

Vasquez, J. (1993). *The war puzzle*. Cambridge: Cambridge University Press.

Vasquez, J. (1998). *The power of power politics*. Cambridge: Cambridge University Press.

Walker, L. (2015, July 12). Real time cyber-attack map shows scope of global cyber war. *Newsweek*. Retrieved from http://www.newsweek.com/real-time-cyber-attack-map-shows-scope-global-cyber-war-352886

About the Authors

Brandon Valeriano is the Donald Bren Chair of Armed Conflict at the Marine Corps University. He has published five books and dozens of articles. His two most recent books are *Cyber War versus Cyber Reality* (2015) and *Cyber Strategy* (2018), both with Oxford University Press. Ongoing research explores cyber coercion, biological examinations of cyber threat, repression in cyberspace, and the influence of video games on foreign policy outlooks.

Ryan C. Maness is an assistant professor of Cyber Conflict and Security in the Defense Analysis Department at the Naval Postgraduate School. His current research explores cyber strategy and coercive effects and how the tactic fits within overall military strategies for various countries. His specific focus is Russia's use of cyber and disinformation tactics in foreign policy as well as military strategy. His research is based on the collection of cyber events through quantitative methods and is currently constructing a cyber incidents dataset that will not only encompass state actors, but non-state actors as well.

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 61–72
DOI: 10.17645/pag.v6i2.1279

Article

Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats

Miguel Alberto Gomez [1,*] and Eula Bianca Villar [2]

[1] Center for Security Studies, ETH Zurich, 8092 Zurich, Switzerland; E-Mail: miguel.gomez@sipo.gess.ethz.ch
[2] Department of Business and Technology, La Salle Universitat Ramon Llull, 08022 Barcelona, Spain; E-Mail: ebvillar@salleurl.edu

* Corresponding author

Submitted: 22 November 2017 | Accepted: 7 March 2018 | Published: 11 June 2018

Abstract
Advances in cyber capabilities continue to cause apprehension among the public. With states engaging in cyber operations in pursuit of its perceived strategic utility, it is unsurprising that images of a "Cyber Pearl Harbor" remain appealing. It is crucial to note, however, that the offensive action in cyberspace has only had limited success over the past decade. It is estimated that less than 5% of these have achieved their stated political or strategic objectives. Moreover, only five states are thought to have the capabilities to inflict or threaten substantial damage. Consequently, this raises the question of what accounts for the continued sense of dread in cyberspace. The article posits that this dread results from the inappropriate use of cognitive shortcuts or heuristics. The findings herein suggest that the lack of experience in dealing with cyber operations encourages uncertainty, which motivates decision-makers to base their judgements on pre-existing, and possibly incorrect, conceptions of cyberspace. In response, the article segues into potential solutions that can mitigate unsubstantiated dread towards cyberspace by peering into the role that attributes at the organizational level can play in tempering the position of individuals. The suggested considerations are rooted in the interactions between the micro and macro level processes in forming judgments, sensemaking, and ultimately, mobilizing actions.

Keywords
cybersecurity; cyber threats; dread; experiment; heuristics

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

On Friday, May 12, 2017, the United Kingdom's National Health Service (NHS), Spain's Telefonica, and other entities were incapacitated by the WannaCry malware which infected over 200,000 computers in nearly 150 countries (R. Goldman, 2017). In 2001, Code Red exploited vulnerabilities leading to the infection of over 300,000 computers (Perrone, 2001). In 2003, Slammer initiated a denial-of-service attack and stalled Internet traffic while compromising approximately 75,000 computers within ten minutes (Boutin, 2003). These events reinforce negative perceptions towards cyber threats, yet overstate the scope of the problem. Anderson et al. (2013) note that the actual cost of cybercrime is much lower than that reported by the private sector or the media. Expounding on this argument, Jardine (2015, 2017) notes that malicious activity in cyberspace is far less likely to occur when viewed relative to the growth of the domain and when vulnerable actors are disaggregated and studied in isolation. More closely related to this article, Maness and Valeriano's (2016) study highlights that out of 68 states with cybersecurity programs, only five (5) demonstrated the capability to inflict noteworthy damage. Furthermore, less than 5% of these operations have resulted in behavioural changes on the part of the target as intended by the aggressor. Consequently, this raises the question as to why dread continues to persist as a re-

sponse to cyber operations (Jarvis, Macdonald, & Whiting, 2017).

Dread is defined in this article as the apprehension of the negative consequences of an event. This perception of dread in cyberspace is often attributed to increasing technological dependence and the strategic exploitation by state actors. The literature analyses this phenomenon mainly through the lens of rational choice theory, while underemphasizing individual cognitive processes (Dean & McDermott, 2017; Edwards, Furnas, Forrest, & Axelrod, 2017; Gartzke & Lindsay, 2015). Consequently, this article explores dread in response to cyber operations as a reflection of heuristic usage resulting in sub-optimal judgements.

Using two vignette survey experiments, it forwards three main arguments. First, the lack of experience and the novelty of this threat generates an environment of uncertainty with respect to cyber operations (Gigerenzer, 2008; Hafenbradl, Waeger, Marewski, & Gigerenzer, 2016; Kruglanski, Orehek, Dechesne, & Pierro, 2010). Second, judgmental errors that facilitate elevated levels of dread are not suggestive of irrationality but rather stem from the use of inappropriate cognitive strategies. Finally, errors may be tempered by attributes defined at the organizational level.

Before proceeding with the rest of the article, it should be noted that the results do not serve to explicitly identify the use of a specific heuristic. Rather, heuristic usage is inferred from the level of dread demonstrated by participants and suggests that the use of these strategies in this context merits further inquiry.

2. Framing Cyber Threats

A cyber threat, in the context of this article, is an expectation of harm to a political body through the malicious manipulation of cyberspace which reduces its capability to meet strategic, political, or economic objectives (Creppell, 2011). While threat conceptualizations vary, these are dependent on the domain's technological characteristics. Increased dependence on cyberspace elevates a society's exposure to potential threats, and consequently, the perception of dread brought by unforeseen consequences (Hansen & Nissenbaum, 2009; Kuehl, 2009). Furthermore, its growth coincides with Perrow's (2011) claim that complexity and interdependency result in *normal accidents* that emerge from the inherent characteristics of systems—compounding attempts to secure the domain. Experience, however, has proven less consequential. In 2010, Stuxnet affected nearly a third of Iran's nuclear centrifuges; yet damage did not exceed expected operational wear-and-tear (Lindsay, 2013). Likewise, disruption to segments of Ukraine's power grid in 2015 required the exploitation of interdependent systems but only resulted in temporary disruption (Zetter, 2016). Given its coercive intent, aggressors failed to achieve their objectives despite the exploitation of these valuable systems[1] (Iasiello, 2013; Maness & Valeriano, 2016).

Besides its technological fragility, the domain's strategic value also enjoys attention (Dunn Cavelty, 2012). Specifically, its perceived offensive advantage reflected by its low cost of entry and the difficulty of defending against aggressors is thought to serve as an equalizer within the international system (Lawson, 2013). For instance, the availability of tools stands in contrast with how hard it is to defend against aggressors. Consequently, weaker powers may offset their material disadvantage through cyberspace (Valeriano & Maness, 2014). Moreover, offensive acts are thought to be easier than defensive acts, further emboldening aggressors (Edwards et al., 2017).

No actor, however, has met its objectives by cyber means alone (Iasiello, 2013). Its low cost of entry is proportional to the expected gains (Pytlak & Mitchell, 2016; Slayton, 2017). While disruptive events require minimal effort, degradative operations demand substantial investments on the part of the aggressor. This is due to the organizational demands of an effective offensive campaign that is often overlooked in favour of technological considerations (Buchanan, 2017; Rid & Buchanan, 2015; Slayton, 2017). Consequently, this weakens arguments in favour of a cyber offensive-advantage. In addition, the evidence also illustrates restraint on the part of aggressors with their actions occurring below thresholds that are likely to result in escalation (Valeriano & Maness, 2015).

Despite its suggested exceptionalism, cyberspace remains subject to systemic, organizational, and material constraints such that operations have, thus far, achieved limited gains (Healey, 2016; Iasiello, 2013; Lawson, 2013; Sheldon, 2014). Yet whether one ascribes it to one or all of the above reasons, empirical evidence has yet to account for the continued sense of dread (Jarvis et al., 2017).

3. A Case for Cognitive Heuristics

The previous section suggests that a degree of irrationality influences judgements vis-à-vis cyber operations. Assuming the uniformity of the underlying technologies[2] and the move towards greater societal dependence, these deviations cannot be justified solely by technological or systemic variations. A classical understanding of rationality requires that decision-makers possess knowledge of all possible alternatives. Such conditions are rarely met and result in bounded rationality where individuals operate as satisfiers rather than optimizers (Dawes, 1979; De Neys, Rossi, & Houde, 2013; Kahneman, 2003; Thompson, Turner, & Pennycook, 2011).

Extending this argument further, Savage (1972) labels conditions of perfect information as *small worlds*,

[1] Stuxnet did not result in the discontinuation of the Iranian Nuclear Programme and the Ukraine attack did not shift the balance of the conflict in favour of Russia.

[2] A similar sense of dread has occurred in response to novel technologies. It is crucial to note that cyberspace is not exceptional in this case.

distinguishing these from *large worlds* where judgements informed by rational choice cannot be presumed to be the correct response. Research demonstrates that strategies that deviate from normative models are preferred when conditions with less than or almost perfect information exist (Binmore, 2008). The resulting less-is-more effect challenges the convention of rational cognition and brought renewed interest to the concept of heuristics.

Gigerenzer and Gaissmaier (2011, p. 454) define heuristics as a strategy that "ignores part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods". Although the classical approach to heuristics emphasizes its propensity to generate sub-optimal judgements, satisfactory results are possible when the strategy exploits the statistical characteristics of the information environment (Gigerenzer, 2008; Kruglanski et al., 2010; Martignon & Hoffrage, 1999).

The information environment plays a crucial role in making judgements. Assuming that information is readily available, the introduction of free parameters is unproblematic. This, however, is rarely the case. Most environments wherein judgements concerning future events are crucial involve *large worlds* in which relevant information is unknown or uncertain and is derived from a small sample. The introduction of additional parameters to improve fit risks the introduction of noise. Consequently, normative strategies such as expected utility are disadvantaged.

4. Cyberspace: A Very Large World

Heuristics may outperform normative strategies in uncertain environments. While it may be counterintuitive to assert that judgements regarding cyberspace are best approached through this frugal process, its characteristics are better aligned with the notion of a large rather than a small world.

4.1. An Uncertain Domain

Cyberspace is unpredictable. While its history is marked by efforts to reduce uncertainty, these do not eradicate the effects of increased complexity that limit predictive accuracy. Consequently, the significance of offensive or defensive acts cannot be fully anticipated (Farrell & Glaser, 2017).

