Author: MN Njotini

PROTECTING CRITICAL DATABASES – TOWARDS A RISK BASED ASSESSMENT OF CRITICAL INFORMATION INFRASTRUCTURES (CIIS) IN SOUTH AFRICA

ISSN 1727-3781

2013 VOLUME 16 No 1

http://dx.doi.org/10.4314/pelj.v16i1.14

PROTECTING CRITICAL DATABASES – TOWARDS A RISK BASED ASSESSMENT OF CRITICAL INFORMATION INFRASTRUCTURES (CIIS) IN SOUTH AFRICA

MN Njotini*

1 Introduction

South Africa has long recognised the need to protect critical infrastructures (CIs). For example, legislations such as the *Defence Act*[1] and the *National Strategic Intelligence Act*[2] contain measures that, amongst others, guarantee the safeguarding of CIs. More specifically, the *Defence Act* requires the gathering, collating, evaluating and using of strategic intelligence related *inter alia* to the security of South Africa.[3] The strategic intelligence is gathered, collated, evaluated and used in order to assess the attacks or threats of attacks to the security of South Africa's CIs.[4] In general, CIs encompass structural and physical places or areas that are of strategic interest to a country,[5] places or areas that are vital to the country's safety and security and the wellbeing of its citizens.[6] Examples of CIs include *inter alia* petro-chemical stores (eg pump stations and oil refineries), international airports, the reserve bank, electricity distribution stations, strategic power stations, and water storage and distribution facilities. Attacks or threats of attacks to CIs have in the recent past proved to be real and pervasive. These attacks or threats of attacks can take various forms. For example, CIs can be damaged or destroyed by deliberate acts of terrorism, natural disasters, negligence or malicious behaviour.[7] Two independent attacks to CIs are described below in illustration. The first was an

* Mzukisi Niven Njotini. LLB, (Vista University), LLM *Cum Laude*: Information Technology Law, (University of South Africa), LLD Candidate, (University of South Africa). Senior Lecturer, Department of Jurisprudence, College of Law: University of South Africa. Email: njotim@unisa.ac.za.

1 *Defence Act* 42 of 2002.

2 *National Strategic Intelligence Act* 39 of 1994.

3 Section 34(a) *Defence Act* 42 of 2002.

4 Section 1(xvi) *National Strategic Intelligence Act* 39 of 1994.

5 Section 1 *National Key Points Act* 102 of 1980.

6 Section 1 read with s 2 *National Key Points Act* 102 of 1980.

7 Commission of the European Communities 2006 http://bit.ly/Z497fe.

attack that on parts of the United States of America (the US) and Canada. It occurred during August 2003 and targeted the Eastern Seaboard Power Plant, which transmits electricity to certain parts of the US and Canada.[8] It caused power outages to an area of about 50 million people consisting of nine US states and the Canadian province of Ontario.[9] As a result of these outages, an amount estimated at 12 billion US dollars is reported to have been lost.[10] The second attack was a security breach in the Oak Ridge nuclear plant in the US (the Y-12 National Security Complex). In this instance, the attackers are reported to have targeted an area adjacent to the Highly Enriched Uranium Materials Facility (HEUMF).[11] The HEUMF keeps large amounts of uranium, which is used during the process leading to the manufacture of nuclear weapons.[12] Despite the fact that no harm was done to the HEUMF, it is accepted that the attack could have had catastrophic consequences.[13]

The emergence of novel technologies (ICTs), for example, the Internet and the World Wide Web or the Web, has changed the rules of the game regarding the safeguarding of CIs. ICTs can be used as a vehicle to foster socio-economic development. Some are essential in conducting business and exchanging information[14] by or between governments, businesses or individual ICT users, thus facilitating the establishment of our information society,[15] which enjoys the benefits *inter alia* of cheaper and faster access to ICTs; the provision of digital content for

8 US-Canada Power System Outage Task Force 2004 http://1.usa.gov/10t19NH.

9 Anderson *et al* 2005 *IEEE Transactions on Power Systems* 1922; VandenBrink 2011 http://bit.ly/Yr6ok9.

10 US-Canada Power System Outage Task Force 2004 http://1.usa.gov/10t19NH.

11 US Department of Energy 2012 http://1.usa.gov/XmvVwl.

12 US Department of Energy 2012 http://1.usa.gov/XmvVwl.

13 US Department of Energy 2012 http://1.usa.gov/XmvVwl.

14 The term information means a "piece of news with a meaning for the recipient; its assimilation usually causes a change within the recipient" (see Sieber "Emergence of Information Law" 10-11).

