BOOK REVIEW

The Ethics of Cybersecurity, edited by Markus Christen, Bert Gordijn and Michele Lor (2020) 384pp., $US115 (hardback) Springer Open, Cham, Switzerland, ISBN: 978-030-29052-8

The greatest challenge in putting together any sort of resource on ethical cybersecurity policy is that it requires building a bridge between two disparate groups of analysts and readers. Social scientists and legal scholars, focused on such issues as regulation and accountability, often have little background in the technical aspects of cybersecurity. But before analysing what is desirable, lawful or ethical in the field of, for example, privacy-tracking apps, one must first understand how they work, what constraints exist in regard to such issues as technological modifications, as well as specific challenges related to data storage, and vulnerabilities, such as hacking, theft and espionage. At the same time, those practitioners whose primary interest is in one or more specific applications of technology in a particular setting may struggle to understand the relevance of such seemingly esoteric concepts as Kantian ethics or ontology when describing what is ethically acceptable or desirable.

A second obstacle, however, is that traditionally the term 'cybersecurity ethics' itself (and for that matter, 'cybersecurity') has not actually meant the same thing to the two disparate audiences – technical practitioners and scholars in the social sciences. As Kosseff (2018) has argued, not all analysts or practitioners agree about exactly who or what is being secured in carrying out cybersecurity activities. Rather, as he notes, cybersecurity is often seen as overlapping with data security, and different states may understand the term differently. For a social scientist, cybersecurity is most often understood as a subset of national security concerns and therefore ethical, moral and legal questions are most often read within an existing set of understandings about national security and national security policymaking. American analysts in particular (many of whom come from a military background) tend to present cybersecurity from both a particularly American and a particularly nationalist framework. The overriding assumption is that the referent object of security (the object being protected) is the state. A secondary assumption is that the security interests of the state and of the private sector are often at odds (see Libicki, 2016). Ensuring cybersecurity, then, is particularly about protecting American national security at the state level, with safeguarding individual rights, such as a privacy, a distant second in terms of ethical, legal, and moral concerns. At the same time, however, for technology practitioners 'cybersecurity' often refers specifically to the protection of data resources, regardless of whether such resources are owned or managed by the government, the private sector or some other entity. (A compliance officer at a firm sees data not as, say, American or French, nor as a national security asset, but simply as an asset to be protected.)

At present, only a few practitioners and institutions have engaged seriously with both cybersecurity as a set of technological understandings and processes, and cybersecurity as national security. Among those who have done so, we can consider in particular Luciano Floridi and Mariarosario Taddeo, two academics affiliated with Oxford's Internet Institute, who have written on such topics as the moral responsibilities of internet providers to both their customers and the larger national security community, as well as on the new challenges produced by cybersecurity technologies enabled by artificial intelligence and their moral import (Taddeo and Floridi, 2015; Taddeo *et al*., 2019). Their work accomplishes the goal of speaking to diverse audiences – from policymakers to technology entrepreneurs – and specifying a set of ethical understandings which are relevant and accessible to both audiences.

The demands of two diverse audiences have been an obstacle to the creation of edited volumes in both cybersecurity in general and cybersecurity ethics in particular. Many existing volumes

focus on military, legal, and regulatory issues, or on one or two highly specific technology issues (such as the ethical application of specific technologies in the military realm) (see, e.g., Perkovich. and Levite, 2017; Vallor, 2017). The challenge is to create a volume that is relevant to both technology practitioners and to social scientists. In this regard, the work of Markus Christen, Bert Gordijn and Michele Lor is a monumental achievement. As the they note in their introduction, the volume grew out of the research activities of the CANVAS Consortium (Constructing an Alliance for Value-Driven Cybersecurity), funded by the European Commission. The CANVAS project, coordinated by the Center for Ethics at the University of Zurich, includes eleven partners (both academic and non-academic institutions) located in seven European countries.[1]

This volume begins with a basic overview of technology concepts which analysts then build upon in explaining the universe of regulatory and legal challenges in the field of cybersecurity ethics. Christen *et al.* introduce the notion of 'values conflict' – multiple competing value perspectives which can be applied to an existing situation. Attempts to pursue one value (such as openness) may result in other values (such as security) being neglected. Values conflict serves as an organizing device for the volume as a whole, allowing the reader to think through how such conflicts appear in a variety of situations and the various ways in which these conflicts have been navigated, negotiated and resolved. As the editors note in their Introduction:

> a governmental computer emergency response team (CERT) may fight a ransomware attack by turning off the payment servers and destroying the business model of the attackers to prevent future attacks – but this means that people whose data already has been encrypted would never retrieve it. A medical implants producer may want to protect the data transfer between implant and receiver server by means of suitable cryptography – but this significantly increases the energy consumption of the implant and frequently requires more surgeries for battery exchange.

