Protection of Australia in the Cyber Age

Matthew J. Warren, Deakin University, Australia

Shona Leitch, Deakin University, Australia

ABSTRACT

Australia has developed sophisticated national security policies and physical security agencies to protect against current and future security threats associated with critical infrastructure protection and cyber warfare protection. In this paper, the authors examine some common security risks that face Australia and how government policies and strategies have been developed and changed over time, for example, the proposed Australian Homeland Security department. This paper discusses the different steps that Australia has undertaken in relation to developing national policies to deal with critical infrastructure protection.

Keywords: *Critical Infrastructure Protection, Cyber Warfare, National Security Policy, Security Agencies, Security Threats*

INTRODUCTION

Australia is a modern society and is highly dependent on key critical systems at the national and state level. These key systems have become more dominant as the Information Age has developed. These key systems are grouped together and described as critical infrastructure; this is infrastructure so vital that its incapacity or destruction would have a debilitating impact on defence and national security (Lewis, 2006). Many of these critical systems are based upon ICT (Information and Communication Technology) systems.

Australia takes ICT security very seriously, it has been estimated that Australian organisations spend between A$1.37 – A$1.74 billion per year on IT security, and the total financial losses due to computer-related security incidents in the 2006 financial year have been estimated to be between $595 and $649 million (Australian Institute of Criminology, 2009).

This paper will review the current strategies used by Australia over a decade and evaluate their differences and discuss the reasons for these differences. Future threats such as Cyber Warfare and the steps that are being proposed will be considered. This paper will highlight current Australian best practices in critical infrastructure and cyber warfare protection many of which may be applicable in a European context and provide an informative contrast.

Initial View of the Australian Federal Government

The initial focus of the Australian Federal Government policy was that critical infrastructure protection was a commercial consideration

DOI: 10.4018/ijcwt.2011010104

Copyright © 2011, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

and related to Information Security (Busuttil & Warren, 2004).The Australian Federal Government has been aware of the problems that Australian corporations may have with dealing with these new security issues. The Australian Federal Government has responded by offering advice for corporations. The initial Australian Government advice (Australian Government: Attorney-General's Department, 1998) suggested ways in which organisations could reduce Critical Infrastructure Protection risks (Busuttil & Warren, 2004):

- Organisations should implement protective security such as passwords, etc., in accordance to a defined security standard such as as/nzs 4444 (now 17799) (information security management);
- Organisations should formally accredit themselves against security standards such as as/nzs 4444 (17799);
- Organisations should raise awareness of security issues such as password security, e-commerce risks among their staff;
- Organisations should train their staff in how to use computer security systems efficiently and effectively.

This advice was subsequently updated and in 2004 the Australian Government responded with new security advice (Department of the Prime Minister and Cabinet, 2004):

- The Australian and New Zealand Standard for Risk Management AS/NZS 4360:1999 is the standard by which all critical infrastructure will be assessed to assist with the review of risk management plans for prevention (including security), preparedness, response and recovery.

In 2004 the Australian Federal Government formally defined the following; "Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security" (Department of the Prime Minister and Cabinet, 2004). In essence this description describes organisations that exist at a government level or at a corporate level (Department of the Prime Minister and Cabinet, 2004).

Historically, much of Australia's infrastructure was originally owned and operated by the public sector at the federal, state and local government levels (Smith, 2004) however the majority of Australia's critical infrastructure has now been privatised and is under private sector ownership. Consequently, protecting Australia's critical infrastructure now requires a higher level of cooperation between all levels of government and the private sector owners. Hence, the federal government has developed a policy for critical infrastructure protection that focuses broadly on addressing the following strategies (Department of the Prime Minister and Cabinet, 2004; Australian Government: Attorney-General's Department, 2004):

- Distinguishing critical infrastructures and ascertaining the risk areas;
- Aligning the strategies for reducing potential risk to critical infrastructure;
- Encouraging and developing effective partnerships with state and territory governments and the private sector;
- Advancing both domestic and international best practice for critical infrastructure protection.

As Warren and Leitch discussed (2010), the Australian Federal Government recognised the importance of crucial systems and the development of new industry support mechanisms, in particular Trusted Information Sharing Network (TISN).

The TISN is a forum in which the owners and operators of critical infrastructure work together by sharing information on security issues which affect critical infrastructure (TISN,

Copyright © 2011, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/protection-australia-cyber-age/61329

Related Content

Risks of Critical Infrastructure Adoption of Cloud Computing by Government
Mansoor Al-Gharibi, Matthew Warrenand William Yeoh (2020). *International Journal of Cyber Warfare and Terrorism (pp. 47-58).*
www.irma-international.org/article/risks-of-critical-infrastructure-adoption-of-cloud-computing-by-government/257518

Ethos Construction, Identification, and Authenticity in the Discourses of AWSA: The Arab Women's Solidarity Association International
Samaa Gamie (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 1629-1655).*
www.irma-international.org/chapter/ethos-construction-identification-and-authenticity-in-the-discourses-of-awsa/251515

OSNs as Cyberterrorist Weapons against the General Public
Nicholas Ayres, Leandros Maglarasand Helge Janicke (2017). *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities (pp. 179-197).*
www.irma-international.org/chapter/osns-as-cyberterrorist-weapons-against-the-general-public/172296

An Internet-Mediated Pathway for Online Radicalisation: RECRO
Loo Seng Neo (2019). *Violent Extremism: Breakthroughs in Research and Practice (pp. 62-89).*
www.irma-international.org/chapter/an-internet-mediated-pathway-for-online-radicalisation/213299

Tracing the Cultural Background of Lone-Wolf Terrorism: Dilemmas, Contradictions, and Opportunities for the Next Decade
Maximiliano Emanuel Korstanje (2021). *International Journal of Cyber Warfare and Terrorism (pp. 45-56).*
www.irma-international.org/article/tracing-the-cultural-background-of-lone-wolf-terrorism/270456