15 Dissimilar definitions of the concept "information society" have emerged, each being influenced by various technological, economic, spatial and cultural developments over the years (see Webster *Theories* 8-25). For the purposes of this research, the concept "information society" mean a society that is "characterised by a high level of information intensity in the everyday lives of most citizens, in most organisations and workplaces, by the use of common or compatible technology for a wide range of personal, social, educational or business activities, and by the ability to transmit, receive and exchange digital data rapidly between places irrespective of distance" (Durrani *Information and Liberation* 256).

worldwide networks,[16] and the acceleration of electronic commerce (e-commerce).[17] The ease of accessing recent ICTs results in or can result in the emergence of certain risks that weaken the security and stability of the information society. These include, amongst others, dishonesty, the illicit revelation of secret information, corruption, theft, deliberate disruption of the system, the destruction of ICT resources, and cyber-terrorism.[18] These risks demand that the information or data[19] recoded or kept on computers or computer software be safeguarded,[20] through the establishment of a dedicated information security structure referred to as a critical information infrastructure (CII).[21] CIIs generally form part of a country's overall cyber-infrastructure.[22] CIIs guard the various information systems[23] or networks that, if disrupted or destroyed, could have a prejudicial or adverse impact on the health, safety, security and monetary well-being of the citizens of a country or on the effective functioning or performance of a government or economy.[24]

Countries such as the US and Canada recognise the importance of safeguarding CIIs. More specifically, the US has framed a number of statutes in response to the attacks or threats of attacks on its CIIs. These include the *Computer Fraud and*

16 A network is an "intricately connected system of things or people." See Milone 2002 *Business Lawyer* 383.

17 See Council of the European Union and Commission of the European Communities 2000 http://bit.ly/YZQlMX.

18 For an interesting definition of the term "cyber-terrorism", see Denning 2000 http://bit.ly/16rUw3i.

19 The meaning of the term "data" in this context is different from that in the more usual context of computer data. Here the term data means the electronic representation of information in any form. See s 1 of the *Electronic Communications and Transactions Act* 25 of 2002 (the *ECT Act*). For further interesting reading, see the *Council of Europe's Convention on Cybercrime* (2001). This paper argues that the provisions of the *Electronic Communications Security Pty (Ltd) Act* 68 of 2002 may also be of assistance to the general scheme of securing CII. However, this paper examines the provisions of the *ECT Act*.

20 Katyal 2001 *U Pa L Rev* 1003-1006.

21 This paper acknowledges that information safeguarding extends beyond CIIs. In particular, information protection also encompasses *inter alia* authentication or validation and identity management processes.

22 Okhravi et al 2012 *IJCIP* 30.

23 Article 1(a) of the *Council of the European Union Framework Decision on Attacks Against Information Systems* (2005) [hereinafter referred to as Council Framework Decision 2005/222/JHA] defines an information system as any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for purposes of their operation, use, protection or maintenance.

24 Bendisch *et al* "Towards a European Agenda" 1-2; Van Niekerk and Maharaj 2011 *South African Journal of Military Studies* 101.

Abuse Act, 1986, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, 2001 (the so-called USA Patriotic Act), the *Cyber Security Enhancement Act*, 2002 and the *Cyber Security Research and Development Act*, 2002. Furthermore, a number of international organisations, eg the United Nations (the UN) and the Organisation for Economic Co-operation and Development (the OECD)[25] promote the need to safeguard CIIs. South Africa follows the approaches that are adopted by these countries or organisations. South Africa particularly utilises its national key points' security framework as a model to protect CIIs. This framework is set out in the *National Key Points Act* as amended. This paper investigates the South African approach to safeguarding CIIs to establish whether the South African framework is comparable to those of its international counterparts. In doing so, the OECD approach to secure CIIs will be used as a guide. The rationale is to establish inconsistencies and/or inadequacies, if there are any, in South Africa's CII protection framework.

The structure of the paper is straightforward: Section 2 discusses the notion "critical databases". The analysis includes an examination of a number of concepts that have relevance to the study of critical databases. Section 3 describes the different approaches to the safeguarding of critical databases. The approaches adopted and implemented by the OECD and South Africa, amongst others, will be investigated. Section 4 investigates the importance of the risk-based approach to safeguarding CIIs. Lastly, section 5 of this paper draws conclusions.

