Foreword
by Professor Kim C. Beazley

In 2002 I visited Afghanistan as part of a parliamentary delegation. At Bagram base, while visiting our Special Air Service (SAS) contingent, we were hosted at the headquarters of the 10th Mountain Division on one of the first of their seemingly interminable deployments to the Afghanistan fight. There we saw soldiers sitting behind banks of personal computers controlling everything from the Division's logistics to the units in the field.

We witnessed the interaction between US dominance of the electro-magnetic sphere and its use of cyber-space. Satellites beamed in the ongoing battle and communications relevant to the forces engaged. The Division Commander had the exact location of his forces and those they engaged. We could see the practical effects with orders for A-10 ground support or helicopter extraction as the base responded instantly to requests and constantly added to the information of company and platoon commanders in the field. I asked the Division's Commander how he resisted taking over platoon command in such a situation. "It's difficult," he responded. We were witnessing what the Australian Defence Force described in its 2020 vision statement as 'network-enabled operations'.

It was clear from our subsequent conversations with SAS personnel how much their small unit patrols were enveloped by the plethora of information on their situation which came from a multiplicity of surveillance capabilities and the array of responses and advice they could draw on from the levels of command they were plugged into. It was a privileged view of warriors standing on the bottom rung of future information age warfare.

Politics has distorted what is really important in the Australian debate on our future defence needs. We are obsessed with platforms and personnel numbers. Over the last decade, the Australian Government has burnished its popular security credentials by junking any serious study of platform needs and acquiring capabilities based on immensity with big dollar signs attached, thereby seeking to impress public opinion with size and cost whilst saying little of relevance about modern and future warfighting.

We are a clever and technologically capable people. Partly courtesy of our allied relationship, we are deeply aware of the US ability to exploit the possibilities of electro-magnetic waves and cyber-space. We host and participate in the operation of cutting-edge installations such as those at Pine Gap. Involvement in Iraq (and even more in Afghanistan) and collaboration in the 'war on terror' have given us access to the heart of frontier advances in information operations. Through organisations like the Defence Signals Directorate we make direct contributions. Scattered through Defence and security related departments, like the Attorney-General's, we have institutions responsible

for exploiting electro-magnetic and cyber-space for information on those who are our enemies or would be enemies, and using the same space to combat them.

George Orwell said during the Second World War that we sleep safe in our beds because rough men do violence in the night to those who would wish us harm. The rough men are now joined by the 'geeks' of both genders. Yet there are gaps in capability, objectives and missions. As the Australian Government sits down to contemplate its defence White Paper, we expect answers on extra battalions of soldiers, the necessity for the *Super Hornet*, the value of the *Canberra* class LHDs, and the timing of the next generation of submarines. No-one is waiting with bated breath for what it will say about our ability to conduct cyber-warfare or even on what is meant by our capabilities in network-enabled operations. Certainly no-one is waiting to read about our intelligence services transitioning to warfighting operations.

Except perhaps the authors of this study. I cannot begin to attest to the veracity of the material which follows. Like most politicians I have been caught up for a decade in the need for the quick fix in responses to the crises that have emerged since the 11 September 2001 terrorist attacks on the United States.

Whatever emerges in the debate over the next few years on the White Paper, one perception in the White Paper I was responsible for over 20 years ago remains valid today. Our long-term survival depends on a clear understanding of capabilities which may be used against us and on the clear need for a small nation to sustain a technological edge in meeting them. We live in a broader region which is, as one of the authors points out, a test-bed for future information warfare. To this point the edge has been sought defensively; in the future it will need to be sought aggressively.

The authors seek the establishment of an Australian Cyber-warfare Centre to coordinate the development of capabilities that will decisively enhance our forces in the field—but, more than that, ensure that the tools which enhance our warriors are tools in the fight itself. This is a timely book which transcends old debates on priorities for the defence of Australia or forward commitments. It transcends debates about globalism and regionalism. These are global capabilities, but with a multitude of effects in any part of geography that is vital. This book will serve as an invaluable compendium for subsequent judgement about official documents and commentaries that will deluge us as all sections of the Australian Government rethink our national security priorities.

Kim C. Beazley

Professor of Social and Political Theory
University of Western Australia
(Minister for Defence, 1984–90)

March 2008