An Approach to Governance of CyberSecurity in South Africa

Joey Jansen van Vuuren, Council for Industrial and Scientific Research, Pretoria, South Africa

Louise Leenen, Council for Industrial and Scientific Research, Pretoria, South Africa

Jackie Phahlamohlaka, Council for Industrial and Scientific Research, Pretoria, South Africa

Jannie Zaaiman, University of Venda, Thohoyandou, South Africa

ABSTRACT

A government has the responsibility to provide, regulate and maintain national security, which includes human security for its citizens. Recent declarations from the UK and USA governments about setting up cybersecurity organisations and the appointment of cyber czars reflect a global recognition that the Internet is part of the national critical infrastructure that needs to be safeguarded and protected. Although the South African government approved a draft National Cyber Security Policy Framework in March 2012, the country still needs a national cybersecurity governance structure in order to effectively control and protect its cyber infrastructure. Whilst various structures have been established to deal with cybersecurity in South Africa, they are inadequate and implementation of the policy is still in the very early stages. Structures need to be in place to set the security controls and policies and also to govern their implementation. It is important to have a holistic approach to cybersecurity, with partnerships between business, government and civil society put in place to achieve this goal. This paper investigates different government organisational structures created for the control of national cybersecurity in selected countries of the world. The main contribution is a proposed approach that South Africa could follow in implementing its proposed cybersecurity policy framework, taking into account the challenges of legislation and control of cybersecurity in Africa, and in particular, in South Africa.

Keywords: *Cybersecurity, Cybersecurity Awareness Toolkit, Governance, National Security, Policy Implementation*

1. INTRODUCTION

Around the world cybersecurity challenges give rise to serious national security alarms. There is an international drive by various governments to either develop and implement, or review existing cybersecurity policies. From the point of view of the United States of America (USA), these policies include strategies and standards regarding the security of and operations in cyberspace, and encompass the full range of threat reduction, vulnerability reduction, de-

DOI: 10.4018/ijcwt.2012100102

terrence, international engagement, incident response, resiliency, and recovery policies and activities - including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The USA has created a Cyber Command (CYBERCOM) under the Strategic Command led by the head of the National Security Agency (NSA) which reports directly to the President. The main stated reason for this command chain was that the current capabilities to operate in cyberspace have outpaced the development of policy, law and precedent to guide and control these operations.

Developing nations such as South Africa focus more on the increase of connectivity and neglect the risks that accompany the connectivity. An over-reliance on cyberspace compelled the USA to start all its cybersecurity initiatives. Developing nations will have no option but to join in the race for cybersecurity policy development and implementation. These countries need to satisfy themselves, as well as instil the confidence across their nations, that the networks that support their national security and economic wellbeing are safe and resilient. Statistics also has shown that despite a low Internet penetration rate, South Africa ranks third in the world after the USA and United Kingdom (UK) in terms of the number of cyber attacks a country encounters (Amit, 2011).

In its draft cybersecurity policy (SA Government Gazette, 2010), the South African government has acknowledged that it does not have a coordinated approach in dealing with cyber security. Whilst various structures have been established since the approval of the policy in 2012 (South African Government Information, 2012) to deal with cybersecurity issues, they are inadequate to deal with the issues holistically. Although some interventions to deal with cybercrime have been put in place, there is a need for a partnership between business, government and civil society to develop an efficient cyber security strategy. South Africa's efforts to ensure a secured cyberspace could be severely compromised without this holistic approach. As part of the cybersecurity strategy and implementation, we propose a cybersecurity governance structure and an implementation model based on the Cyber Security Awareness Toolkit (CyberSAT) (Phahlamohlaka, Jansen van Vuuren, & Coetzee, 2011) that is underpinned by key National Security imperatives as well as by international approaches. Our proposal draws on several analyses of international trends and comparisons with key elements of South Africa's cybersecurity policy.

Section 2 contains an overview of the evolution of cybersecurity structures and policies in Estonia, the USA, UK, South Korea, China and Australia. In Section 3 we draw on these international approaches to craft a proposal for cybersecurity structures and the implementation of a cybersecurity policy for South Africa. The paper is concluded in Section 4.

2. INTERNATIONAL APPROACHES

In this section we give a brief overview of the development and status of cybersecurity structures and policies in several other countries.

2.1. Estonian Approach and NATO Developments

Estonia is seen as the world's first victim of cyber war, although web traffic was already jammed during the Kosovo war 10 years ago. When Estonia came under cyber attack in 2007, the country realised the necessity of a cyber defence policy. Multiple botnets were used to conduct Distributed Denial of Service (DDoS) attacks against critical national infrastructure, media, telecommunications and the main banks. Websites were also defaced and a significant portion of the economy and government ground to a halt. Although it was suspected that the culprits were Russian nationals, the Russian government did not want to assist in the search for these cyber attackers (Boyd, 2010). These attacks resulted in the North Atlantic Treaty Organization (NATO) creating the NATO Cyber