2 Critical databases

2.1 Background to the study

It is difficult to give a concise and accurate description of the term "critical database". Any attempt to do so should probably begin with scrutinising the

[25] The OECD is formally referred to as the Organisation for European Economic Cooperation or OEEC. It is an intergovernmental body that was established in 1961. The OECD currently has 34 member countries that continuously identify, discuss and analyse global challenges and problems, and promote policies to address those challenges and solve those problems.

meaning of the word "database" itself. Botma *et al* define a database as an organised collection of electronic software or tools that is used to store information.[26] This collection facilitates the accessing, retrieving and using of information or documents that are stored in databases.[27] Databases usually consist of data and metadata.[28] On the one hand, the term data refers to the electronic representation of information in any form.[29] The notion "any form" is generally misleading. It is submitted, however, that information can be represented either manually or mechanically. However, this representation should, insofar as it amounts to a processing of information or data, meet the principles regarding the protection of personal information.[30] The requirements relate to processing limitations, purpose specifications, further processing limitations, information or data quality, openness, security safeguards, individual participation and accountability.[31] On the other hand, metadata encompasses data or information which describes the structure of the data within a database.[32]

It is furthermore accepted that particular databases are generally more critical or more important than others. The criticality of these databases therefore makes them susceptible or vulnerable to outside attacks. Examples of outside attacks are computer hacking[33], pharming or spoofing[34], phishing[35] and cyber-terrorism. Outside

---

26 Botma *et al Navigating Information Literacy* 84. For further interesting reading, see Brown, Bryan and Conley 1999 http://bit.ly/16rT8h8 2-6.

27 Botma *et al Navigating Information Literacy* 6.

28 Taylor *SQL for Dummies* 9.

29 See s 1 of the *ECT Act*.

30 See Chapter 3 of the *Protection of Personal Information Bill*, 1998.

31 Principle 1-8 of the *Protection of Personal Information Bill*, 1998.

32 Taylor *SQL for Dummies* 9.

33 Hacking is one of the techniques that are employed by criminals to compromise personal or sensitive information stored in a computer system or network. Hacking is actually an act of illegally breaking into other people's computer systems or networks for purposes of soliciting information or data that is stored or reserved in the systems or networks (see Taylor "Hacktivism" 61; McAfee Date unknown http://bit.ly/11d0cwJ).

34 Pharming or spoofing is performed by a "mechanical vandal that creates a fake site masquerading as that of a legitimate provider" in order to steal information or data from unsuspecting persons and/or disrupt operating businesses (see Kapoor *Computerised Banking* 16).

35 Various definitions of the crime of phishing diverge. The differences seems to be influenced by the ever-changing nature of contemporary forms of technologies. For example, Myers provides that phishing encompasses social engineering and/or technical attacks (see Myers "Introduction to Phishing" 1-2.) Such attacks are commonly orchestrated by the sending of electronic mails to a web user falsely claiming to be an established legitimate enterprise, in an attempt to scam the

attacks generally rely on nefarious techniques or attacks to weaken the integrity of these databases. Furthermore, outside attacks commonly inhibit the quality of databases and data.[36] Outside attacks can generally be classified as either passive or active attacks.[37] Passive attacks occur in cases where an e-system or network is infiltrated surreptitiously and without detection.[38] Active attacks take the form of altering or adapting an e-system or network.[39]

Critical databases are collections of critical data in an electronic form kept in a site from where the data may be accessed, reproduced or extracted.[40] In South Africa, critical data is that the protection of which is declared by the Minister[41] to be of importance to national security or the economic or social well-being of its citizens.[42] This includes data that is essential to the daily functioning of an information society.[43] Furthermore, critical databases include data the interruption or destruction of which could have widespread effects and consequently result in or generate grave consequences to an information society.[44] At a governmental level, an interruption or destruction of critical databases could hamper and/or delay the delivery of services.[45]

The critical nature of databases requires the taking of steps to preserve their integrity and quality. Their preservation is often guarded in ordered to alleviate the impact of outside attacks. The steps to preserve the integrity and quality of databases are discussed in the section below.

---

web user into surrendering private information that will be used for identity theft (see Granova and Eloff 2005 *Computer Fraud and Security* 6).