The growth of technologically-driven solutions does not abolish the challenge of uncertainty. First, additional information does not translate to a generalizable view of threats. Although cyberspace operates on pre-defined rules[3], the interconnection between components varies by function. Relying on public threat information generated from a limited sample does not adequately capture this reality. Second, trust in automated systems to collect, identify, and model threats aggravate the problem of overfitting. These systems are dependent on pre-existing signatures, the development of which is left to individuals or organizations with a limited worldview and are unable to capture the full spectrum of threats. Finally, efforts to reduce bias through increased information sharing and exchange[4] is problematic. The exchange of information is non-obligatory and active participants share similarities in terms of technology and worldview. Moreover, the integrity of such information cannot be guaranteed.

4.2. Limited Experience

Cyber operations that significantly affect a state's strategic interests or normal day-to-day life are rare. This infrequency provides decision-makers with a limited sample from which to generalize. Valeriano and Maness (2014), for instance, identified less than fifty (50) instances where cyber threats inflicted noticeable damage to critical infrastructure. Judgements emerging from these may not reflect reality. Furthermore, efforts to increase the availability of threat intelligence, as mentioned above, may increase the volume of information, but not necessarily its quality.

In reference to Slovic's (2016) model of risk perception, events that are both uncertain and exhibit the potential (real or imagined) for catastrophe increase the level of dread. Translating this into the realm of politics, decision-makers operating in an uncertain environment with incomplete information tend to over-estimate risks associated with events such as the threat posed by an adversarial state (Jervis, 2017). Note, however, that while research has shown that appropriate judgements may still emerge using heuristics. This, however, is contingent on its fit with the existing information environment—also known as a heuristic's ecological rationality (Gigerenzer & Gaissmaier, 2011).

4.3. Constraints on Ecological Rationality

While the characteristics of cyberspace make it an ideal candidate for heuristic use, the selected heuristic must be able to exploit the environmental structures of uncertainty, sample size, redundancy, and variability in cue weights (Todd & Gigerenzer, 2012). The environmental structures of redundancy and variability in cue weights are of particular interest for this article. The former refers to the correlation between cues or the extent to which two or more sources of evidence are related to one another. For instance, to what extent does the ability to compromise the banking system in Country A indicate the vulnerability of the same country's power generation facilities? Relatedly, the variability of cue weights deter-

[3] The underlying components of cyberspace interact with the aid of pre-defined architectures (e.g., the Von Neumann architecture common to most modern-day computers) and protocols (e.g. Hypertext Transfer Protocol, HTTP).
[4] In the form of crowd-sourced threat intelligence such as the Open Threat Exchange (OTX).

mines whether the relevance of these cues is normally distributed or skewed. Building on the previous example, to what extent would Country B's banking system be vulnerable if that of Country A was exploited? Although heuristics have been proven to outperform more deliberate strategies, the ability to discern these characteristic is crucial for this task. Failure to do so results in ecologically irrational strategies being selected that, in turn, leads to inappropriate judgements. While factors such as time-pressure, cognitive resources, and pre-existing bias hinder the ability to select ecologically rational strategies, this article is interested primarily in the enabling role of domain expertise with respect to cyberspace (Kruglanski & Gigerenzer, 2011).

Although cyberspace appears monolithic to laymen, its inner workings are greatly segmented. Such abstraction is crucial to allow individuals to exploit its functionality for their professional or day-to-day tasks. However, attempts to explain its finer points have resulted to the use of analogies that poorly explain the functioning of this domain and which have resulted in many misconceptions amongst the public (Betz & Stevens, 2013; E. Goldman & Arquilla, 2014). While simplification aids communication, it limits the ability to form sound judgements which could otherwise emerge in light of a better, if not complete, understanding of cyberspace. Authors such as Hansen and Nissenbaum (2009) have cited knowledge discrepancies between experts and non-experts as the source of alarmism over cyberspace. Similarly, a recent study of media articles covering cyber operations has found no difference in how threats are perceived between different states and those that occur domestically (Jarvis et al., 2017). In the earlier example, if both power generation (Country A) and banking (Country B) used identical systems and were equally vulnerable then heuristics such as "Take the Best" would work just as well, if not better, than more deliberate cognitive strategies (Gigerenzer, 2008). However, expertise gained through experience or formal training would prompt decision-makers to recognize the differences between these systems resulting in the use of more ecologically rational strategies. Taken collectively, questions concerning the lack of experience and expertise towards cyber operations leads to two key propositions:

(a) Hypothesis 1: *Limited of experience with cyber operations creates an environment of uncertainty resulting in the use of cognitive heuristics*.

(b) Hypothesis 2: *The absence of domain knowledge in cyberspace prompts the selection of inappropriate heuristics resulting in elevated levels of dread*.

5. Experimental Design

5.1. Operationalization and General Design

To demonstrate the role of heuristics, the article implements a 2×2 between-group vignette survey experiment (Auspurg & Albanese, 2015; Rousseau & Garcia-Retamero, 2007; Sniderman, 2011). The treatment is applied through the manipulation of *Internal* and *External* variables that reflect positive or negative events. For the purposes of this experiment, these events are cyber operations targeting a state's power generation facilities. These are made to vary slightly with respect to their cause, impact, and time, and to reflect the uncertainty of the informational environment. Participants are also denied information regarding other events besides that of a second state's experience with a cyber operation. These are meant to operationalize the concept of uncertainty and limited experience which is crucial to the above framework. Furthermore, the countries depicted in the vignette are portrayed as being nearly identical to one another in terms of their usage of cyberspace. No specific information is provided regarding the specific technologies used or how they vary. This is intended to stimulate the participant's knowledge of cyberspace and operationalizes the concepts of redundancy and variability, which entails that those with greater knowledge of the domain ought to be able to recognize the possible differences that may exist. These characteristics meant that both hypotheses could be tested.

Before reading the vignette, participants responded to a set of questions to measures their trust in cyberspace to act as a control for pre-treatment effects. The questionnaire is based on Jian, Bisantz and Drury's (2000) measure of trust in automated systems. This is followed by the vignette in which the participants are instructed to evaluate the extent to which they perceive cyberspace as threatening. Threat is measured with a 10-point Likert scale.[5] The baseline value is five (5), which suggests a neutral perception of the domain.[6] Higher values indicate elevated levels of dread while lower values reflect its absence.

The choice to operationalize the concept of dread as the threatening (or not) nature of cyberspace is grounded in the vernacular understanding of a threat. A threat may be an indication of something impending (e.g. threat of a blackout). In the context of the vignette, this is presented as the threat of the negative consequences of a cyber operation. Analytically, this is equivalent to Slovic's (2016) notion of dread which is viewed as the apprehension of the negative consequences of an activity.

[5] The Likert scale is a widely used instrument for measuring a participant's attitude in survey research. For more information, refer to the Sage Research Methods webpage (Lavrakas, 2008).
[6] As there is no available baseline as to the "appropriate" level of dread, this value was deemed appropriate given the objectives of the study.
[7] An Internet-based platform for recruiting participants specifically for research.

5.2. Participant Recruitment

Participants were recruited through Prolific[7]. While concerns regarding data quality from Internet sources persist, no significant difference has been found with respect to experiments investigating cognitive processes (Casler, Bickel, & Hackett, 2013; Crump, McDonnell, & Gureckis, 2013; Peer, Brandimarte, Samat, & Acquisti, 2017). Special care, however, is required as participants are often less engaged with the experiment. Consequently, two attention check questions are included such that failing one requires the removal of a participant.

The participants consist of university students divided into two groups. The first are those pursuing degrees in Computer Science and related disciplines while the second are those who do not have the same educational background. The former represents "domain experts" while the latter are viewed as "domain non-experts". Participants are then randomly assigned to one of four versions of the vignette. Given the absence of methodologically similar research for this problem domain, the authors assumed a moderately large effect size ($f = 0.3$). Consequently, a minimum sample size with appropriate statistical power ($1 - \beta = 0.8$) was estimated at 90.[8] It ought to be noted that the results contained herein are valid with respect to the samples used and are therefore not immediately generalizable. Replications studies are necessary before more generalizable conclusions are made.

6. Experimental Results

6.1. Experiment 1: Domain Non-Experts

The first experiment recruited 202 participants. Of these, 50.99% (103) were female and the remaining 49.01% (99) were male. Issues concerning engagement were encountered leading to the removal of 27.72% (56).[9] To ensure a balanced analysis, random samples were drawn based on the size of the smallest treatment group resulting in 120 samples with thirty (30) samples per treatment group.

Analysis reveals that 65.9% (79) of participants began the experiment with a distrust of cyberspace while the remaining 34.1% (41) indicated that they either trusted the domain or held no preference. The mean for *Threat*, however, does not suggest an elevated sense of dread ($\bar{x} = 5.5$, baseline = 5.0).

To determine the effect of *Trust* and the absence or presence of *External* and *Internal* events on *Threat*, a blocked factorial Analysis of Variance (ANOVA)[10] was performed. For this analysis, the effects on *Trust* (i.e. Positive, Negative, Neutral) was controlled for through blocking.

The results of the experiment shows a significant Average Treatment Effect (ATE) due to the *External*, $F(1,114) = 10.33$ and *Internal* $F(1,114) = 7.37$ treatments as well the pre-existing level of *Trust* $F(2,144) = 4$ on *Threat* at the $p < 0.05$ level.[11] A Post Hoc comparison reveals that the main effects are significant at $p < 0.05$. The presence of an *External* event had a main effect of 1.34 on *Threat*. An Internal event, on the other hand, had a main effect of 1.13. Finally, *Trust* had a significant main effect of 1.27 between Positive and Negative groups. No significant interactions were observed in this experiment.

6.2. Experiment 2: Domain Experts

The second experiment recruited 166 participants. Of these, 22.29% (37) were female and the remaining 77.71% (129) were male. Issues concerning engagement were encountered leading to the removal of 32.53% (54). To ensure a balanced analysis, random samples were drawn based on the size of the smallest treatment group resulting in 112 samples with twenty-eight (28) samples per treatment group.

Analysis reveals that 50.89% (57) of participants began the experiment with a distrust of cyberspace while the remaining 49.11% (55) indicated that they either trusted the domain or held no preference. The mean for *Threat*, however, does not suggest an elevated sense of dread ($\bar{x} = 5.71$, baseline = 5.0). To determine the effect of *Trust* and the absence or presence of *External* and *Internal* events on *Threat*, a blocked factorial ANOVA was performed. For this analysis, the effects to *Trust* was controlled for through blocking.

The analysis does not reveal a significant ATE of the *Internal*, or *Trust* treatments on *Threat* at the $p < 0.05$ level[12]. External $F(1,106) = 2.72$, $p = 0.06$, however, had a barely significant main effect on *Threat*. A Post Hoc comparison illustrates that there is no statistically significant difference across different treatment groups in terms of *Threat* for this given experiment. No significant interactions are observed in this experiment.

7. General Discussion

7.1. Non-Experts and Motivated Reasoning

The results indicate that dread is not noticeably elevated for domain non-experts ($\bar{x} = 5.5$). When comparisons

[8] The approximation that 90 participants are necessary to ensure that the findings were not simply the result of chance and that the treatment has resulted in a valid and observable effect.

[9] Studies concerning the lack of attention on Internet-based platforms suggest that attrition can be as high as 50%. A rate less than 30% exceeds expectations (Peer et al., 2017).

