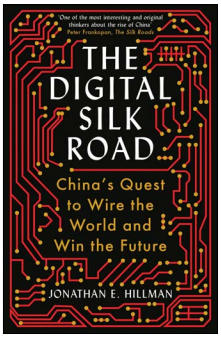
Book Review



The Digital Silk Road: China's Quest to Wire the World and Win the Future

Author: Jonathan E Hillman

Publisher: Profile Books Ltd (2022) (**ISBN:** 978-1788166867), 368 pages

Reviewed by Flight Lieutenant Ethan Haylock

Introduction

The Digital Silk Road: China's Quest to Wire the World and Win the Future represents a timely and accessible account of China's swift rise as a digital superpower, and the global permutations should China supplant the US as the world's technological hegemon. The book examines trends pertaining to China's 'Digital Silk Road' white paper released in 2015, which itself represented an extension on China's 2013-announced 'Belt and Road Initiative'. Hillman conveys his cautionary tone on China's digital policy through pairing the lenses of - wireless networks, internet connected devices, internet backbone and satellites, with rigorously researched case studies. Hillman lucidly conveys the significance of China's vast digital reach in terms of hardware, enabling the generalist reader to comprehend the significance of potentially unrivalled Chinese oversight over vast quantities of data, financial markets and global communications.

Hillman is a Senior Fellow at the Centre for Strategic and Industrial Strategy and former Fulbright Scholar, specialising in tracking China's Belt and Road Initiative. Writing during the pandemic, the author remarks on the impact of COVID-19 in expediting the migration of key services into the online space, in turn increasing the importance of physical hardware supporting virtual infrastructure. Hillman's background in international trade also enables

him to equate the significance of China's expanding digital hardware footprint domestically and overseas, with its ability to insulate itself from prospective US economic sanctions, a notion that is particularly apt given ongoing debate pertaining to the territorial status of Taiwan.

The Digital Silk Road begins by charting the progress of China in the post-Cold War technological space, pairing its rise with the mistaken belief of Western Governments that the proliferation of the internet would inherently spread liberty. Hillman clarifies the subsequent Chinese policy, whereby a domestic version of the internet resembling a 'medieval castle' (p. 2) was developed within China, while Chinese companies, ostensibly extensions of the state, began engaging with developed and developing states globally, including through the proliferation of authoritarian surveillance technologies. China's underlying ability to exploit data is identified throughout as a potential threat to western commercial and strategic advantages in the virtual domain.

Hillman uses the downfall and eventual bankruptcy of the Canadian company Northern Telecom (Nortel), and corresponding rise of Huawei as a cautionary anecdote for what the author perceives as the subversive motives of Chinese telecommunications strategy. Indeed, the case study of Nortel is employed to highlight China's propensity to use its economic market as 'bait' (p. 22) as a mechanism to copy and replicate western technology. Despite opening a facility in Beijing in 1994, Nortel was allegedly the target of a cyber-attack in 2004 which leaked numerous technical documents purportedly traced to People's Liberation Unit 61398. Huawei's subsequent expansion of operations in North America, at Nortel's expense, is articulated as testament to the ruthlessness of China's discrete authoritarian telecommunications strategy.

The reach of China's state-subsidised telecommunications companies such as Hikvision and Huawei is brought home by case studies such as one charting the success of Huawei in installing virtual infrastructure in Glasgow, Wyoming, one of the United States' most remote towns. Hillman also effectively encompasses the virtual reach of China within the developing world, including in Africa, where China has built 70 per cent of extant 4G internet hardware. The scale of the challenge to the US' strategic position as the world's foremost network operator is cogently communicated throughout, with a series of warnings made to western governments also of direct relevance to the commanders and aviators of tomorrow.

The author outlines a series of recommendations to US and western policy makers, who are encouraged to continue nascent measures to contest the reach and entrenchment of Chinese hardware in the western and developing world. Hikvision and Huawei 'sell capabilities as well as methods' (p. 128), alluding to the potential for Chinese telecommunications policy to shape and codify a new and increasingly authoritarian digital reality, including through coercive measures facilitated by the very reach of their hardware Digital Silk Road. Hillman's contribution is valuable precisely because it conveys the process by which China is shaping

global hardware and software standards, and the potential consequences this will have, as well as the costs of Chinese primacy over vast quantities of data.

The Digital Silk Road complements a popular and growing field of writing pertaining to China's worldview, and its employment and control of information in support of strategic objectives. Where David Kilcullen discusses China's conceptual broadening of its perception of warfare in *The Dragons and the Snakes*, and James Griffiths investigates the domestic controls China has placed on virtual information in *The Great Firewall of China*, Hillman focuses directly on the reach of Chinese telecommunications hardware internationally and the pervasiveness of its values telecommunications, even compared to Congress-subsidised US firms. The banning of TikTok on UK government devices, and the UK government's announcement of the removal of Huawei technology from UK 5G networks by 2027, are testament to Hillman's observations, which are likely to remain pertinent for some time yet.

All military professionals should consider reading *The Digital Silk Road* given the *Integrated Review Refresh's* acknowledgement of the 'systemic challenge' posed by China under the Chinese Communist Party. As the great power competition between states permeates into the digital domain, commanders and aviators will be increasingly expected to possess a cognisance of how the virtual sphere is used by state actors such as China as a mechanism for 'redrawing the map of the internet' (p. 131). These actions are of direct relevance to western air forces who must keep astride of their relevance in the Air, Cyber and Space Domains.