36 West "Preventing System Intrusions" 39.

37 West "Preventing System Intrusions" 39.

38 West "Preventing System Intrusions" 39.

39 West "Preventing System Intrusions" 39.

40 Section 1 of the *ECT Act*.

41 The relevant Minister is the Minister of Communications.

42 See s 1 of the *ECT Act.*

43 Milone 2002 *Business Lawyer* 383-384.

44 Von Solms "Critical Information Infrastructure Protection" 37.

45 Chapter 5, Part II, Principle A of Procl R1 in GG 21951 of 1 January 2001.

2.2 Protecting critical databases

In modern times, attacks or threats of attacks to critical databases have become more pervasive and widespread. It is argued that these attacks or threats existed long before the 9/11 attacks that occurred in the US.[46] For example, the attacks that are alleged in the Riggs case took place during September 1988. An accused (Riggs and another) devised a scheme in order to defraud a company (Bell South Telephone Company) that provides telephone services to numerous states in the US.[47] In this case a computer was used to gain unlawful access to the company's computer system and networks. When access was gained the accused downloaded a computer file that contained sensitive information. The information detailed the manner in which emergency calls by the police, fire brigade, ambulance and other municipal emergency services by were responded to.[48]

It is furthermore argued that the hacker attacks on various databases such as those of the Bank of America[49] and the state-owned oil company in Saudi Arabia[50] reveal that the threats posed by outside attacks to the integrity and quality of databases still exists. In particular, the US Industrial Control Systems Cyber Emergency Response Team Control Systems Program (ICS-CERT) details the gravity of these outside attacks.[51] For example, the ICS-CERT enunciates that a total of 198 attacks to some of the critical databases in the US were reported during 2011.[52] It is therefore submitted that the interconnectedness of modern societies can increase the mayhem that could be caused by outside attacks. An attack on a particular database could have adverse effects on other databases. In some cases, an attack on one country's database(s) could have pervasive consequences on the databases of other countries.

---

46 See in general *United States v Robert J Riggs* 739 FSupp 414 (North District of Illinois 1990); *United States v Morris* 928 F2N 504 (2nd Circuit Court 1991).

47 *United States v Robert J Riggs* 739 FSupp 414 (North District of Illinois 1990) 45-46.

48 *United States v Robert J Riggs* 739 FSupp 414 (North District of Illinois 1990) 45-46.

49 Francis 2012 http://abcn.ws/ZwFUJH; Fikle and Fikle and Rothacker 2012 http://reut.rs/179qwdK 2012.

50 Perlroth 2012 http://nyti.ms/13M0EWG.

51 ICS-CERT 2009-2011 http://1.usa.gov/16fCWxp.

52 ICS-CERT 2009-2011 http://1.usa.gov/16fCWxp.

A scrutiny of the protection paradigms of critical databases reveals that they are generally only as strong as their weakest elements.[53] Put differently, outside attacks will continue to take place as long as technologies continue to develop.[54] The OECD recognises this fact, which is why it developed an all-encompassing framework to alleviate the attacks to critical databases.[55] In the terminology of the OECD the measures are referred to as the structure to protect CIIs.

Section 3 below is divided into two parts. Part 3.1 discusses the OECD structure to protect CIIs. Part 3.2 reviews the South African approach to safeguarding CIIs.

3 Approaches to securing CIIs

3.1 The OECD approach

The OECD framework to protect CIIs has four essential components or elements,[56] namely prevention, detection, response and recovery. No particular order is necessarily followed in addressing each of these elements, but it is generally accepted that each one element builds on the others.[57] This paper therefore delves into the meaning and importance of these elements in relation to the safeguarding of CIIs.

3.1.1 Prevention

Various provisions of the Marsh Report[58] are essential to the element of prevention. For example, the Marsh Report states that "waiting for disaster (to happen) is a

53 Commission of the European Communities 2006 http://bit.ly/Z497fe.
54 Commission of the European Communities 2006 http://bit.ly/Z497fe.
55 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
56 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
57 Cukier 2005 http://bit.ly/179q6UO.
58 The Marsh Report is the product of the United States of America (the US) President's Commission on Critical Information Infrastructure Protection (President's Commission). The President's Commission was set up by the then US president (President Clinton) and Robert T Marsh was appointed as the chairman of the Commission. See Marsh 1997 http://bit.ly/Z4cWkx.