[10] A collection of statistical techniques used to analyze the difference of means between groups. For further information, refer to *Introduction to Analysis of Variance* (Turner & Thayer, 2001).

[11] Effect Size (Cohen's f): $\text{Trust}_f = 0.265$; $\text{External}_f = 0.301$; $\text{Internal}_f = 0.254$.

[12] Effect Size (Cohen's f): $\text{Trust}_f = 0.206$; $\text{External}_f = 0.187$; $\text{Internal}_f = 0.136$.

are made between treatment groups, however, a different picture emerges. Treatment groups exposed solely to *External* events ($\bar{x} = 5.7$, $p = 0.044$) and those that experienced both *External* and *Internal* events ($\bar{x} = 6.7$, $p = 0.0$) reflect elevated and statistically significant levels of dread in comparison to the control ($\bar{x} = 4.167$).

While the design of the experiment does not permit the identification of specific cognitive heuristic, it allows one to infer the possible processes involved. For groups in which negative *External* and *Internal* events occurred, the imagery of an extended period of power loss experienced by a similar country is set in the memory of the participant. The participant is then informed of a similar event taking place in their hypothetical country—resulting in an emotional association between the two events. This process of emotional association has been identified as a cornerstone of motivated reasoning in which decision-makers strive to maintain cognitive consistency with respect to their existing beliefs (Jervis, 2017). Furthermore, these beliefs are self-reinforcing with later experiences confirming or strengthening one's position on the matter (Holmes, 2015; Mercer, 2010; Roach, 2016). Yet this association may not be dependent solely on the debilitative experience of a third-party. The existing levels of *Trust* by participants may have also played a role.

For treatment groups experiencing only negative *External* events, the mean of *Threat* was 2.2 points higher for participants who distrusted cyberspace ($p = 0.01$). This similarity in direction between *Trust* and *Threat* suggests an association between the two, which may have led participants to use the former to inform their judgements. Unfortunately, this process is not observed in cases where both *External* and *Internal* events are negative in nature where the difference due to *Trust* is only 0.8 points ($p = 0.5$). This does not discredit earlier arguments.

The level of dread may have been a manifestation of motivated reasoning—the need to believe in the dangers of cyberspace. But the emotional association may have been caused by the recency effect (Krosnick, Li, & Lehman, 1990). When participants are asked to evaluate the level of *Threat*, those exposed to negative *Internal* events begin their associated memory search with their most recent experience. If a negative *External* event had recently been shown, the recency effect could result in an association forming between the two. In its absence, participants would have to extend the search of their stored memory which may include pre-existing trust in cyberspace.

The above process also accounts for the absence of elevated levels of *Threat* (i.e. negative *Internal* event only). Prior to applying the *Internal* treatment, participants are informed that "domestically, your country, like others, occasionally experiences trouble with criminals in cyberspace who target individuals and small to medium-sized enterprises for financial gain". Consequently, it is possible that participants form an association with this statement. The absence of a negative *External* event reinforces the benign nature of cyberspace as other countries with seemingly similar characteristics have not encountered problems. Additionally, the similarity in the levels of *Threat* irrespective of *Trust* rules the latter out as a source of association. Finally, the lack of difference between the level of *Threat* of this group and that of the control suggests that the participants perceive the situation as routine.

7.2. Motivated Reasoning and Inappropriate Strategies

The presence of motivated reasoning in the formation of judgement does not necessarily result in sub-optimal outcomes. The literature on motivated reasoning identifies two modes of thinking: accuracy-oriented and goal-oriented (Kunda, 1990; Taber, Lodge, & Glathar, 2001). The former assumes that individuals will engage in more deliberate and cognitively demanding processing to reach the best conclusion. The latter, in contrast, motivates individuals to maintain pre-determined beliefs resulting in selective information processing which reinforces existing biases.

With respect to the article, the situation in the vignette is framed such that it encourages a goal-oriented mindset. Participants play the role of an appointed elite with no apparent accountability to the public. Moreover, there are no explicitly stated consequences that may result from bad judgement (Lerner & Tetlock, 1999). Furthermore, the stereotypical use of *External* and *Internal* events (as well as *Trust*) suggests an attempt to maintain pre-existing beliefs by building associations (specified in the vignette or from past experience) to serve as reference points to assess the current state of cyberspace.

The representativeness heuristic is employed when making judgements in uncertain environments. When in use, individuals resort to the comparison of salient features exhibited by objects or events (Kahneman, 2011). In the experiment, participants appear to draw similarities between their hypothetical country and others regarding the use of cyberspace and its corresponding vulnerability as well as between the situation presented in the vignette and their own pre-existing notions concerning cyberspace (i.e. *Trust*).

A cursory evaluation of the vignette encourages readers to identify and find similarities between the countries being discussed. Both hypothetical countries invested in and enjoyed the economic benefits of ICT. For those that experienced negative *External* and *Internal* events, both had their power plants affected to varying degrees. A few assumptions may be made given these. First, ICT (and in turn cyberspace) is a monolithic and homogenous construct. Second, all power plants that depend on these technologies are vulnerable. Third, these vulnerabilities can easily be exploited. Finally, the consequences of such a compromise are predictable. These raise questions whether the redundancy and variability of cues within the information environment were suffi-

ciently recognized by the participants. Failure to do so results in the selection of ecologically irrational strategies and accounts for the observed level of dread.

As logical as these propositions may be, they fail to grasp certain realities. Indeed, cyberspace is by no means a homogenous entity. While these technologies do share commonalities that allow for integration, they retain enough individual characteristics to make each unique. For instance, while both Windows and Unix systems share common protocols, a vulnerability in the former is not necessarily shared by the latter. And even if a vulnerability is found to exist, it is not a confirmation of its exploitability. Both intent and capabilities need to exist for this to occur (Edwards et al., 2017; Maurer, 2018). Absent an interested actor, a vulnerability may continue to exist without any further repercussions. Moreover, the successful exploitation of a vulnerability also depends on the capabilities of both parties involved. In the case of Stuxnet, significant resources were invested to overcome the physical and technological barriers raised to secure the targeted systems. Finally, the consequences of such an interdependent and interconnected system failing cannot be predicted beforehand with absolute certainty (Perrow, 2011).

This depth of knowledge cannot be expected from the average participant in Experiment 1. This results in uncertainty that prompts the use of the representativeness heuristics. The results suggest that participants attempted to find similarities between the events and structures presented resulting in unsuitable stereotypes being drawn between *External* and *Internal* events as well as between these and their personal experiences with cyberspace. Consequently, the behaviour observed with non-experts confirms the assertions of Hypothesis 1 that limited experience with cyber operations creates an environment of uncertainty that prompts the use of heuristics.

7.3. A Brief Note on Domain Experts

As with the first experiment, the level of dread reflected by experts does not appear to rise significantly above the established baseline ($\bar{x} = 5.71$). When treatment groups are compared to the control, however, no statistical difference is noted. This suggests that experts maintain a consistent perception of cyberspace regardless of the treatment provided. This is corroborated by the fact that neither *External*, *Internal*, or *Trust* had a statistically significant impact on the outcome. This supports the argument that knowledgeable individuals would not create inappropriate stereotypes and appears. Consequently, this supports Hypothesis 2 which asserts that domain knowledge would result in lower levels of dread given the use of appropriate heuristics. However, it does not allow us to rule out the use of goal-oriented motivations as a means of maintaining bias-prone beliefs. Although findings are inconclusive, it opens the possibility of further inquiry into the decision-making processes used by experts. Past research demonstrates that experts formulate sound judgements while utilizing cognitive shortcuts. This, however, is dependent on the past information environment matching the present (Lau & Redlawsk, 2001).

The past decade has seen the growth of malicious interstate activities in cyberspace. Yet the aggressive use of these technologies existed long before events in Estonia (i.e. 2007). The context, however, has changed. Although the participants in Experiment 2 are most likely aware of these developments, the body of knowledge they possess through their formal education was developed from combating non-state actors[13]. While the authors are not arguing that the current mechanisms in place are insufficient, the possibility exists that they are not the most efficient and may limit the ability of states to act.

The inconclusive results of the second experiment should not be treated as a failure. Rather, it serves to inform future research how experiments involving domain experts ought to be designed. Specifically, it narrows the factors that may serve to influence the quality of expert judgements.

8. Tempering Bias and the Organization

The findings demonstrate that decision-makers can resort to motivated reasoning when formulating judgements regarding cyberspace. These tendencies have implications in two related ambits: (a) the cost consequences within the immediate context that decisions must be made, and (b) considerations for tempering bias to minimize cost consequences.

8.1. Consequences for Mobilization due to Perceptions of Dread

The context in which judgements regarding cyberspace are made occur within specific institutional boundaries. Policies are formed as a result of judgements undertaken within an organized context. On that note, consequences for this context are spread across two levels—the organization, and the state that the organization represents. When decision-makers resort to intuitive thinking, the probability that their perception of dread relative to a specific cyber issue is reasonably congruent with the actual level of dread varies according to three likely scenarios: (a) deflation, where the perceived threat is less than the actual threat; (b) congruence, where the perceived threat is congruent with the actual threat; and (c) inflation, where the perceived threat is greater than the actual threat.

Consequently, any of the scenarios above can frame the deployment of capabilities and tools in response to

[13]The curriculum used to teach Information Security in Computer Science departments is built on past efforts to combat hacking and cyber-crime. Frameworks such as the $(ISC)^2$ Common Body of Knowledge (Brecht, 2017) are examples of this. While some of the technical concepts are applicable to state actors, the political context may be unique and requires additional insights beyond these frameworks.

an impending event in the cyberspace (Dunn Cavelty, 2013). This has consequences for the resulting strategy for mobilization, which in turn comes with costs incurred by the organization.

As far as consequent mobilization strategies are concerned, there are three possibilities. First, it can occur in a form of a race to the extent that it may be intended as an offensive position. Second, it can occur in a form that meets the minimum capabilities necessary to be in a position of defence. Finally, it can occur in a manner where base capabilities are developed for decreasing vulnerabilities and increasing resilience to potential attacks. The underlying costs for the deployment of capabilities is a complex feat because approximating the symmetry between the perceived threat and the actual threat is not always optimal. An individual making the judgment who is at the same in a position of authority may either overestimate or underestimate the threat and could, therefore, impose material and immaterial costs for both the organization and the state.

Beyond theoretical assertions, the implications of (in)correctly providing security assessments ought to be considered considering the pace at which states are developing their respective cyber capabilities. While congruence has long been the desired state, the inherent characteristics of the domain compounds the persistent difficulty of assessing an adversary's intent and capabilities (Buchanan, 2017). The essential secrecy that obscures capabilities in cyberspace generates uncertainty on the part of assessor states. In the absence of knowledge regarding a potential adversary's true capabilities, states are left to form judgements based on past behaviour; judgements which may, in themselves, be subject to bias.

Interestingly, the need for insight into a potential adversary's capabilities may itself lead to greater instability. Regardless of whether a cyber operation is meant for intelligence gathering or as a first step of a larger offensive campaign, unauthorized access to a secure system is necessary. If discovered, the inherent characteristics of cyberspace do not permit the victim to determine which of the two objectives led to this event. At this point, the victim's own pre-existing beliefs may determine its potential response which could range from a tacit acknowledgement of routine (and expected) espionage to one of an escalatory spiral (Buchanan, 2017).

