Chapter 19
Good Governance and Virtue in South Africa's Cyber Security Policy Implementation

Oliver Burmeister
Charles Sturt University, Australia

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

Yeslam Al-Saggaf
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?

1. INTRODUCTION

Cybersecurity policy is a necessary part of the governance process of a nation state. Good governance is typically seen ethically from either a deontological viewpoint, that is or duty, or from a utility viewpoint, that is, protecting the greater public good. Rarely is it discussed from a virtue ethics point of view, although this third major normative ethic also has contributions to make. Although often seen in individual terms (Vallor, 2013), that is, in terms of a person's moral character, the notion of agency within

DOI: 10.4018/978-1-5225-5634-3.ch019

it also allows for a corporate social responsibility (CSR) perspective, which encourages stewardship, or good governance processes. More generally, cyberdefence policies address ethical issues including the 'attribution problem', moral responsibility, the inadequacy of secure systems, risk mitigation, and the moral justification of a cyber attack on a nation state's vital interests in response to a cyber attack carried out by people residing in that nation state.

While the 'attribution problem', the moral responsibility of nation states, as opposed to that of individuals within a nation state, and the moral justification of a cyber attack are still debated, cyber attacks continue to pose real threats. Those threats need to be recognised when they occur and responded to immediately, to protect sensitive infrastructure, as well as individual citizens. Governance of security policies could ensure that national interests are safe-guarded, that peaceful solutions to threats are effected, and that where necessary, counter-measures are successfully implemented.

Using a discourse analysis of the "0x Omar"-Israeli conflict of 2012, as reported in the Arabic and English media and on the Internet, this article explores the ethical issues. It examines how the risks posed could be mitigated through policy implementation. The "0x Omar"-Israeli conflict of 2012 revealed multiple areas that a nation needs to safe-guard against. Initially it appeared an isolated incident, then it appeared to be a coordinated attack against national infrastructure. Deception was involved not only in the strategy employed to make it appear isolated initially, but also in terms of who the attackers were. At first it was not clear if it was the work of an isolated terrorist, or something more sinister. Even when it became clear that the nation initially thought responsible for the attack was not responsible, and there was strong evidence that it was another nation, that evidence was inconclusive for some time.

This article begins with a literature review, firstly of virtue ethics as it relates to good governance, and secondly of national security within the context of cyber attacks. It examines how policies have been developed to mitigate the threats posed by such attacks, and goes on to examine the case allegedly involving "0x Omar" and Israel. Then an analysis of relevant elements of the South African cybersecurity policy framework is conducted in relation to ethical dimensions of the "0x Omar"-Israeli case. Finally implications are drawn for other national security policies.

2. LITERATURE REVIEW

Cyberdefence has grown in scope over recent decades, particularly as nations have taken steps to provide wider segments of their society with access to information infrastructure. There have been numerous instances of attacks on national infrastructure, such as the well publicised attacks on Estonia (Shackelford, 2009). As nations expand their national broadband capabilities, they become more attractive targets to cyber attacks (Phahlamohlaka, van Vuuren, & Coetzee, 2011). The ethical positions on cyberwar frequently focus on only two of the three major normative ethics theories. We begin with a view of the third, that of virtue ethics. Thereafter we examine three areas which define what is encompassed by the terms 'national security' and 'cyberwar', as well as showing how policies could act as mitigation strategies.

2.1. Good Governance

In ethical discussions concerning the governance process, the theory usually in evidence is that of utility. However, in terms of CSR good governance can also be seen in virtue ethics terms. Before describing how virtue is part of good governance, it is necessary to first discuss virtue ethics more generally.