Global Cybersecurity: New Directions in Theory and Methods

Stevens, Tim

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance*, *6*(2), 1-4. https://doi.org/10.17645/pag.v6i2.1569

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*.