Consequently, the need for sufficient, if not optimal judgement, is mandatory on both sides of an interstate interaction. Parties must temper pre-existing beliefs to avoid engaging in either provocative action (aggressor) or unnecessary escalatory responses. Although the escalation of hostilities into the physical domain is unlikely, the disruption of cyberspace carries potential and avoidable costs.

8.2. Tempering Bias to Minimize Unnecessary Costs

This, in turn, begs the question: how can bias be tempered to minimize the likelihood of accruing costs? Our findings reveal the recurring use of heuristics at the individual level, which is critical because individuals who respond to cyber operations are assumed to be in a position of authority and able to make decisions which may, in turn, have repercussions for the organizations and states they represent. Indeed, judgments formed at the individual level frame decisions, and in turn, incur cost implications and related repercussions within the immediate social context for which the decision-maker is undertaking the decisions for. To this end, considerations for minimizing costs at the organizational level which emanate from inaccurate judgments at the individual level are inevitably linked with considerations for how micro-level processes contribute to macro-level outcomes.

However, our findings are limited to the extent that they do not consider the embeddedness of the individual within the organizational setting in undertaking decisions. Considering that decisions pertaining to cyber operations are undertaken within a context with institutional boundaries, it is possible that the direction of effects of the inaccurate judgments on the organization does not occur in one direction from the individual to the organization. Instead, we posit the likelihood that the organizations which individuals represent also possess certain attributes that can modulate individual biases. In the study of organizations, these micro-macro process considerations during uncertain contexts such as cyber operations are reminiscent of sensemaking within organizations (Weick, Sutcliffe, & Obstfeld, 2005), and how institutions enter the meaning-making processes of individuals in critical times (Weber & Glynn, 2006).

Sensemaking is broadly defined as a process by which people seek to make plausible sense of ambiguous, equivocal, or confusing issues and events (Brown, Colville, & Pye, 2015; Maitlis & Sonenshein, 2010) so as to be able to mobilize an appropriate response (Weick et al., 2005). Sensemaking has been studied particularly within the context of crises and emergencies (Maitlis & Sonenshein, 2010; Weick, 1993) where individual members of an organization become suddenly faced with a situation that is difficult to approximate with certainty, while at the same time being constrained by both information and time, as well as having to provide an immediate justifiable response. Given that the findings of this article infer the use of heuristics by individuals, it would also be interesting to extend the investigation regarding how intuitive judgements can be minimized during an overall sensemaking process that involves various cues from the organization that the individuals are a part of. Note that sensemaking is a means by which individuals are enabled to continuously stay in action amidst a disruptive shock (Weick et al., 2005) and to stay in action, individuals draw from certain "frameworks including institutional constraints, organizational premises, plans, expectations, acceptable justifications and traditions inherited from predecessors" (Weick et al., 2005). In cyber operations, as much as individuals with a position of authority articulate a judgment, it is also important to consider

the institutional boundaries that shape ways in which decisions are made. Empirically, it would be interesting to extend the experiment in a context where individuals are exposed to interactions with other individuals with the same organizational membership and see how such interactions may either weaken or strengthen the extent of ecological rationality in cyberspace operations.

Broadly, institutions influence the sense-making process (Weber & Glynn, 2006). These institutional influences are exerted concretely through various ways within the sensemaking process of the individual. For example, institutions can affect individual sensemaking through institutional policing, which may be embedded in the structural hierarchies and command-and-control approaches of the organization. This can be explored by considering how structure, templates, and other manifestations of organizational control may affect the way decision-makers in cyberspace make meaning. Sensemaking can also be triggered by the institution through interactions within groups that are oriented towards a specific organizational goal. Cyberspace operations are presently deemed ubiquitous for purposes that involve policy of the state, where conventions regarding its use have yet to converge and be institutionalized. This has an implication for the composition of groups involved in cyberspace operations, namely, those with positions of authority to enact certain policies related to cyberspace have a variety of backgrounds and turf representations. Future research may thus investigate how group composition, group dynamics, and group interaction among various individuals with specific types of judgments and biases can influence collective sensemaking, and ultimately temper the perception of dread in cyberspace.

9. Conclusions

The phenomenon of dread in cyberspace is a confluence of the domain's inherent characteristics and individual cognitive processes. The complex interdependencies within the domain generate a significant amount of uncertainty regarding the consequences of cyber operations aimed at disrupting its routine operations. While preventive measures may be taken to reduce its impact, its true scope cannot be determined beforehand. Consequently, individual decision-makers, particularly those lacking experience, resort to similar (though possibly unrelated) events to form judgements regarding the situation at hand. This causes decision-makers fall into the trap of finding correlations between events where none exist, resulting in the use of strategies that are deemed ecologically irrational. In doing so, the resulting judgements may either overestimate or underestimate the level of threat that can result in inappropriate policies which can complicate existing interstate relations.

To mitigate these issues, organizations to which these individuals belong should take appropriate steps to encourage accuracy-oriented reasoning on the part of decision-makers. While this does not eliminate the influence of bias, it increases the likelihood that assessments will be congruent to current realities. This minimizes the likelihood that costs will be incurred through the unnecessary development of capabilities or as the consequences of escalation between parties.

Interstate interactions in cyberspace is an emergent phenomenon that demands further analysis. While existing theories concerning material or systemic constraints have proven useful, it is necessary to move towards micro- and meso-level factors to better account for behaviour in this man-made domain. To this end, this article contributes to the on-going discourse by providing the initial steps needed to strengthen this line of inquiry.

Acknowledgements

We would like to thank Dr. Margarita Petrova for allowing us to conduct the initial pilot study for these experiments at the *Institut Barcelona d'Estudis Internacionals* (IBEI); the results contributed significantly to the development of the experimental instruments. We would also like to extend our gratitude to Nadiya Kostyuk, Dr. Christopher Whyte and the other members of the Digital Issues Discussion Group (DIDG) whose insights allowed us to better frame our arguments.

Conflict of Interests

The authors declare no conflict of interests.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.). *The economics of information security and privacy* (pp. 265–300): New York, NY: Springer.

Auspurg, K., & Albanese, J. (2015). *Factorial survey experiments*. Los Angeles, CA: SAGE.

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

Binmore, K. (2008). *Rational decisions*. Princeton, NJ: Princeton University Press.

Boutin, P. (2003). *Slammed! Wired Magazine*. Retrieved from https://www.wired.com/2003/07/slammer

Brecht, D. (2017). The CISSP CBK domains: Information and updates. *Infosec Institute*. Retrieved from http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/#gref

Brown, A. D., Colville, I., & Pye, A. (2015). Making sense of sensemaking in organization studies. *Organization Studies*, *36*(2), 265–277.

Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*. London: Hurst & Company.

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-

face behavioral testing. *Computers in Human Behavior*, *29*(6), 2156–2160.

Creppell, I. (2011). The concept of normative threat. *International Theory*, *3*(3), 450–487.

Crump, M., McDonnell, J. V., & Gureckis, T. M. (2013). Evaluating Amazon's Mechanical Turk as a tool for experimental behavioral research. *PloS one*, *8*(3), e57410.

Dawes, R. M. (1979). The robust beauty of improper linear models in decision making. *American Psychologist*, *34*(7), 571–582.

De Neys, W., Rossi, S., & Houde, O. (2013). Bats, balls, and substitution sensitivity: Cognitive misers are no happy fools. *Psychonomic Bulletin & Review*, *20*(2), 269–273.

Dean, B., & McDermott, R. (2017). A research agenda to improve decision making in cyber security policy. *Penn State Journal of Law & International Affairs*, *5*, 29–164.

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th international conference on cyber conflict* (pp. 1–13). Tallinn: IEEE.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, *114*(11), 2825–2830. doi:1700442114

Farrell, H., & Glaser, C. L. (2017). The role of effects, saliencies and norms in US cyberwar doctrine. *Journal of Cybersecurity*, *3*(1), 7–17.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Gigerenzer, G. (2008). Why heuristics work. *Perspectives On Psychological Science*, *3*(1), 20–29.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. *Annual Review Of Psychology*, *62*, 451–482.

Goldman, E., & Arquilla, J. (2014). *Cyber analogies*. Monterey: Naval Postgraduate School.

Goldman, R. (2017). What we know and don't know about the international cyberattack. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html?_r=0

Hafenbradl, S., Waeger, D., Marewski, J. N., & Gigerenzer, G. (2016). Applied decision making with fast-and-frugal heuristics. *Journal of Applied Research in Memory and Cognition*, *5*(2), 215–231.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Healey, J. (2016). Winning and losing in cyberspace. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), *2016 8th international conference on cyber conflict* (pp. 37–49). Tallinn: IEEE.

Holmes, M. (2015). Believing this and alieving that: Theorizing affect and intuitions in international politics. *International Studies Quarterly*, *59*(4), 706–720.

Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *2013 5th international conference on cyber conflict* (pp. 451–470). Tallinn: IEEE.

Jardine, E. (2015). *Global cyberspace is safer than you think: Real trends in cybercrime*. Waterloo: Centre for International Governance Innovation.

Jardine, E. (2017). *Sometimes three rights really do make a wrong: Measuring cybersecurity and Simpson's paradox*. Paper presented at the Workshop on the Economics of Information Security, La Jolla, CA.

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*, *2*(1), 64–87.

Jensen, B., Maness, R. C., & Valeriano, B. (2016). *Cyber victory: The efficacy of cyber coercion*. Paper presented at the Annual Meeting of the International Studies Association, Atlanta, USA.

Jervis, R. (2017). *Perception and misperception in international politics*. Princeton, NJ: Princeton University Press.

Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, *4*(1), 53–71.

Kahneman, D. (2003). A perspective on judgment and choice—Mapping bounded rationality. *American Psychologist*, *58*(9), 697–720.

Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.

Krosnick, J. A., Li, F., & Lehman, D. R. (1990). Conversational conventions, order of information acquisition, and the effect of base rates and individuating information on social judgments. *Journal of Personality And Social Psychology*, *59*(6), 1140–1152.

Kruglanski, A. W., & Gigerenzer, G. (2011). Intuitive and deliberate judgments are based on common principles. *Psychological Review*, *118*(1), 97–109.

Kruglanski, A. W., Orehek, E., Dechesne, M., & Pierro, A. (2010). Lay epistemic theory: The motivational, cognitive, and social aspects of knowledge formation. *Social and Personality Psychology Compass*, *4*(10), 939–950.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. S. Kramer, Stuart H.; Wentz, Larry (Eds.), *Cyberpower and national security* (pp. 24–42). Dulles, VA: Potomac Books.

Kunda, Z. (1990). The case for motivated reasoning. *Psychological Bulletin*, *108*(3), 480–498.

Lau, R., R., & Redlawsk, D. P. (2001). Advantages and disadvantages of cognitive heuristics in political decision making. *American Journal of Political Science*, *45*(4), 951–971.

Lavrakas, P. J. (2008). Likert scale. *Sage Research Methods*. Retrieved from http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n273.xml

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. *Psychological Bulletin*, *125*(2), 255–275.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.

