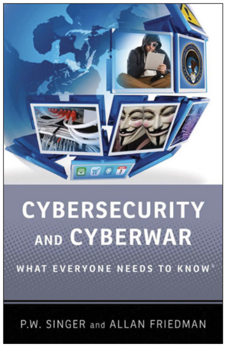
Citation for published version (APA):
Withers, P. (2015). Review: P.W. Singer and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. *The Chief of the Air Staff's Reading List*, 20-21.

Cybersecurity and Cyberwar: What Everyone Needs to Know



By P.W. Singer and Allan Friedman

Publisher: Oxford University Press 2014
ISBN: 978-0-19-991811-9, 306 pages

Reviewed by Squadron Leader Paul Withers

Cybersecurity and Cyberwar is a wide ranging and detailed examination of the issues related to the cyber environment. The authors were motivated the write the book after hearing a senior leader in the US Department of Defense struggle to articulate the importance of cyberspace, having only been capable of describing the complexity of the problem as 'all this cyber stuff'. The main premise of the book is to address 'the cybersecurity knowledge gap and the dangers it presents'. Singer and Friedman assert that the gap is partly generational but also due to cybersecurity sitting in a 'no man's land' between those who understand the technology and those who understand the broader policy and operating environment.

Peter Singer has developed a reputation for expertise in the implications of unmanned and autonomous systems and is perhaps best known for his book *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (see CAS' Reading List 2011). He is a former Senior Fellow at the Brookings Institution and is currently a strategist at the public policy 'think tank', New America Foundation. Allan Friedman has a similar background in think tanks, having also been a Brookings Fellow and crucially has an academic background that spans both Computer Science and Public Policy. The book is written with academic rigour and published by a prestigious publishing house but is clearly not written solely for academics. The authors highlight the condition known as 'the glaze', that 'unmistakable look of profound confusion and disinterest that takes hold whenever conversation turns to workings of a computer'. They contrast 'the glaze' with the rolling of the eyes displayed by the 'computer savvy' who see the world through a technological lens, but may not appreciate the bigger picture. The content and style of *Cybersecurity and Cyberwar* produce a text that is accessible for both extremes of audience and everyone in between.

Singer and Friedman structure the text in a Question and Answer format, with the answer to each question being a combination of eloquent explanation, historical analysis and first-hand experience from a range of Subject Matter Experts. The book is split into three main parts, with Part I addressing 'How it all Works.' The authors explain the terminology and concepts behind cyberspace in an easy to absorb manner, managing to distil the technical detail into a story encompassing history and topography, rather than the underpinning computer science. Doctrinal purists might argue with the precision and completeness of some of the definitions given, but they are nonetheless thought provoking and challenging. Crucially they draw out the issue that cyberspace is as much a human sciences challenge as it is computer science. Despite the technical nature of a cyberspace exploit, it is more often than not the human factors associated with an attack that prove to be the weakest link. This is illustrated through their discussion of often quite sophisticated 'phishing' attacks through to the 2008 attack known as Buckshot Yankee, where a soldier picked up a flash drive in a car park and introduced it into US Central Command's network. The drive contained malicious software originating from a Foreign Intelligence Service and led to a 14 month clean-up operation.

The first part of the book provides the reader with the foundation of knowledge that allows them to move on to ask the key 'so what?' question in Part II, 'Why it all matters'. This part examines the implications of cybercrime, cyberespionage and hacktivism, before moving onto the areas that should raise the specific interest of the military audience: conflict in and through cyberspace. Singer and Friedman draw out some of the lessons of notable historical events in Estonia, Georgia, the Stuxnet attack on Iran, and the Israeli integration of air power with Computer Network Operations during Operation Orchard. They discuss what this means for the conduct of warfare, including issues around 'cyber weapons' and the associated ethical and legal implications. Two case studies of military approaches to cyber warfighting are offered through examination of the US and China before going on to question the 'cult of the offensive' in cyber warfare, arguing for the importance of cyber defence.

Part III of the study looks at 'What we can do about it', addressing some of the practical measures to address cyber security challenges, whilst explaining the limits of the State and the partnership that needs to exist between the public and private sectors. Of key concern is the 'Human Capital Crisis in Cyber Security', overcoming an acute shortage of skilled and educated cyber professionals that affects industry and government across the developed world. It offers some insight into addressing the problem for the UK military, which suffers from the same challenge in microcosm - growing and retaining Cyber Warfighters.

This book retains the engaging and often humorous style that has been a feature of Singer's previous work. The authors manage to examine the serious issues with appropriate gravitas and academic rigour whilst still capturing the 'whimsy' of the Internet and elements of popular culture. Where there was previously a paucity of credible, non-sensationalist literature, this book adds to a growing body of work that is grounded in reality but adds insight. This is a good book for anyone who wishes to be both educated and entertained. However, for those airmen and women who are serious about developing their understanding of the cyberspace environment, this is another important book. If we accept the vital importance of cyberspace threats and opportunities for air power, this book will help equip the practitioner to engage in the conceptual and practical development of the cyberspace environment. It should be studied alongside Healey's '*A Fierce Domain*' (see CAS' Reading List 2014) and Rid's '*Cyberwar Will Not Take Place*' (see Air Power Review Vol 16 No 3). Airmen and women undoubtedly have a great deal to offer in the development of cyberspace operations, but in order to contribute both conceptually and operationally, they must develop a credible understanding and an intuitive feel for the cyberspace environment. *Cyberspace and Cyberwar* is an excellent book and will assist in closing the 'knowledge gap'.