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).

© 2018 by the author; licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

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-
The article explores public-private partnerships (PPPs), this work complements other critical engagements with private critical infrastructure ownership with the state's re-Iterations. McCarthy's PPPs are reproductive of a liberal or-polarity, for example, they find that states are restrained in State actions and intentions. Contrary to received wis-

2. Shortcomings and Gaps

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 pri-vate critical infrastructure ownership with the state’s re-sponsibility to provide cybersecurity as a public good. Extant discussions of PPPs assume binary distinctions—public/private, state/market—that obscure power rela-tions. McCarthy’s PPPs are reproductive of a liberal or-der 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 infra-structure design and ownership, its warping effects on cy-bersecurity 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 bina-ries like local/global and employs assemblage thinking to sketch the multiplicity of actors and interests compet-ing 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 cy-bersecurity literature: a technical focus on cybersecurity as a means to fix ‘broken’ objects and a social-scientific perspective that diagnoses the perceived misuse of tech-nological 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 be-tween 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 investi-gate sociological sites of cybersecurity. Through partici-pant observation of cybersecurity conferences, Shires (2018) introduces the notion of ‘ritual’ space-time per-formativity of expertise. Systematized rituals of organiza-tion 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 establish-ing 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 tech-nology design obscure digital service-users’ needs and desires. This establishes that cybersecurity measures must develop community trust by design, rather than in-creasing citizen’s insecurity and thereby failing to achieve collective security gains. This is a significant corrective to conven-tional 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) re-port on a long-term project to gather data on interna-tional cyber conflict, through which to test hypotheses of state actions and intentions. Contrary to received wis-dom, 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 Valeri-ano 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 ‘eco-

logical 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


**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*. 