Maitlis, S., & Sonenshein, S. (2010). Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of Management Studies*, *47*(3), 551–580.

Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces & Society*, *42*(2), 301–323.

Martignon, L., & Hoffrage, U. (1999). Why does one-reason decision making work? In G. Gigerenzer, P. M. Todd, & T. A. R. Group (Eds.), *Simple heuristics that make us smart* (pp. 119–140). New York, NY: Oxford University Press.

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. New York, NY: Cambridge University Press.

Mercer, J. (2010). Emotional beliefs. *International Organization*, *64*(1), 1–31.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, *70*, 153–163.

Perrone, J. (2001). Code Red worm. *The Guardian*. Retrieved from https://www.theguardian.com/world/2001/aug/01/qanda.janeperrone

Perrow, C. (2011). *Normal accidents: Living with high risk technologies*. Princeton, NJ: Princeton University Press.

Pytlak, A., & Mitchell, G. E. (2016). Power, rivalry, and cyber conflict: An empirical analysis. In K. Friis & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 65–82). London: Routledge.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1/2), 4–37.

Roach, S. C. (2016). Affective values in international relations: Theorizing emotional actions and the value of resilience. *Politics*, *36*(4), 400–412.

Rousseau, D. L., & Garcia-Retamero, R. (2007). Identity, power, and threat perception—A cross-national experimental study. *Journal of Conflict Resolution*, *51*(5), 744–771.

Savage, L. J. (1972). *The foundations of statistics*. New York, NY: Dover Publications.

Sheldon, J. B. (2014). Geopolitics and cyber power: Why geography still matters. *American Foreign Policy Interests*, *36*(5), 286–293.

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, *41*(3), 72–109.

Slovic, P. (2016). *The perception of risk*. New York, NY: Earthscan.

Sniderman, P. M. (2011). The logic and design of the survey experiment. In J. N. Druckman, D. P. Green, J. H. Kuklinski, & A. Lupia (Eds.), *Cambridge handbook of experimental political science* (pp. 102–114). New York, NY: Cambridge University Press.

Taber, C. S., Lodge, M., & Glathar, J. (2001). The motivated construction of political judgments. In J. H. Kuklinski (Ed.), *Citizens and politics: Perspectives from political psychology* (pp. 198–226). Cambridge: Cambridge University Press.

Thompson, V., Turner, J. A., & Pennycook, G. (2011). Intuition, reason, and metacognition. *Cognitive Psychology*, *63*(3), 107–140.

Todd, P., & Gigerenzer, G. (2012). *Ecological rationality: Intelligence in the world*. New York, NY: Oxford University Press.

Turner, J. R., & Thayer, J. F. (2001). *Introduction to analysis of variance: Design, analysis, & interpretation*. Thousand Oaks, CA: Sage Publications.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford; New York, NY: Oxford University Press.

Weber, K., & Glynn, M. A. (2006). Making sense with institutions: Context, thought and action in Karl Weick's theory. *Organization Studies*, *27*(11), 1639–1660.

Weick, K. E. (1993). The collapse of sensemaking in organizations—The Mann Gulch disaster. *Administrative Science Quarterly*, *38*(4), 628–652.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, *16*(4), 409–421.

Zetter, K. (2016). Inside the cunning, unprecendented hack of Ukraine's power grid. *Wired Magazine*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

About the Authors

Miguel Alberto Gomez is Senior Researcher with the Center for Security Studies (CSS) at the ETH in Zurich and is a doctoral candidate at the School of Law and Politics at Cardiff University. His current research focuses on political psychology and its implications for the coercive use of cyber power.

Eula Bianca Villar is a Researcher and PhD Candidate at the Department of Business and Technology in La Salle Universitat Ramon Llull in Barcelona, Spain. She was a grant recipient of the European Union Marie Curie Fellowship for the project "A Networked and IT-Enabled Firm's Approach to Crisis Management". Her research focuses on organizing processes in extreme environments.

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 73–82
DOI: 10.17645/pag.v6i2.1338

Article

Crossing the Digital Divide: Monism, Dualism and the Reason Collective Action is Critical for Cyber Theory Production

Christopher Whyte

L. Douglas Wilder School of Government and Public Affairs, Virginia Commonwealth University, Richmond, VA 23284, USA; E-Mail: cewhyte@vcu.edu

Submitted: 31 December 2017 | Accepted: 12 February 2018 | Published: 11 June 2018

Abstract
In studying topics in cyber conflict and cyber-security governance, scholars must ask—arguably more so than has been the case with any other emergent research agenda—where the epistemological and ontological value of different methods lies. This article describes the unique, dual methodological challenges inherent in the multifaceted program on global cyber-security and asks how problematic they are for scholarly efforts to construct knowledge about digital dynamics in world affairs. I argue that any answer to this question will vary depending on how one perceives the social science enterprise. While traditional dualistic perspectives on social science imply unique challenges for researcher, a monistic perspective of Weberian objectivity does not. Regardless of one's perspective, however, the most important steps to be taken at the level of the research program are clearly those focused on constructing the trappings of community. To this end, I outline steps that might be taken to develop a range of community-building and -supporting mechanisms that can simultaneously support a micro-foundational approach to research and expose community elements to one another. Doing this stands to better opportunities for the production of knowledge and direct researchers towards fruitful avenues whilst shortening gaps between the ivory tower and the real world.

Keywords
cyber; dualism; epistemology; monism; ontology; philosophy of science

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

For almost half a century, new information and communications technologies (ICT) based on packet-switching and related network-oriented design features have worked to rewire the international system. The digitization of global infrastructure has transformed the constitution of global commerce, social connections and security relationships alike. Given the scope of the impact of this most recent information revolution, it seems reasonable to assert that cyber-security—i.e. the security of socio-technical systems and, more specifically, practices involved therein—is, thus, a policy field aimed at more than *only* technical, organizational or national security. Wherever ICT undergird societal functions, questions of cyber-security abound. And, since ICT have also augured unique changes to the global information environment, cyber-security analyses and prescriptions must necessarily consider the broader intersection of technology and the normative fabric of world affairs. In short, the scope of the scholarly research program on cyber-security governance, conflict and economics is immense.

And yet, the broad field of cyber issues studies faces unprecedented foundational challenges with respect to the construction of new knowledge. Specifically, and perhaps moreso than has been the case with any other emergent research agendas in recent history, scholars studying cyber matters must consistently grapple with distinct epistemological and ontological questions. Given the inherent difficulties in obtaining data and validating observational inferences, how can we presume to know what we think we know? If the link between our empir-

ical resources and inferred findings is open to question, how can we be sure that the phenomena and dynamic forces we study are as we see them? All social scientists must confront such issues in their approach to understanding the world around them and, from Hutchins (1995) seminal work on cognition to Mindell's (2002) cybernetics exploration of interacting control systems, there exists a rich literature on both the challenges and value proposition inherent in studying the interaction of technology and human systems.

But with cyber-security issues the potential obstacles are uniquely pronounced. While it is certainly possible to study, for instance, traditional questions of bureaucracy and politicking around Internet-oriented bodies without considering technological variables, a great deal of work is inevitably aimed at assessing technology as it supports, impacts and enables kinetic human interactions. As such, a substantial element of the academy in this area must attempt to link technological empirical foundations with socio-physical outcomes.

This article asks how problematic core methodological challenges commonly identified by cyber-security researchers really are and describes steps that might be made to improve prospects for knowledge construction at the level of the research program. Over and above environmental problems in obtaining data, the cyber-security research program suffers from acute attributional challenges. To date, scholars employing data obtained through public-sphere observation or in collaboration with technology vendors have taken one of two approaches to data collection, with scope conditions being set by either socio-kinetic or technical system details. Though both approaches are promising, the basis of each suggests inherent challenges in cross-validating results and building macro theory. It is often extremely hard to attribute digital patterns to sociopolitical wherewithal; likewise, inquiry that selects on specific actors in world politics is often unable to capture the scope of covert digital actions. In essence, though existing research certainly stands to contribute to the body of knowledge on cyber politics and cyber-security governance, contradictory bases for investigation combine with the domain's unique attribution challenges to make analysis of sociopolitical phenomena systematically difficult.

The challenges before the multi-faceted cyber research program are not new and are novel only insofar as ICT regularly produce a disconnect between domain-specific actions or outcomes and real world ones. In truth, the question of methodological approach to cyber issues is one of reconciling existing perspectives with advancing work in such a way as to develop a scientifically healthy research program. In the sections below, I describe competing perspectives on the ability of social science approaches to build a body of knowledge that impartially describes the real world. I point out that while dominant dualistic perspectives on social science suggest that attribution challenges for empirical work in the cyber field are severe, a monistic interpretation of the social science enterprise implies they are problematic only insofar as scholars should ideally be able to gauge the shape of all elements of the real world for purposes of forming impressions. I then argue that, regardless of the perspective one adopts, scholars in the burgeoning cyber-security research program should take steps to develop a range of community-building and -supporting mechanisms that can simultaneously support a coordinated micro-foundational approach to knowledge construction and expose community elements to one another. The sections below outline the case for this in greater detail and make a series of specific recommendations.

The remainder of this article proceeds in five parts. First, it considers the nature and aims of the cyber-security research program within the social sciences. Then, it briefly discusses competing philosophical perspectives on the constitution of knowledge in research on the world around us and fleshes out unique, dual attributional problems that many researchers must inevitably face in efforts to link technical foundations to socio-physical context. Thirdly, the article discusses open source research in the broader program of investigation and adjudicates on the degree to which unique attributional problems matter. Finally, it argues that, regardless of one's perspective on the nature of the social science enterprise, a community-oriented organization of research efforts is critical for efforts to construct macro theory and generate meaningful inference. Here, I make specific suggestions at the level of the research program, before concluding.

2. The Shape and Focus of Digital Studies Research

Cyber studies constitute an immensely broad field of investigation. This is a necessary condition because of the unique foundational feature of the network technologies that lie at the heart of the field. Simply put, changes to global society in this most recent information revolution have emerged from a multiform application of new design features to the full range of societal infrastructure. Information technology is crosscutting to such a degree that it is the rare social, political or economic issue that has not been impacted. As such, cyber studies possess an incredible broad substantive remit. At the highest level, we might consider this remit to include the dynamics of technology adoption across global society (Choucri, 2012), the role of governments in problematizing and meeting cyber challenges (see among others, Knake, 2010; Nye, 2014; Stevens, 2017), the resultant management of international security and the fundamental institutional, technological and societal prerequisites of security.

Though it might otherwise do to categorize the cyber studies research program into different academic areas of focus, from global cyber-security governance (Choucri, Madnick, & Ferwerda, 2014) and cyber conflict mechanisms (see among others, Buchanan, 2017; Gartzke & Lindsay, 2015; Valeriano & Maness, 2015) to the organization of social movements in virtual spaces (for in-

stance, Beyer, 2014) and the cutting edge of ICT development, the fact of the matter is that methodological issues and imperatives in this vein emerge from a simple proposition—that the most recent information revolution has fundamentally altered not only the nature of human interactions on a global scale, but also the constitution (i.e. the context) thereof. If this proposition is accurate or even accepted in part, then the field's remit is truly unique. Different from research sub-programs across the social sciences that study specific tools of human interaction, the study of world politics as couched in the context of ICT adoption and integration is the investigation of transformed environmental conditions on a global scale. Though man-made, the evolving digitization of global infrastructure presents as *both* an exogenous determinant of human interconnections and an endogenous modifier of specific relationships.

