The Rules of Security: Staying Safe in a Risky World

Paul Martin

In 2024, *The Rules of Security: Staying Safe in a Risky World* has renewed importance. This review is especially interested in its contribution to bridging physical security and cyber security in a 'responsibilised' society. And given that the work was written three years before the start of Russia's full-scale invasion of Ukraine, now is a good opportunity to compare the work's views of the cyber domain against what has occurred throughout the cyberwar that has accompanied the ongoing conflict.

Writing in a 1996 issue of the *British Journal of Criminology* (p. 452), David Garland referred to 'responsibilisation' as the practice of neoliberal governments delegating the responsibility for protective security to their citizens. Martin's work recognises this approach but carefully strives to strike a balance between the UK government's responsibility and citizens' responsibility for personal security (p. 6). The book is structured around 10 security rules, each forming a separate chapter. In total, these rules support the book's principal focus: on framing security as a real-world human need.

The approach is predominantly strategic, with relatively less attention on the day-to-day practical steps that individuals can take. It might therefore be more suited to readers with an interest in these strategic questions. In line with Rule 3, the author forces the reader to switch perspectives and think both from the perspective of defence as well as attack. Yet despite the seriousness of the topic, the language is generally straightforward, even casual, with humour being used to keep the reader's attention.

One particularly important contribution is the work's ability to guide the reader through the basics of physical security, and especially how risks from the physical world transfer into the cyber world. It is only after giving the reader this necessary foundation that the author progresses into the cyber sphere.

In Rule 8, Martin correctly points out that the cyber sphere offers anonymity to attackers since victims do not know that they have been attacked and/or are reluctant to report incidents (p. 146) – a point further underscored by Juraj Sikra, Karen V Renaud and Daniel R Thomas in a 2023 article in the *Commonwealth Cybercrime Journal*. Yet, Martin avoids victim-blaming. As stated in Rule 6, people are not the weakest link in security but the glue that holds everything together (p. 96). This is because they form the most complex and least understood link in security, which opens a plethora of avenues for attack, but also new and creative ways of defence.

The author makes a persuasive critique of the cyber security responsibilisation strategy, noting that awareness-raising campaigns are ineffective and based on faulty psychology (p. 153). In a 2018 article in *Computers & Security*, Karen Renaud et al. explored these flaws, arguing that cyber security responsibilisation focused on educating people about cyber threats rather than explicitly supporting them in recovering post-attack. This approach, they argue, is unsatisfactory: not only does it fail to develop expertise, but it is also injudicious, because one attack can infect an entire network. Therefore, an interventionist approach by the UK government would be more effective.

Turning to the war in Ukraine, the ongoing conflict allows for a reconsideration of Martin's views of cyber warfare. Specifically, Martin remarks that several states, including the US and the UK, would regard a serious cyber attack worthy of a conventional retaliation (p. 161). Martin does not pinpoint what the threshold for 'triggering an old-fashioned shooting war' would be, but he highlights that foreign nations are in a phase where they are experimenting with how far they are allowed to go.

However, five years after the book's publication, conventional responses to cyber attacks have rarely been seen. In those five years, cyber attacks have impacted the US, the UK and Russia with the US attacked the most (as Anh Vu et al. state in their 2024 paper presented at the ACM Web Conference 2024, pp. 4–6). Yet, following these attacks, the adversaries were wise to avoid conventional retaliation.

The conflict in Ukraine has showed the practical difficulties of retaliating, even when states are inclined to do so. A large portion of

website defacers and distributed denial of services (DDoS) attackers engaging in cyber warfare in the war in Ukraine were not associated with either NATO allies or Russia. Rather, as Vu et al.'s 2024 paper notes, these actors undertook acts of solidarity and bravado, and were located all over the world. Consequently, it became difficult for the adversaries to justify conventional retaliation given the mismatch between the dispersed, atomised cyber battlefield and the real-world frontlines.

Martin provides his audience with a strategic perspective on how the 10 rules he outlines can strengthen security. The work reminds readers that the UK government's approach to cyber security responsibilisation is ineffective and that a more interventionist approach is warranted. At the same time, events in Russia's war against Ukraine have showed how difficult it is for states to respond to cyber attacks using conventional means. This shows – even in the short five years s ince t his work was written – just how complex the cyber landscape has become.