wide audience. Given the dearth of publications in History of Science (and STS) in Portugal, this book provides a much-needed contribution to the field. Also, the book brings to the light the “invisible” scientific endeavors carried out in a southern European country during the 19th and early 20th century, putting into question the dominant narrative that Portugal had barely any scientific activity until the accession to the European Community in the 1980s.

References

Agar, J., and C. Smith (eds.) (1998) *Making Space for Science. Territorial Themes in the Shaping of Knowledge*, London, Palgrave Macmillan.

Galison, P. and E. Thompson (eds.) (1999) *The Architecture of Science*, Cambridge, MIT Press.

Macedo, M. (2012) *Projectar e Construir a Nação: Engenheiros, ciência e território em Portugal no século XIX*, Lisbon, Imprensa de Ciências Sociais.

Nieto-Galan, A. and O. Hochadel (eds.) (2019), *Urban Histories of Science*, London, Routledge.

Saraiva, T. (2005) *Ciencia y Ciudad: Madrid y Lisboa (1851–1900*), Madrid, Ayuntamiento de Madrid.

* * *

Howard Shrobe, David L. Shrier and Alex Pentland (eds.)
New Solutions for Cybersecurity, Cambridge MA, MIT Press, 2018, pp.491

Stefano De Paoli *Abertay University*

Cybersecurity and cybercrime are fast becoming two of the most important issues of our digital society and, as such, they deserve attention from Science and Technology Studies (STS). We can define cybersecurity as the theory and practice of preventing or detecting attacks on digital systems. We can define cybercrime as the unauthorised access to digital systems for a variety of purposes, which can include disruption, manipulation, deception and crime more generally, among others. Much of what exists in social sciences research especially around cybercrime comes from criminological studies. However, criminologists are debating on the problem of using traditional criminological approaches (that focus on the study of human criminals and social structures) to the study of phenomena deeply ingrained with digital technologies. Thus, criminologists speak about the problem of the “Novelty of Cybercrime” (e.g. Yar 2005). Few authors in criminology have started to look at STS approaches as potential alternatives to traditional approaches. At present, we indeed have limited STS contributions studying cybersecurity and cybercrime. Few of the known exceptions are the papers by Van Der Wagen and Pieters (2015; 2018) on cyborg crimes and hybrid victims. I would also like to highlight a recently funded research project in the UK called "Scaling Trust: An Anthropology of Cyber Security", led by Matthew Spencer at the University of Warwick.

We live in a world increasingly shaped by digital technologies, whether computers, algorithms, infrastructures or the Internet of Things, and all come with the purpose of serving a multiplicity of needs such as the running of business, the offering of public services or making our cities smart, among others. However, it has long been known that computers (and by extension all digital technologies) can be attacked often with malicious intents. Designing secure systems has been a main concern since the creation of shared computing resources in the early '60s of the last century. Security still is a major concern today as it is clear that the increased complexity of our digital technologies, their pervasiveness and our overreliance on them can only bring increases in risks and in the sophistication of the attacks toward them. All of this could cause major disruptions to our society's life, as the quite recent case of the Wannacry attack has demonstrated (ENISA 2017). Cybercrime is major problem for many actors, whether companies, public authorities or even just citizens. Consequently cybersecurity becomes a necessity, which is however often overlooked for a variety of reasons that can include costs, lack of skills or simply disinterest.

The book *New Solutions for Cybersecurity* edited by Shrobe, Shier and Pentland (2018) thus contributes to this important field. The book contains chapters written by leading academics and researchers from the MIT. Now, to be clear, this book does "what it says on the thin", to use a catchphrase. It is a book that offers solutions, i.e. practical solutions to cybersecurity problems. It is not a book that advances theoretical thinking or empirical research specifically, although all the chapters are based on high quality research. The book does not have research or academia as its main audiences. This is a book aimed at practitioners, people working for companies, public authorities and organisations, which are looking for recent and advanced cybersecurity solutions, hence the title "new solutions". Solutions, those offered in the book, which could be often readily implemented to solve technical or organisational problems around cybersecurity. Each of the chapter is very lightweight in terms of discussing debates, theories or providing reviews. Each focuses on a solution to a specific problem, whether this is a more secure computing architecture, the need for tapping into bug-hunters expertise or advances in social network analysis that can be used for prevention or detection of crimes. The book is organised in three main blocks geared respectively toward: a) "Management, Organizations and Strategy", b) "Architecture" and c)

"Systems". The first block proposes mostly solutions that can be implemented at organisational level for incresing or improving cybersecurity. The second block reports on solutions for the architecture of secure computer systems and for overcoming limits in the traditional design of computer architectures. The third block contains chapters wich broadly encompass a variety of systems, such as Internet of Things security or the DarkWeb. The three proposed blocks seem also an emergent way of organising and clustering a variety of solutions, as proposed in the book's chapters.

Now I will concentrate on some of the chapters, in order to highlight a few of the main contributions of the three main blocks of the book. I will also concentrate on the chapters that I believe are representative of the content of the book and that in my perspective may be of interest from an STS angle.

The chapter 1 of the book entitled *Institutions for Cybersecurity: International Responses and Data Sharing Initiatives* is part of the "Management, Organization and Strategy" block of the book. It provides an overview of the main institutional actors involved in cybersecurity, also detailing different institutionalisation processes that took place in both the USA and Europe. The main contribution of this chapter, I would suggest, is a table providing a detailed list of organisations and their roles in cybersecurity. This table thus offers a useful reference map to navigate the quite complex variety of institutional actors dealing with cybersecurity, including Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs) and other national and international players.