It would not do here to go on without recognizing that there exists a rich and well-trodden literature on the interaction of human institutions and the tools they employ. Nestled in the field of science and technology studies, research on cybernetics has for many decades described the manner in which technology is not simply a material feature of the world that humans engage with in the course of our actions (see among others, Mindell, 2002; Mindell, Segal, & Gerovitch, 2003; Wiener, 1961, 1988). Rather, technology is a tangible variable that both shapes human agency and determines the normative context of human interactions (Hutchins, 1995). What's unique about the most recent information revolution is the twofold manner in which new ICT both provide for human interaction substantially detached from real world context and do so systematically at the global level. Thus, while literature that takes reference from work on cybernetics, social network theories and more is relevant to the research program on cyber-security—and, indeed, has recently been the focus of a handful of unique contributions to the field—the methodological challenges facing scholars today is of unique scale.

The result of such a dynamic is reasonably clear. Though, again, it is possible to study cyber effects without looking beyond what some have called the "real-kinetic" empirical dynamics of world affairs (Choucri, 2012), much of the broad-scoped cyber studies research program will enduringly be required to look at the intersection of specific ICT usage, implementation dynamics and resultant human behavior. In reference to a well-developed program of study on the nature of power and position in international relations (Barnett & Duvall, 2005), it seems reasonable to bound such work in two ways. First, much cyber-security research aims to understand how ICT play a role in augmenting human interactions of various kinds. Some, for instance, has attempted to map out the shift in how humans and human institutions problem-solve given today's global network-centric environment (see among others, Amoore, 2009; Dreyfus, 2008; Galloway & Thacker, 2007; Shaviro, 2003). Here, researchers are already grappling with the challenge of matching data on the use of ICT with a range of sociopolitical outcomes. And again, as is broached further below, there exists in cybernetics scholarship a nuanced basis for examining closed systems of technology incorporated into human structures. Second, yet other work aims to understand how ICT might act to alter—either directly or reflexively through societal reactions to the information revolution—the context of those interactions. Here, a range of research sub-programs in the psychology, biology, business and sociology fields has emerged to assess the manner in which the most recent information revolution has fundamentally changed patterns of human behavior. In both cases, the need to link information on direct human interactions with ICT to related outcomes is clear. Across the board, however, this imperative presents as a unique challenge wherein attribution of digital actions to various kinds of outcomes is not only difficult methodologically, but fundamentally linked with scholars' ability to infer.

3. The Digital Divide: With Cyber Research, How Do We Know What We Know?

When it comes to linking human behavior enabled via use of ICT, there are two distinct challenges for the researcher. One of these is technical, the other preferential. The first is that links between digital realities and human actions are tenuous. Whether the subject of focus is patterns of cryptocurrency usage (Sat, Krylov, Evgenyevich, Kasatkin, & Kornev, 2016) or the attribution of cyber attacks (Rid & Buchanan, 2015), tying evidence of digital behavior to human input is difficult. The second challenge is that resources necessary for doing so are often hidden behind not only technical barriers, but also socio-institutional ones.

With regards to attribution of cyber activities, much has been written across both the technical and social sciences. For the purposes of social scientists, it is enough to say that attribution of digital actions can be immensely challenging simply because of the layered manner in which relative ease in masking digital signatures meshes with the additional difficulties involved in linking virtual actions to human behavior (Guitton & Korzak, 2013). Technical attribution—i.e. the linking of cyber actions with indicators of action instigated by humans or human-programmed systems—is not dichotomous. It would be disingenuous to say that a measure of technical attribution of digital actions either does or does not point the finger at specific causes of disruption or compromise. Attribution short of linking ICT usage to human agency runs the full gamut from technical abilities to convince investigators of a given pattern of action to the much rarer ability to lay out a case that an informed public audience would be hard pressed to argue with (Geers, 2010). This is made yet more problematic given that opponents are not unitary. As Rid and Buchanan (2015) point out in their discussion of Moonlight Maze as an example, efforts to confirm attribution evidence pointing to Russian security

services ran into the problem of a clear compartmentalization of knowledge of offensive operations within the Russian government. Some operators knew about the expansive espionage campaign; many did not.

And yet, when it comes to attribution of digital actions, technical demonstration of the origination thereof is just part of the challenge. Indeed, it is arguably the lesser part of the challenge. Even where data is made available wherein technical attribution is possible to a high degree of certainty, there inevitably exist additional certitude problems for any scholar or analyst attempting to link digital actions to sociopolitical ones. For scholars, such intelligence gathering as a component part of cyber research is particularly challenging, as we must often trust (given a certain ability to control for uncertainty) the nature of information that attributes particular actions to actors. This naturally speaks to a higher-level problem with the attribution of digital dynamics to real-kinetic ones such that research on the broad gamut of digital issues are faced with unique ontological problems, namely that sources and providers of relevant information suffer from a broad range of measurement and reliability problems.

In research on cyber conflict, in particular, it is apparent to a broad range of scholars that barriers across which lie the ability to generalize about digital actions are more opaque than they are with traditional areas of security work (see among others, Kello, 2013; Rid & Buchanan, 2015; Valeriano & Maness, 2014). The nature of global network infrastructure as being substantially privately owned means that access to Internet traffic data and innumerable related metrics is hidden behind preferential access walls. In essence, robust analysis is difficult for those operating in the public sphere because we must contend with the incentives that both private industry and government operators have to either not report or misrepresent what they know about the digital domain. Private firms must consider their reputation, their standing with stakeholders, the value of their intellectual property and a maze of compliance requirements when deciding how to report information and whether or not to share data with academics and the public (Byres & Lowe, 2004; Sgouras, Birda, & Labridis, 2014). Moreover, operators willing to share relevant data for use in research often enforce rules about how data can be used (to enhance their public standing, for instance) and government sub-organizations inevitably favor intelligence and defense community research in their decision-making. What topics of interest do not suffer from this issue—such as the use of ICT by activists for inherently public-facing efforts (see, for instance, Morozov, 2012; Shirky, 2008; Yang, 2009)—are virtually unique in that observation of digital actions does not require interaction with a gatekeeper of some kind.

These dual challenges to research progress constitute a digital divide wherein linking observation of digital dynamics to sociopolitical corollaries is systematically difficult, both technically and logistically. Given these foundational challenges with linking the growing base of knowledge about a range of digital issues with actual patterns of human interaction in the digital domain, how can scholars possibly know what we think we know (Jackson & Nexon, 2013)? In particular, beyond the scope of individual projects that find unique ways to obtain, validate and employ data, how can an entire field of study act to remedy the clear problem of socio-technical gatekeeping that mires research—in the aggregate—in ontological uncertainty?

4. How Problematic Are Such Challenges? The Dualist and Monist Perspectives

To consider these questions, it is necessary to consider different philosophical perspectives on the nature of social science and the development of effective research programs. Broadly, effective assessment of a research program's health and viability demands consideration of the nature of the relationship between knowledge held and assumed by scholars, on the one hand, and the empirical nature of the world around humans on the other. Do our observations and subsequent inferences accurately describe the real world? Or do they, since human consciousness and operation is inherently a function of the subjective way in which our minds view particular parts of the world, lead to the development of a base of knowledge that only makes sense in the context of human biases and interpretations? Recognizing these competing perspectives and subsequent implications for the knowledge generation process is critical for adjudicating on the best paths that might help remedy the cyber-security research program's inherent ontological challenges.

To be clear, in the immense literature on the philosophy of science (and particularly on the ontological challenges of scholarly research), the questions posed above in no way suggest some division between an idealistic view of knowledge creation by researchers and a more pragmatic one. The assertion that human stores of knowledge do not accurately reflect the world around us is simply a function of recognizing the role that prior knowledge plays, in the form of biases and preconditioned modes of problem solving, in shaping research design and interpretation (see among others, Bennett, 2013; Lake, 2011; Sil & Katzenstein, 2010). In assessing a unique dynamic scientifically, researchers are invariably prompted to address methods, practices and results that the broader research community assess are adjacent to the current venture. And regardless of how effective a given research design is at preventing the introduction of bias, interpretation of results and the subsequent task of placing new knowledge in the context of a broader knowledge base inevitably prompts researchers to interact with a broader construct (Habermas, 1987). This is particularly the case given that interpretation of results is rarely the task of individual researchers or investigative teams, but is inevitably at some point a task undertaken by broader elements of a research community

that need not observe scientific controls in their attempt to consensually place new knowledge amongst the rest. The result is a disconnected body of knowledge that only represents the real world in the context of the practices of those who developed that knowledge in the first place (Jackson, 2008). This notion of the relationship between empirics and human knowledge is called *dualism*.

By contrast, *monism* pushes back on the narrative of dualism as reflecting an inevitable divergence in the shape of the real world and human understanding of the real world. Monism is the perspective that human knowledge and the real-kinetic landscape of the world around us are one and the same (Weber, 2017). This is not because advocates of monism reject the notion that bias can infect and skew the results of the scientific enterprise. Rather, monists recognize that the parameters of what humans *might* understand about the world around us is inherently a function of how we categorize "things" in the world (Weber, 1904). Humans give meaning to what we are studying by identifying them to begin with. Thus, focusing purely on real-kinetic events, dynamics and fundamentals in the world around us allows us to understand *both* the "things" that we understand to be in the world (i.e. the landscape of the world around us) and the knowledge we hold about those things (Jackson, 2008). Whereas dualism holds that there is an objective reality about the real world that is separate from human knowledge of the world, monism holds that understanding critical junctures and events via observation allows us to understand the world in such a way that our body of knowledge is essentially congruent with the condition of the world.

The debate over the nature of the social science enterprise between monists and dualists has seen a range of developments in recent years. Pushing back against the correlative narrative of both classical and seminal dualists, in particular, a series of works (for instance, Bennett, 2010) and conference publications (Mackay, 2007) have organized around the concept of factual or speculative materialism. Advocates of such thinking propose that objects are not elements of "the real world" to be assessed and characterized as one thing or another, but are multi-factual constructs as potentially complex as human beings (Bryant, Snricek, & Harman, 2011; Phetteplace, 2010). Thus, far from accepting the notion that inferential analysis cedes knowledge about a world in which humans operate, speculative materialists (or realists) join others in conceptualizing systems wherein humans are not unique as animate objects.

5. Dualism and Monism as Competing (Approaches to the) Social Sciences

In a discussion of the ontological challenges faced by the cyber-security research program, why should we care about competing philosophical perspectives on the nature of the social science enterprise? Simply put, advocacy of one or the other leads to a diverse set of prescriptions on what kinds of scholarly activities are most likely to build a useful, accurate and accessible store of knowledge by the academy. The shape of such activities, in turn, suggests the degree to which the challenges inherent in undertaking empirical work on many cybersecurity topics are problematic for the development of the research program.

