

Australia and Cyber-warfare

Gary Waters, Desmond Ball, Ian Dudgeon

This book explores Australia's prospective cyber-warfare requirements and challenges. It describes the current state of planning and thinking within the Australian Defence Force with respect to Network Centric Warfare, and discusses the vulnerabilities that accompany the use by Defence of the National Information Infrastructure (NII), as well as Defence's responsibility for the protection of the NII. It notes the multitude of agencies concerned in various ways with information security, and argues that mechanisms are required to enhance coordination between them. It also argues that Australia has been laggard with respect to the development of offensive cyber-warfare plans and capabilities. Finally, it proposes the establishment of an Australian Cyber-warfare Centre responsible for the planning and conduct of both the defensive and offensive dimensions of cyber-warfare, for developing doctrine and operational concepts, and for identifying new capability requirements. It argues that the matter is urgent in order to ensure that Australia will have the necessary capabilities for conducting technically and strategically sophisticated cyber-warfare activities by the 2020s.

The Foreword has been contributed by Professor Kim C. Beazley, former Minister for Defence (1984–90), who describes it as 'a timely book which transcends old debates on priorities for the defence of Australia or forward commitments, [and] debates about globalism and regionalism', and as 'an invaluable compendium' to the current process of refining the strategic guidance for Australia's future defence policies and capabilities.



E P R E S S

ISBN 9781921313790 \$19.95 (GST inclusive)

ISBN 9781921313806 (Online)

First published July 2008



http://epress.anu.edu.au/cyber_warfare_citation.html