The Darkening Web: The War for Cyberspace,

by Alexander Klimburg, New York: Penguin Random House, 2017, Kindle Edition, pp. 432, $15.99

Cherian Samuel*

The introduction to Alexander Klimburg's book, *The Darkening Web: The War for Cyberspace*, begins by referencing the Indian parable of the Blind Men of Hindoostan and the elephant to bring out the difficulty of 'grasping the entirety of cyberspace'. The focus of his book is on international security, and more specifically, the security interests of states in cyberspace. That said, a large part of the book focuses on three countries—the United States, Russia and China—and their approaches and actions in cyberspace. Europe is mentioned largely in the context of privacy and data laws.

Klimsburg is a Research Fellow at the Hague Centre for Strategic Studies, but what is unusual about the book is its distinctly non-academic nature with nary a footnote adorning its pages. The book may be seen as a primer from a distinctly Western perspective on the current state of play in cyberspace. It is exhaustive in painting a broad canvas and highlighting the various elements that have led to what he sees as the present situation of instability and uncertainty in cyberspace, as reflected in the title.

The war for cyberspace is a many layered and multi-dimensional one with a variety of actors and interests. Elaborating on and deconstructing these relationships makes most bodies of work on cyberspace quite unwieldy; and Klimburg's tome, stretching to 432 pages, is no exception.

* The reviewer is Research Fellow in the Strategic Technologies Centre at IDSA.

ISSN 0976-1004 print
© 2017 Institute for Defence Studies and Analyses
Journal of Defence Studies, Vol. 11, No. 4, October–December 2017, pp. 109–113

It begins with a description of the nuts and bolts of cyberspace interlaced with history to explain the development of the basic principles of the domain, many of which have stood the test of time, and enabled it to scale up from a few networks between universities to the well over 40,000-odd networks with nearly 4 billion people online. Though it regurgitates earlier descriptions and analyses of cyberspace, there is enough new information along with quotable quotes to keep the reader interested. To wit: 'The Internet is the first thing that humanity has built that humanity does not understand', according to Eric Schmidt, Executive Chairman of Alphabet, Google's parent company (p. 25).

Klimburg draws on the 2008 definition of cyberspace by the US government to assert that 'Cyberspace therefore includes not only technology but also human behaviours and arguably Internet technology-enabled social interactions' (p. 27). He also lays out his core theme which pulsates through the book, that 'there are marked differences between the "hacking" and technical-attack-oriented cyber-war narratives of liberal democracies and the psychological-attack information-warfare narrative on which countries like Russia and China are fixated' (p. 15). The sum total of Klimburg's argument is that liberal democracies can do no bad; that even when they do so, it is done not for malicious reasons but almost inadvertently. He reaches into the social sciences and pulls out the theory of path dependency to explain the shenanigans of the national security establishment in the United States (US), as exposed through various hacks and leakages. The quest for dominance in all warfighting domains has been carried over into cyberspace without adequate analysis of its impact on American moral standing as well as its foreign relations. This offence-first policy, carried over from US policy in other domains, was given further impetus in the global war on terror. Klimsburg believes it has gone so far as to put the US on the path to psychological information warfare even while it decries Russian policies that seek to legitimise information warfare.

The other main actors that animate US cyberpolicy, civil society (including the InfoSec[information security] community) and the private sector, and the tensions among these three actors make for interesting and troubling reading. This is more so because their actions and responses have a disproportionately large impact on all users of cyberspace, not just those in the US. Whilst the various stakeholders have an array of tools at their disposal, from legislation to the courts, to forcing norms of behaviour, the disregard for the rights of non-US persons and the

collaboration between the American private sector and intelligence agencies should disabuse us of any misplaced notion that the rest of the World comes under the protection of the US Constitution. It might well be that cyberspace is a creation of the Central Intelligence Agency (CIA) to facilitate global surveillance, as the Russians would have us believe. That notwithstanding, Klimburg divides the world between the good guys—the 'free internet coalition', largely comprising the Western democracies—and the bad guys—the 'cyber-sovereignty bloc', a group of countries led by Russia and China.