Dualist perspectives on the social sciences are, by far, more commonplace than are monist ones. Though most social science work from the mid-20th century onwards tends to self-describe as "positivist" (or variations thereof) in nature, the reality is that most scholars reject the notion that observation is synonymous with the shape of the real world. Rather, most are dualists of one kind of another that essentially seek to dispense with the character of their own perspectives in order to better understand empirically the environment in which humans exist and interact. Again, though most social scientists today would likely identify as positivists, the better term to use would, according to Jackson (2008), be *neopositivists*.[1] Such scholars, divided as they are on a range of philosophical points (see Blaug, 1975; Fuller, 2004; see also Kuhn, 1970; Popper, 1970), nevertheless uniformly reject the monism of positivism and agree to the central importance of one particular scholarly activity as critical for the generation of knowledge that increasingly describes the real world accurately—falsification (Lakatos, 1976). Falsification, simply put, is the design of observational scientific procedures such that different hypothetical suppositions can be rigorously tested and eliminated if certain conditions are not met. It is an activity that, by definition, dictates the existence of a divide between human activity in research practices and the world around us.

By contrast with prevailing dualist perspectives on the social sciences, monist ones reject the entire notion that what we see in the world around us is some kind of neutral tapestry on which humans draw and from which we take reference. As Jackson (2008) describes, monism's most well-known proponent—Max Weber—argues that there can be no social science enterprise without pre-defined and assumed socio-cultural understanding of what is actually under study (Weber, 1904). Here, Weber addresses the most common criticism of dualist—and particularly neopositivist—approaches to research. Since neopositivism necessitates the dispensation of human inputs to the observational process through some form of falsification in research design, it intrinsically demands some kind of agreed-upon standards of evidence and objectivity. In a comparative study, this would manifest in one or several agreed-upon methods for operationalizing both the dependent and inde-

[1] Though they are awarded singular focus in treatments of dualistic perspectives on the social science enterprise, neo-positivists are not alone in their view of human knowledge and real world dynamics being inherently separate. Jackson (2008) describes both critical realists and "partisans of 'communicative action'" (p. 130) as belonging in the dualist category.

pendent variables. This, of course, is the greatest weakness of dualism as social science. There is simply no way that scholars can confirm the validity of a given hypothesis, no matter the amount of otherwise seemingly-robust testing it endures, as *more correct* in its representation of the world around us (Hacking, 1999). Moreover, the requirement that researchers pick some measurements of the real world over others inherently weakens the falsification process in some instances in that hypotheses may constitute conventional wisdom or consensus positions in its parts. Such hypotheses might survive in scholarship because its construction is uncontroversial, regardless of the shape of evidence brought to bear. The Democratic Peace Theory is a paradigmatic example of such a hypothesis wherein the component elements are (or at least were for many years) broadly considered common sense without further operationalization (see among others, Layne, 1994; Risse-Kappen, 1995; Rosato, 2003).

The solution to such an inescapable inability to ever perfectly, objectively describe the world around us, according to a monist perspective on the social science enterprise, would be not to try. Rather than focus on accurately describing the world around us as a set of facts, scholars should assess ideal-type constructions of our world with consistent analytic premises (Lindbekk, 1992). These premises need not be free of bias in any way, but simply must be consistent and logically applied across research (Jackson, 2008). Such work is then judged to be more or less meaningful to the broader body of human knowledge given the degree to which is can successfully persuade an audience of diverse persuasions. In other words, good social science is that which can persuade the most people that hold contradictory perspectives on how the world works. Already in the well-dispersed literature on the information revolution, there are examples of monistic research designs implemented in compelling and robust fashion (see among others, Anderson, Kearnes, McFarlane, & Swanton, 2012; Balzacq & Dunn Cavelty, 2016; Berry, 2015). Whereas empirical efforts like those of Valeriano and Manesss (2015) rely on a series of assumptions external to the methods and data employed in analysis, work that draws upon socio-spatial theories and frameworks is able to nest assessment of a given phenomenon within fixed parameters only relevant to the study at hand. As a result, while opportunities for correlative findings pertaining to such phenomena are lacking, there are clear pathways to thick description thereof.

6. Open Source Research and Challenges for the Development of the Research Program

Given these competing approaches to knowledge generation and the organization of research programs, how problematic are barriers to effective observation of digital dynamics for researchers? While it is possible that individual researchers, research teams and institutions might find access to proprietary information that allows for unique analysis of a given phenomenon, the reality is that most investigation in the cyber-security research program is done—and will enduringly be done—off the back of open source data collection. Whether mining event data from news reports and wire feeds (as in Radford, 2016) or conducting ethnographic research into the shape of communities and institutions (as in Sowell, 2012), social scientists interested in undertaking work in this domain must largely do so absent the special access conditions held by stakeholders in the domain. Academic researchers may occasionally be allowed unique access to private data (for instance, King, Pan, & Roberts, 2013; Kostyuk & Zhukov, 2017) and are often supported by grants that enhance the power of observation at the level of the researcher, but they do not hold specialized roles—as do Internet service providers, intelligence entities or private cyber-security vendors, for instance—that might enduringly allow for access to information that could serve to bridge the attribution gap described above. A range of promising work has been done in the social sciences that empirically selects on either sociopolitical dynamics (for instance, Valeriano & Maness, 2015) or technical details (e.g. Mezzour, Carley, & Carley, 2015) as the basis for generalizing about a given phenomenon. In almost all cases, however, there exist clear shortcomings in the ability of researchers to validate their findings such that inference is possible. And while some creative solutions exist that have bridged the digital methodological divide at the level of discrete research projects, it is difficult to see how such challenges might be remedied at the level of the research program.

For dualists, the specter of such an enduring organizational and validating challenge in cyber research is particularly problematic. How research programs should and do emerge is hotly debated by both seminal and contemporary dualist philosophers, but the general idea is that research programs are layered constructions of knowledge wherein peripheral hypotheses linked with core theses are tested in order to advance the state of a given field (Jackson, 2008). Sometimes, hypothesis testing leads to such rapid advancement in the shape of specific knowledge that there is a revolution in general knowledge—in the theoretical bases of a research field. The manner in which this occurs is the subject of classical debate between thinkers like Kuhn and Popper. Regardless, the idea is roughly similar across the board and so it is easy to see why ontological problems in work focused on ICT and their impact dominate so completely. Systematic barriers to the robust implementation of falsification-based research designs are an impediment to the process of knowledge construction. Adding to this, the cyber-security research program is still in its infancy. The shape of general knowledge at the heart of the research program is unclear, suggesting that efforts to improve our knowledge base by rejecting pre-existing theory are premature and that, moreso than is common with established areas of scholarship, there is a strong imperative to articulate macro-theoretical perspectives. Taken to-

gether, the path ahead for efforts to construct an effective dualist social science research program is laden with likely pitfalls and uncertainty.

For monists, these challenges are less severe. Again, the monistic position is that scholars should assess ideal-type constructions of our world with consistent analytic premises rather than simply aim to describe the real world as a set of facts. As long as a researcher's premises are consistent and logically applied across research in the form of a clearly delineated analytic framework, good social science work is possible. The point is simply to persuade the most people that hold contradictory perspectives on how the world works. From this point of view, objective research on and around the cyber domain is entirely possible without specific systematic remedy to the ontological problems inherent in observational work across the board. Indeed, some such research is already emerging. Though it does not generalize on global patterns of cyber conflict, Balzacq and Dunn Cavelty's (2016) exploration of the applicability of Actor-Network Theory (ANT) demonstrates the manner in which network functionality and control can be shaped by fluid syntactic threats in the form of malware.[2] Such work has clear value to strategic planners. Punctuated successes like this that bridge the digital divide are as meaningful for the research program as would be a broad-scoped revolution in approaches to cross-validation and data obtainment within the field. Certainly, a monistic perspective might recognize that any effort to advance access to the means of observing all aspects of the domain is conducive to good social science insofar as greater exposure to information about the world will lead to a proliferation of world views and, thus, incentivize the production of more compelling analytic work. But lack of full observational data about the world around us is not necessarily a hard barrier to continued development of the research program. Indeed, even given a revolution in methods of approach to correlative research, speculative investigation seems better suited to providing scholars the means to consider the validity of non-obvious relationships.

7. Recommendations: A Need for Community and Collective Action

Obviously, the field of scholars interested in conducting cyber-security research—broadly construed—is diverse and destined to be constituted of elements that value different approaches to knowledge construction. This is perhaps more the case here than with other traditional fields of study within the social science enterprise given the degree to which the most recent information revolution has transformed the social, political and economic substrates of world affairs in a crosscutting fashion, attracting students of varied interests and research inclinations. Nevertheless, I argue that there exists a set of steps to be taken that addresses the imperatives of competing philosophical perspectives on approaches to be taken in such research in common. Specifically, these steps involve the construction of strong community mechanisms around the research program that can *both* encourage adoption of a micro-foundational framework for developing new dualistic research projects and expose diverse scholarly sub-communities (and their perspectives) to others in such a way that expands prospects for what monists might call a robust social science focused on cyber-security issues. Indeed, I posit that developments akin to those suggested below are necessary for the viability of a cross-cutting digital studies research program specifically because knowledge construction at the level of the program is impossible—regardless of a given scholar's dualistic or monistic conceptualization of the social science enterprise in this vein—without consensus and the mechanisms thereof.

Scholarly Responsibility. To some degree, the simplest mechanism for advancing the research program is quite simply continued and improved commitment to responsible scholarly practices at the level of the researchers and the research project. At present, the diverse cyber-security field is a somewhat fragmented beast insofar as best practices are not determined via reference to the research program so much as they are via reference to the traditional academic domains from which individual researchers hail. This is no clearer than with the case of standards for replication of investigatory work and hypothesis testing. At least at the level of the researcher, a voluntary commitment to adopt in-group replication as a basic standard for publication of evidence would help remedy the clear issue that arises from unique proprietary access to data that cannot be publicly provided. In essence, a commitment to allow an independent group of collaborators *not* co-investigating a given project should be common practice as a means for controlling for lack of replication options during and after the publication process (where data from vendors, interviews, etc. are used in a central role). Pre-publication replication would make work more credible and would tie scholarly reputation to a given research finding beyond what author(s) or results-*sans*-data might. Secondarily, the field should adopt standards for claiming inference from the medical and psychology fields wherein multiple independent studies (i.e. datasets) are employed and rated based on their credibility (see Francis, 2012; Maxwell, Lau, & Howard, 2015). Naturally, such efforts should be supported and bolstered via the purposive organization of research forums and conference programs around such principles of community cross-validation and debate. Likewise, jour-

[2] For a full introduction to ANT, see Latour (2005). Latour outlines ANT as both related to and a pushback against the monism described by Jackson (2008) and others. Latour sees most social science as being overly laden with suppositions about the character of actors and objects in world affairs. In essence, he argues for austere form of approach to understanding sociological assemblages—including security assemblages—in the world based on a materialist view of connections that cede meaning.

nal special editions and special conference proceedings would do well to be planned across outlets in coordination with such forums.

