**Cyber war will not take place. By Thomas Rid.** London: Hurst. 2013. 218pp. Index. Pb.: £14.99. ISBN 978 1 84904 280 2. Available as e-book.

In this book, Thomas Rid, a Reader in War Studies at King's College London, puts forth the titled thesis that *Cyber war will not take place*. While this sentiment on cyber war is structured in the future tense, Rid extends the premise to the past and present. This book emerges in the midst of an ongoing, and often contentious, international dialogue around cyber threats and their corresponding security challenges. Rid enters the fray of the debate, bridging the chasm between the current rhetoric and the operational realities of the cyber threat. He does so by presenting a scholarly analysis of the meaning of cyber war, the operational realities of cyber attacks and future considerations in this space.

Rid anchors his argument that cyber war has not, is not currently and will not take place upon Clausewitz's definition of war and the presupposition that violence is a prerequisite thereof. Given that 'not a single human being has ever been killed or hurt as a result of a code-triggered cyber attack' (p. 13), the use of 'cyber war' serves more as a loose metaphor for a range of motives than an apt description of reality. Rid acknowledges that cyber weapons do exist and that real lives will not be cut short because of future cyber attacks. However, when such attacks do occur, they will be indirect as they are dependent upon the kinetic impact or



*International Affairs* **90**: 1, 2014

mechanical failure of a device that is reliant upon or interacting with the weaponized code. As such, cyber violence will always be 'less physical, less emotional, less symbolic, and, as a result, less instrumental than more conventional use of political violence' (p. 166).

Rid categorizes cyber attacks in three distinct modes of operation and dedicates a chapter to each: sabotage, espionage and subversion. The chapters on sabotage and espionage artfully articulate the contemporary and familiar threats in their respective domains. He offers a thorough analysis of the destructive powers of the Shamoon virus and sophistication of Stuxnet that are emblematic of the tactical efficacy of cyber weapons for disruptive or destructive means. When examining espionage, Operation Titan Rain and Shady RAT are used to illustrate the depth and breadth of penetration that can be achieved through cyber means. While academically interesting, the chapter dedicated to subversion struggled for relevance as a cyber threat when juxtaposed against the other categories: sabotage and espionage.

One of the more intriguing and thought-provoking contributions by Rid is his statement that 'the rise of cyber offence represents an attack on violence itself' (p. 166). The advent of the information age has provided greater opportunity for digital than kinetic engagement to achieve the same, or at least similar, tactical and operational advantage. When a cyber attack is weighed against a traditional military response, the former will often be ethically preferable as it is likely to limit, or altogether exclude, collateral damage and loss of life. While this may be true with present capabilities, it will be interesting to see if this remains so and meets the test of time as technology advances.

Rid's concluding thoughts challenge what he views as the unconstrained use of cyber war as a metaphor. He argues that such use has devalued the dialogue and militarized the debate around cyberspace. In so doing, this tone of discourse 'overhypes offence and blunts the discourse on defence' (p. 174). While there may be a kernel of truth in this line of reasoning, there are other confounding factors as to why offence is overemphasized. Many states have comprehensive national strategies that address both defensive and offensive capabilities in cyberspace. Defensive capabilities are bolstered through the establishment of security standards, oversight and investment in research while offensive capabilities are inculcated into military operations and structure. As such, the former is fragmented through a myriad of organizations, industry and academia while the latter is centralized into a unified military command.

This book provides a thorough and timely analysis of cyber conflict and makes a reasonable case to temper the dialogue around cyber war. While some of the finer points may be debatable, the supporting arguments are worthy of the time and consideration of policymakers and information security professionals alike.

*Patrick J. Kelly, George Washington University, USA*