The challenge for both technical and social science practitioners is to seek solutions which balance these multiple competing priorities, based on the assumption that there are solution sets which can be found, and that one side does not automatically have the right to profit at the expense of the other. It is important to note that this assumption – that the private and public sectors can work together cooperatively and in complementarity and that they are strongly committed to doing so – may be the default setting for European practitioners, but may not be true universally. This volume reproduces the European assumption that there is often a natural confluence of interests between those in the private and public sectors. This may be so in Europe, but not necessarily elsewhere.

Adam Segal argues in his work that it may not be possible to bridge the gap between the interests and values of entrepreneurs in California's Silicon Valley and policymakers in Washington. He faults Silicon Valley in particular for not regarding the safeguarding of American national security as paramount, much more important than seeking accord and profitable arrangements with China. At the same time, Gjesvik suggests that China's strategic culture has always privileged the policy preferences and interests of the state over and above those of other actors. Therefore, he suggests, the balance of power in cybersecurity policy will likely favour the state over other actors (see Segal, 2017; Gjesvik, 2018). This is not to undermine the arguments of those whose work appears in the volume, but rather to note that the lessons drawn from the volume may not be generalizable to cybersecurity ethics within the international system as a whole. Though the same values conflicts may be present, they may not be solved as easily as they have been in Europe.

If this is a weakness of the volume, it contains far more strengths. Indeed, the volume has two strengths which mirror the strength of the CANVAS program itself: its conscious and concerted effort to reach across academic fields to bring technology specialists and scholars into dialogue with those in the social sciences. The volume is of 18 essays divided into three parts – Foundations,

---

[1] More information about the consortium and its activities can be found at https://canvas-project.eu/about/consortium.html (accessed May 2020).

Problems, and Recommendations. The 25 authors have both applied and academic experience and come from institutions in Europe, Russia and the United States.

Particularly notable contributions are the essay by Dominik Hellman and Henning Pridohl (both at the University of Bamberg) on basic concepts and models of cybersecurity, and that by Karsten Weber and Nadine Kleine on cybersecurity in health care. The latter is a valuable contribution in the emerging field of health and national security, though it already feels a bit dated because of the lack of engagement with specific privacy dilemmas related to pandemic monitoring and data anonymization. Also of note is the essay by Paul Meyer, a 35-year veteran of Canada's foreign service now at Simon Fraser University. In an essay on responsible state behaviour in cyberspace, he queries whether Hobbes' notion of the state of nature can truly be said to apply in cyberspace. In short, this volume provides a valuable overview of the issues and dilemmas in the field of cybersecurity ethics, particularly in the European context. The volume will be of interest to graduate students and academic researchers, and some of the essays will also be useful to undergraduates.

References

Gjesvik, L. (2018) 'China's notion of cybersecurity: the importance of strategic cultures for cyber deterrence', *Proceedings of the European Conference on Cyberwarfare and Security*, June 2018, pp.174–80, available at http://www.academic-bookshop.com/ourshop/prod_6457309-ECCWS-2018-PDF-Proceedings-of-the-17th-European-Conference-on-Cyber-Warfare-and-Security.html (accessed May 2020).

Knight, W., 2020 'The value and ethics of using phone data to monitor COVID-19', *Wired*, 18 March, available at https://www.wired.com/story/value-ethics-using-phone-data-monitor-covid-19/ (accessed May 2020).

Kosseff, J. (2018) 'Defining cybersecurity law', *Iowa Law Review*, 103, 985, pp.985–1032.

Libicki, M. (2016) *Cyberspace in Peace and War*, Naval Institute Press, Annapolis MD.

Perkovich, G. and Levite, A. (eds) (2017) *Understanding Cyber Conflict: Fourteen Analogies*, Georgetown University Press, Washington DC.

Segal, A. (2017) 'Bridging the cyberspace gap: Washington and Silicon Valley', *Prism*, 7, 2, pp.66–77.

Taddeo, M. and Floridi, L. (2015) 'The debate on the moral responsibilities of online service providers', *Science and Engineering Ethics*, 22, 6, pp.1575–1603.

Taddeo, M., McCutcheon, T. and Floridi, L. (2019) 'Trusting artificial intelligence in cybersecurity is a double-edged sword', *Nature Machine Intelligence*, 1, pp.557–66.

Vallor, S. (2017) 'Robots with guns' in Pitt, J. and Shew, A. (eds) *Spaces for the Future: A Companion to the Philosophy of Technology*, Routledge, New York, pp.73–81.

Mary Manjikian
Robertson School of Government
Regent University
mmanjikian@regent.edu