Common Resources. Further, the cyber-security research program should support efforts to build common resources for coordination. Particularly given that the field largely lacks core theoretical division in the way that traditional academic areas of focus do at this juncture, a micro-foundational approach to the production of knowledge—regardless of one's perspective on the nature of good social science—is necessary for the construction of robust foundations for future research. In this vein, coordination across diverse university researchers, centers and counterparts in the private sector is critical if the field is to both avoid rampant duplication of efforts and effectively encourage commitment to new research pathways in a timely fashion. To this end, the community should embrace the incorporation of both new technologies and mechanisms of cooperation found in the natural sciences. To the latter point, inter-scholar discussion groups like those found in the security studies and comparative politics fields should be encouraged via the patronage of organizing associations and full support should be lent to an effort to build a common repository for storing published work and relevant data. To the former point, the field would do well to consider the use of a collaborative blockchain-based system for sharing computing resources and cataloguing research interactions in a public, transparent manner.

A Digital Studies Scholarship Cooperative. Of course, without some kind of organizing force, much of this lies in the realm of suggestion free from an ability to effectively implement at the level of the immense community of scholars and institutions that constitute the cyber-security research program. I argue that such an organizing force, however, should not simply take the form of an association that primarily organizes conferences and provides professional resources to scholars. Rather, because of the unique methodological and coordinative challenges facing the field, I argue that scholars would be best served by participating in a digital studies research cooperative wherein the sole purpose is to enhance the clout and research prospects of the community-at-large. Secondary to a professional association, such a cooperative would be centralized only around an oversight committee of rotating membership that (given relevant review) acted to vouch for scholars negotiating for proprietary data access, ensured protection of such data, allowed for robust implementation of replication standards without violation of non-disclosure agreements and maintained the means for research/resource collaboration suggested above. Regardless of researcher priorities, developing such a cooperative would bring a broad set of benefits for researchers to all, not least the maintenance of a platform for coordinating the storage of new knowledge and orchestrating necessary collaborations amongst scholars undertaking related—even if methodologically distant—investigations.

8. Conclusion

This article has broadly sought to describe why unique attributional and availability challenges in the diverse research program on cyber-security are problematic. In particular, I have sought herein to highlight the monist perspective—an objectivity-based interpretation of the nature of knowledge construction championed by Max Weber—on what constitutes good social science. For monists, the challenges inherent in trying to bridge the digital divide in research are not, fundamentally, impediments to the development of a research program as is often seen to be the case among those of a more dualistic perspective on the social science enterprise. While enhanced abilities to cross-validate technical and sociopolitical observations—as well as to obtain data from otherwise opaque stakeholders that often possess such information—is desirable in general, it does not mean that the research program is doomed to enduringly be on shaky ontological ground. Rather, what is most desirable for the research problem is an expansion of community-supporting features of organization that will allow for better exposure of different world views expressed in analytic frameworks employed in research. Fortunately, such an approach is highly compatible with the imperatives of the research program as dualists might articulate them. Focus on better cooperative organization within the field stands to improve broad commitment to research standards and encourage the development of much-needed provision of common resources for the scholarly community.

Acknowledgments

The author would like to thank both reviewers and the Academic Editor for their comments and suggestions on the work presented in this article.

Conflict of Interests

The author declares no conflict of interests.

References

Amoore, L. (2009). Algorithmic war: Everyday geographies of the war on terror. *Antipode*, *41*(1), 49–69.

Anderson, B., Kearnes, M., McFarlane, C., & Swanton, D. (2012). On assemblages and geography. *Dialogues in Human Geography*, *2*(2), 171–189.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–98.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International organization*, *59*(1), 39–75.

Bennett, A. (2013). The mother of all isms: Causal mechanisms and structured pluralism in International Relations theory. *European Journal of International Relations*, *19*(3), 459–481.

Bennett, J. (2010). *Vibrant matter a political ecology of things*. Durham, NC: Duke University Press.

Berry, D. M. (2015). *Critical theory and the digital*. New York, NY: Bloomsbury Publishing.

Beyer, J. L. (2014). *Expect us: Online communities and political mobilization*. Oxford: Oxford University Press.

Blaug, M. (1975). Kuhn versus Lakatos, or paradigms versus research programmes in the history of economics. *History of Political Economy*, *7*(4), 399–433.

Bryant, L., Srnicek, N., & Harman, G. (Eds.). (2011). *The speculative turn: Continental materialism and realism*. Melbourne: re. press.

Buchanan, B. (2017). *The Cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford: Oxford University Press.

Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *IEEE: Proceedings of the VDE Kongress* (Vol. 116, pp. 213–218). Berlin: IEEE.

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96–121.

Dreyfus, H. L. (2008). *On the Internet*. London: Routledge.

Francis, G. (2012). The psychology of replication and replication in psychology. *Perspectives on Psychological Science*, *7*(6), 585–594.

Fuller, S. (2004). *Kuhn vs. Popper: The struggle for the soul of science*. New York, NY: Columbia University Press.

Galloway, A. R., & Thacker, E. (2007). *The exploit: A theory of networks* (Vol. 21). Minneapolis, MN: University of Minnesota Press.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298–303.

Guitton, C., & Korzak, E. (2013). The sophistication criterion for attribution: Identifying the perpetrators of cyber-attacks. *The RUSI Journal*, *158*(4), 62–68.

Habermas, J. (1987). *The philosophical discourse of modernity*. Cambridge: Polity Press.

Hacking, I. (1999). *The social construction of what?* Cambridge, MA: Harvard University Press.

Hutchins, E. (1995). *Cognition in the wild*. Cambridge, MA: MIT Press.

Jackson, P. T. (2008). Foregrounding ontology: Dualism, monism, and IR theory. *Review of International Studies*, *34*(1), 129–153.

Jackson, P. T., & Nexon, D. H. (2013). International theory in a post-paradigmatic era: From substantive wagers to scientific ontologies. *European Journal of International Relations*, *19*(3), 543–565.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7–40.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326–343.

Knake, R. K. (2010). *Internet governance in an age of cyber insecurity* (No. 56). Washington, DC: Council on Foreign Relations.

Kostyuk, N., & Zhukov, Y. M. (2017). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*. doi: 10.1177/0022002717737138

Kuhn, T. S. (1970). Logic of discovery or psychology of research. In I. Lakatos & A. Musgrave (Eds.), *Criticism and the growth of knowledge* (pp. 91–195). Cambridge: Cambridge University Press.

Lakatos, I. (1976). Falsification and the methodology of scientific research programmes. In I. Lakatos & A. Musgrave (Eds.), *Criticism and the growth of knowledge* (pp. 1–24). Cambridge: Cambridge University Press.

Lake, D. A. (2011). Why "isms" are evil: Theory, epistemology, and academic sects as impediments to understanding and progress. *International Studies Quarterly*, *55*(2), 465–480.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.

Layne, C. (1994). Kant or cant: The myth of the democratic peace. *International security*, *19*(2), 5–49.

Lindbekk, T. (1992). The Weberian ideal-type: Development and continuities. *Acta Sociologica*, *35*(4), 285–297.

Mackay, R. (2007). Editorial introduction. *Collapse*, *2*(1), 3–13.

Maxwell, S. E., Lau, M. Y., & Howard, G. S. (2015). Is psychology suffering from a replication crisis? What does "failure to replicate" really mean? *American Psychologist*, *70*(6), 487–498.

Mezzour, G., Carley, K. M., & Carley, L. R. (2015). An empirical study of global malware encounters. In *Proceedings of the 2015 symposium and bootcamp on the science of security*. New York, NY: ACM.

Mindell, D. A. (2002). *Between human and machine: Feedback, control, and computing before cybernetics*. Baltimore, MD: JHU Press.

Mindell, D. A., Segal, J., & Gerovitch, S. (2003). From communications engineering to communications science: Cybernetics and information theory in the United States, France, and the Soviet Union. In M. Walker (Ed.), *Science and ideology: A comparative history* (pp. 66–96). London: Routledge.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs.

Nye, J. S. (2014). *The regime complex for managing global cyber activities*. Cambridge, MA: Harvard Belfer Center.

Phetteplace, E. (2010). Speculative realism. *College & Research Libraries News*, *71*(6), 305–313.

Popper, K. R. (1970). *Normal science and its dangers*. Cambridge: Cambridge University Press.

Radford, B. J. (2016). *Automated learning of event coding dictionaries for novel domains with an application to cyberspace*. (Doctoral dissertation). Duke University, Durham, NC.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1/2), 4–37.

Risse-Kappen, T. (1995). Democratic peace—Warlike democracies? A social constructivist interpretation of the liberal argument. *European Journal of International Relations*, *1*(4), 491–517.

Rosato, S. (2003). The flawed logic of democratic peace theory. *American Political Science Review*, *97*(4), 585–602.

Sat, D. M., Krylov, G. O., Evgenyevich, K., Kasatkin, A. B., & Kornev, I. A. (2016). Investigation of money laundering methods through cryptocurrency. *Journal of Theoretical and Applied Information Technology*, *83*(2), 244–254.

Sgouras, K. I., Birda, A. D., & Labridis, D. P. (2014). Cyber attack impact on critical smart grid infrastructures. In *Innovative smart grid technologies conference (ISGT), 2014 IEEE PES* (pp. 1–5). New York, NY: IEEE.

Shaviro, S. (2003). *Connected: Or what it means to live in the network society*. Minneapolis, MN: University of Minnesota Press.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. London: Penguin.

Sil, R., & Katzenstein, P. J. (2010). Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions. *Perspectives on Politics*, *8*(2), 411–431.

Sowell, J. H. (2012). *Empirical studies of bottom-up Internet governance*. Cambridge, MA: MIT.

Stevens, T. (2017). Cyberweapons: Power and the governance of the invisible. *International Politics*. doi:10.1057/s41311-017-0088-y

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York, NY: Oxford University Press.

Weber, M. (1904). Die "Objektivität" sozialwissenschaftlicher und sozialpolitischer Erkenntnis. [The "objectivity" of socio-scientific and socio-political knowledge]. *Archiv für Sozialwissenschaft und Sozialpolitik*, *19*(1), 22–87.

Weber, M. (2017). *Methodology of social sciences*. London: Routledge.

Wiener, N. (1961). *Cybernetics or control and communication in the animal and the machine* (Vol. 25). Cambridge, MA: MIT Press.

Wiener, N. (1988). *The human use of human beings: Cybernetics and society*. New York, NY: Perseus Books Group.

Yang, G. (2009). *The power of the Internet in China: Citizen activism online*. New York, NY: Columbia University Press.

About the Author

Christopher Whyte is an Assistant Professor in Homeland Security & Emergency Preparedness at the L. Douglas Wilder School of Government & Public Affairs at Virginia Commonwealth University. He teaches coursework on cyber security policy, conflict and law, and has broadly taught coursework on international security topics, political risk analysis and strategic planning. His research interests include a range of international security topics related to the use of information technology in war and peace, political communication and cybersecurity doctrine/policy.

Politics and Governance (ISSN: 2183-2463)

Politics and Governance is an innovative new offering to the world of online publishing in the Political Sciences. An internationally peer-reviewed open access journal, Politics and Governance publishes significant, cutting-edge and multidisciplinary research drawn from all areas of Political Science.

www.cogitatiopress.com/politicsandgovernance

COGITATIO