Routledge
Taylor & Francis Group

BOOK REVIEW

The security of self: a human-centric approach to cybersecurity, edited by Emily B. Laidlaw and Florian Martin-Bariteau, Ottawa, Ottawa UP, 2025, 222 pp., £35.95 (paperback), ISBN 9780776645605

The Security of Self seeks to 'breathe life' into a shift underway in law, policy, and scholarship on cybersecurity towards a human-centric approach to the topic (4). The Introduction to the volume begins with the observation that '[t]ypically, cybersecurity has been conceived narrowly' as protecting the privacy and integrity of data systems 'usually in the context of national security or to protect corporate assets' (1). The editors argue that 'many of the individual and collective ways that humans are put at risk have been unexamined, or underresearched' (1). Humans have tended to feature in the dominant paradigm only as 'a threat to be stopped, or as potential victims to be saved from some impending doom' (2). The book 'offers a new approach to human-centric cyber-security: the *security of self*' (2). This 'invites a paradigm shift' in which 'cybersecurity's core purpose is to protect people – and society – from harm', and collective rights to a secure cyber environment are central (2).

The editors point to emerging legal frameworks in Europe and Commonwealth countries as evidence of this shift. Various initiatives mark a broadening of cybersecurity concerns from compliance with technical standards and 'incident response mechanisms' to consumer data protection and unfair practices by large digital platforms (3). Laidlaw and Martin-Bariteau also cite a body of scholarship in recent years advocating a shift to a human-centric approach to cybersecurity in these very terms, including work by Deibert (2018), Klein and Hossain (2020), and Grobler, Gaire, and Nepal (2021). The shift, then, is not new; the aim here is to foreground and promote it.

The introductory essay conveys a sense of the difference that a shift to a human-centric approach makes to studying cybersecurity by canvassing a range of vulnerabilities and rights-infringing cases through this lens. These include sextortion, addictive social media algorithms, surveillance through smart home devices, and manipulative practices carried out by AI providers. 'Changing the lens', they note, 'enables different questions to be asked' (5). What guardrails should be in place to govern and protect not only the data collected or shared here, but the underlying human interests engaged in the process? The same logic applies to disinformation, whether it involves propaganda, election interference, or reputational harm. The traditional approach to cybersecurity frames these concerns as threats to state security or democracy, overlooking the more subtle ways in which they harm individual dignity and security.

Before turning to the contributions in the volume, it is worth asking whether the book's framing of a human-centric turn in law and scholarship is apt – and what it leaves out. While it is true that a body of work has emerged in recent years calling for a more human-centric approach, one might ask whether the idea is really new or whether it amounts to a 'paradigm shift' in the field (2). A glance at other recent scholarly collections – for example, *The Oxford Handbook of Cyber Security* (2021) – or Tim Stevens' recent monograph, *What Is Cybersecurity For?* (2023), or a more general work on security, such as *Security Studies: An Applied Introduction* (2024) will show that each of them contains a chapter on human or personal security alongside chapters on the national, international, or market-centred impact of security-related issues. This suggests that human or individual security is best understood

as one of a subset of ongoing concerns within cybersecurity and security studies writ large, and not the product of a new turn.

The framing in this book also leaves out an issue that can only be touched on here, given the limits of space. There is no substantive reflection – in the Introduction or in the contributions to the book – on the concept of security itself as a normative value, a logic, or a governmentality. The drive toward bolstering human security is presented here as an unqualified human good, rather than being questioned as what Mark Neocleous, in his *Critique of Security* (2008), has termed a 'political technology.' The phrase 'security of self', taken up throughout this collection, is mostly understood as synonymous with harm avoidance and rights protection and not as a potentially problematic concept in relation to self-formation or identity. This is not to fault the framing of the book in terms of security but to point to a direction it chooses not to go.

Contributions to the book are divided into two parts: chapters exploring specific risks to individual security and those examining gaps in law or policy needed to address 'harmful behaviours and to support their victims' (8). Canadian law scholars make up the largest group of contributors, but a number are drawn from other disciplines, including politics, media and information studies, computer science, and criminology.

Essays in the first half of the book are concerned with the human impact of security vulnerabilities. A chapter on the Amazon Ring argues that its susceptibility to hacking or being co-opted in ways that can expose users to violence – including intimate partner violence – has been underplayed in the product's development and reception. Other chapters explore the psychological and behavioural impact of information manipulation campaigns and other forms of abuse on social media – framed here as dimensions of cybersecurity.

The second half of the book focuses on gaps in law and policy, seeking to shed further light on how the pivot to a rights-centric approach to cybersecurity could make a practical difference for persons and groups. To lend a sense, one chapter explores various technical advances in machine learning that could better protect personal privacy, such as dataset watermarking and data poisoning, and calls for law mandating their use in AI systems. The two closing chapters offer illuminating case studies of how victims of online fraud (in one case, romance fraud) use online discussion forums to raise awareness and share information to help protect others, calling for better protection in law for the victims of these offences.

The contributions are generally effective in showing how cybersecurity can and should be conceived in broader terms, and what concerns come into sharper view when human impact is in the foreground. Conceptual reframings do matter. *The Security of Self* may not point to something as momentous as a paradigm shift, but it does highlight a fertile development in the field – and a meaningful one at that.

References

Cornish, P., ed. 2021. *The Oxford Handbook of Cyber Security*. Oxford: Oxford University Press.

Deibert, R. J. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32 (4): 411–424.

Grobler, M., R. Gaire, and S. Nepal. 2021. "User, Usage and Usability: Redefining Human Centric Cyber Security." *Frontiers in Big Data* 4 (1): 583723. https://doi.org/10.3389/fdata.2021.583723.

Klein, J., and K. Hossain. 2020. "Conceptualising Human-Centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change." *Arctic Review on Law and Politics* 11: 1–18. https://doi.org/10.23865/arctic.v11.1936.

Neocleous, M. 2008. *Critique of Security*. Edinburgh: Edinburgh University Press.

Rossi, N., and M. Riemann, eds. 2024. *Security Studies: An Applied Introduction*. London: Sage Publications Ltd.

Stevens, T. 2023. *What Is Cybersecurity For?* Bristol: Bristol University Press.

Robert Diab
Thompson Rivers University, Canada
rdiab@tru.ca

https://doi.org/10.1080/23738871.2026.2669136