International Journal of Cyber Warfare and Terrorism (IJCWT), 15(1), 19-29

Good Governance and Virtue in South Africa’s Cyber Security Policy Implementation

Oliver Burmeister, School of Computing and Mathematics, Charles Sturt University, Bathurst,

Australia Jackie Phahlamohlaka, Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa

Yeslam Al-Saggaf, School of Computing and Mathematics, Charles Sturt University, Wagga Wagga, Australia

Abstract

Good governance from an ethical perspective in cyberdefence policy has been seen in terms of duty and consequentialism. Yet the negotiated view of virtue ethics can also address how nation states mitigate the risks of a cyber attack to their national interests and to prepare for a cyber offence in response to an attack. A discourse analysis of the “0x Omar”-Israeli conflict of 2012, as reported in the Arabic and English media and on the Internet, is used to explore ethical issues that this case raises and to examine how the risks posed could be mitigated in relation to relevant elements of the South African cybersecurity policy framework. Questions raised include: At what point does the policy require a nation state to prepare for a cyber offence in response to a cyber attack? Ethically, how are such actions consistent with the principle of good governance?