Chapter 4 entitled *Fixing a Hole: The Labor Market for Bugs*, also part of the "Management, Organization and Strategy" block, offers an interesting analysis of the labour market associated with bug-bounties programs, that is, companies offering rewards to programmers (defined as researchers or sellers) that can find critical bugs in their software. This chapter does well in describing the stratification of the bug bounty labour markets and provides interesting recommendations for companies wishing to use this specific form of labour for reducing the vulnerabilities of their software. The main solution is the suggestion of developing programs geared toward attracting low numbers of sellers but capable of delivering high volume of results (i.e. identification of bugs), rather than large numbers of sellers, which have shown to deliver much less, due to a variety of reasons including lack of knowledge of the codebase.

Although strictly a technical chapter devoted to an architecture called CHERI (Capability Hardware Enhanced RISC Instructions) for increasing systems trustworthiness, and thus included in the "Architecture" block, Chapter 6 *Fundamentals Trustworthiness Principles in CHERI* is quite enjoyable in its discussion and revision of the Saltzer/Schroeder principles of information security (Saltzer and Schroeder 1975). I would recommend this chapter to get a sense of how security policies and mechanisms functions in most advanced secure and trusted architectures. Consequently, the chapter provides an interesting reference point for knowing how current advanced security architectures work toward overcoming the security limits of previous computer architecture designs.

Chapter 10 *Who's Afraid of the Dark Web?*, included in the block on "Systems", provides an interesting discussion about the concepts of privacy, anonymity and the Dark Web. This is, perhaps, the chapter that least of all proposes a specific solution to a problem. It offers, instead, reflections on the role of technologies enhancing privacy and anonymity (such as the onion routing and encryption more general). The chapter also reflects on the difficulties of maintaining the balance between the positive use of these technologies for e.g. protecting privacy and the prevention of their use for fostering criminal enterprising.

Some warnings about the content of a few chapters. Although, as I said earlier, this is not a book particularly strong on theory, I need to flag up that in some chapters there is pervasiveness of positivism and deterministic thinking. I refrain here in this review to discuss a critique of positivism in the field of cybersecurity and I would suggest that probably the measure of success to apply to each of the proposed solution is the extent to which they really offer something to address specific cybersecurity problems. Nonetheless, the positivistic perspective is for example clear in the chapters describing the concept of "social physics" (Chapter 11 chiefly *Social Physics and Cybercrime*, part of the "Systems" block) that, as the term goes, clearly builds a parallel between social action and mechanics, with the intent of identifying patterns in human data, based on "socio-behavioural laws". This perspective is a critique to machine learning, i.e. technology driven and highly expensive approaches to make prediction based on big data. However, social physics clearly resembles the idea that there are laws governing social behaviour and that now, with the amount of data (or better human signals) been generated, by knowing the laws we can anticipate the evolution of behaviour (in this case associated with security). Likewise, the chapter *Cybersafety: A Systems Theory Approach to Managing Cybersecurity Risks* (Chapter 2, included in the "Management, Organization and Strategy block") clearly advocates a strict top-down approach to cybersecurity based on the idea of cybersafety. In this approach the actions to be enacted toward better security (in particular the identification of why control systems were ineffective in incidents) are deduced from set of high-level principles/factors, in particular encompassing missing constraints, inadequate safety, inadequate safety control commands, commands incorrectly executed at lower level and inadequate communications. The authors promote this approach as an alternative to technology driven approaches to control and safety.

To conclude this is not a book I would recommend to a colleague or a student looking for a first introduction to the topics of cybersecurity and cybercrime. I would also not recommend this book specifically to the social scientist that is looking for a publication describing the current theoretical thinking around these topics, from any specific area or research tradition. The main audience of this book, as I stated earlier, are practitioners in medium to large organisations, looking for new solutions and the publication does well in presenting them with the state-of-the-art of what is possible with novel advances. As this stands, it is possible to approach the book only with prior knowledge of the areas of cybersecurity and cybercrime and, for most chapters, with sufficient knowledge of computing and current evolution of cybersecurity.

References

The European Union Agency for Network and Information Security (ENISA) (2017) *WannaCry Ransomware Outburst*, "Cyber security info notes", May 15th.

Saltzer, J. H., and Schroeder, M. D. (1975) *The protection of information in computer systems*, "Proceedings of the IEEE", 63 (9), pp. 1278-1308.

van der Wagen, W. and Pieters, W. (2015) *From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks*, "British journal of criminology", 55 (3), pp. 578-595.

van der Wagen, W. and Pieters, W. (2018) *The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory*, "European Journal of Criminology", 17 (4), 480-497.

Yar, M. (2005) *The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory*, "European Journal of Criminology", 2 (4), pp. 407-427.

* * *

Cornelia Sollfrank (ed.)
The Beautiful Warriors. Technofeminist Praxis in the Twenty-first Century, Colchester, New York and Port Watson, Minor Compositions, 2020, pp. 151

Monika Urban *Universität Bremen*

The #MeToo movement has recently broken silence on feminist matters worldwide. Using mostly social media, the movement has mobilized hundreds of thousands of people on topics such as sexual harassment and sexual assault. With reference to their digital practices, we could well associate the movement with cyberfeminism. This genre of contemporary feminism emerged in the early 1990s. Focusing on new digital technolo-