The chapters on the motivations and approaches of Russia and China towards cyberspace try to provide the counterpoint towards the excessive focus on American interests, formulations, actions and justifications that make up much of the book. While an equal number of pages are devoted to examining the Russian and Chinese approaches and actions, Russia is called out much more than China for being a bad actor in cyber space. The origins of the Russian approach are explained thus: the Russians have seen cyberspace as an existential threat and have responded, both internally and externally, through a series of actions intended to mitigate that threat, and turn the tables on their adversaries using the same medium. Their wariness about information goes back to the days of the Cold War, and the models they have used to counter these threats also come from that era. The symbiotic relationship between Russian intelligence agencies and cyber-criminals is also covered exhaustively, as also the impact of the latter's activities globally. That said, much of the evidence is circumstantial and, sometimes, a bit of a stretch. Some of the issues examined give one a severe sense of *deja vu*. The internet security company Kaspersky, for instance, has always been under a cloud of suspicion for its supposedly close links with Russian intelligence, but again, no conclusive evidence is established. Using the same yardstick, there are any number of American companies that have close links with US intelligence, in some cases even being provided with start-up funding. Klimsburg speculates as to the motivations behind Russian actions in cyberspace, which he feels will only hurt it in the long run. He comes to the conclusion that these are not dissimilar to the North Korean use of threats and bluster that would only result in a similar fate of isolation and being ostracised, and which might simply be a case of wishful thinking.

Though China's perspectives and actions in cyberspace are roughly similar to Russia, the former is treated with much more respect and understanding in the book. China's achievements in the domain and

its use of cyberspace to improve the wellbeing of its citizens are quite commendable and there is an earnest effort made to understand the compulsions that led the Chinese leadership to impose strict controls on the Internet to maintain law and order. The book also examines Chinese cyber espionage and speculates that it is largely the outcome of loose controls on the part of the government. Reduced espionage in the recent past, especially post the Obama-Xi summit of 2015 where President Obama is supposed to have read out the riot act, is seen as proof of this. However, the Chinese efforts at incorporating cyberwarfare into military doctrines, the size and scope of the military forces, and the resources that have been devoted to cyberwarfare are indicators enough that, for better or for worse, the militarisation of cyberspace is gathering pace. Countries that ignore these developments would do so at their peril.

The last part of the book on parsing cyberpower provides some useful takeaways, the crux being that the totem pole in cyberspace is still one in the making. There have been many rankings of cyberpowers based on perceptions of its constituent elements but all have been found wanting. Bean counting of cyber capabilities, cyber weapons, technological prowess,etc., does not work as with hard power capabilities. This is because there are too many variables and many of the components and capabilities are kept hidden. While the US is, based on many of these parameters, the most powerful cyberpower, it is also the most vulnerable, as evidenced by successive attacks on it. As cyber attacks encroach deeper into the information domain, democratic countries find themselves more vulnerable since it is much harder for these countries to balance security versus other myriad considerations.

Like other authors before him, Klimsburg finds it difficult to surmount the chasm between the reality of state perspectives and the utopia of a cyberspace that is free of all encumbrances. As Klimsburg himself states, cyberspace changes so rapidly that the book, begun in an age of innocence seems to have become outrun by events relating to its core theme of warning liberal democracies of the dangers of enlarging cybersecurity to information security.

The book falls short when it comes to examining the role of the middle and emerging democratic powers other than slotting them into the 'free internet coalition' under the leadership of the US. It does not pay sufficient attention to the priorities and motivations that drive the cyberspace policies of many of these countries; for example, middle powers like India and Brazil merit only a few sentences in the book. Doing away

with footnotes means that Klimsburg can make outlandish statements about India and Brazil having 'burgeoning offensive' capabilities without having to provide any reference to substantiate that claim.

That said, *The Darkening Web* is a welcome addition to the burgeoning literature on cyberspace, and adds new insights that helps one further along the path of understanding the quixotic nature of the medium and the various forces that alternately assail and seek to control it. Klimsburg's suggestions to disaggregate and simplify the existing policy dimensions and focus areas of cyberspace look good on paper but would require a unity of purpose in the global community and amongst governments that simply does not exist today. The abiding thought one is left with is that the US had many opportunities to fix global cybersecurity right up to the end of the first decade of the 21st century, but chose not to do so for its own selfish motives.