dangerous strategy."[59] The real-time prevention of attacks on the CIIs must occur. This immediate security should be aimed at preventing future attacks, as well as thwarting present attacks.[60] The OECD concurred, and therefore adopted a range of recommendations made in the Marsh Report. For example, the OECD promotes the adoption of clear and objective policies related to the prevention of attacks (cyber-attacks) on CIIs.[61] These policies are designed to encourage co-operation by or between countries, and by or between countries and the private sector.[62] The co-operation must therefore be at the strategy, policy and operational levels.[63] This collaboration must facilitate the initiating of a practice that enables the apportioning of skills to ascertain generic vulnerabilities of and risks to CIIs. Secondly, the policies must support the aspiration to dispense knowledge and experience regarding the development of policies and practices to secure CIIs.[64]

The OECD further acknowledges that the creation of awareness of the various risks to CIIs is one of the "lines of defence" for any CII protection paradigm.[65] Awareness extends to ascertaining the degree and significance of the risks to CIIs.[66] The rationale for the creation of the awareness is to motivate the design of CII security mechanisms that address and/or respond to the imminent risks.[67]

3.1.2 Detection

The OECD recommends that a country's or an organisation's overall CII protection framework should encompass measures to identify and classify the risks of attacks to CIIs.[68] This identification and classification ought to extend to CIIs that are most

59 Marsh 1997 http://bit.ly/Z4cWkx 6.
60 Marsh 1997 http://bit.ly/Z4cWkx 6.
61 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
62 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
63 OECD 2008 http://bit.ly/11cZ1xh.
64 OECD 2002 http://bit.ly/14Ar0tG.
65 See G8 2003 http://bit.ly/128xThV.
66 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
67 A study regarding corresponding (or balanced) CIIs is made in para 3 (the risk-based approach) below.
68 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.

vulnerable to cyber-attacks.[69] Emergency warning systems or networks such as intrusion detection systems (IDSs) play a significant role in the identification and classification of attacks on CIIs. IDSs must operate as a second line of defence,[70] following prevention.[71] Furthermore, IDSs must encompass, amongst other things, computer software that "automates the intrusion detection process".[72]

IDSs must assist in an incident-monitoring process.[73] Such a process would identify and classify the threat or risk and analyse the degree and extent of the risk(s) posed to a system or network.[74] Once this has been done, information related to the risk(s) should be shared and exchanged, nationally or internationally, as a means of establishing a co-operative framework with the purpose of securing CIIs.[75]

3.1.3 Response

Timely or immediate and co-operative response to attacks on CIIs is indispensable to the process of securing CIIs.[76] Procedures and measures to facilitate this rapid and effective collaboration should be established. Such partnerships can be achieved by setting up malicious packet alerts (MPAs), for example, which are warning alerts[77] that generally observe and report attacks on CIIs.[78] The procedures and measures taken in this regard should support, amongst other things, the establishment of computer emergence response teams (CERTs) or computer security incident response teams (CSIRTs).[79] These CERTs or CSIRTs must be composed of trained professionals[80] who should be able to investigate and provide information on present

69 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
70 See Bolzoni and Etalle "Approaches in Anomaly-based Network Intrusion Detection Systems" 1-2.
71 Scarfone and Mell 2007 http://1.usa.gov/ZwIkbb.
72 Scarfone and Mell 2007 http://1.usa.gov/ZwIkbb.
73 Scarfone and Mell 2007 http://1.usa.gov/ZwIkbb.
74 Baocun and Fei "Information Warfare" 328; Brazzoli "Future Prospects of Information Warfare" 219.
75 OECD 2002 http://bit.ly/14Ar0tG.
76 OECD 2002 http://bit.ly/14Ar0tG.
77 Carcano *et al* "State-based Network Intrusion Detection Systems" 139.
78 Carcano *et al* "State-based Network Intrusion Detection Systems" 139.
79 Nickolov 2005 *Information & Security* 109.
80 Rittinghouse and Hancock *Cybersecurity Operations* 327.

and future attacks or risks to CIIs.[81] Consequently, the CERTs or CSIRTs must be structured in a manner that allows them to assist in the monitoring, warning and alerting of attacks, and must be able to carry out CII recovery measures.[82]

The efficiency and useful functioning of the CERTs and/or CSIRTs must therefore be continuously evaluated. Put differently, the CERTs or CSIRTs must be repeatedly tested and assessed to ensure their proper operation. This testing and assessment must be aimed at guaranteeing that these CERTs or CSIRTs remain secure and stable in emergency situations.[83]

3.1.4 Recovery

The OECD regards incident recovery measures (IRMs) as essential in alleviating the impact of attacks on CIIs.[84] IRMs generally bring operational and functional stability to CIIs. Furthermore, IRMs provide measures related to the recovery processes and progression or improvement of conditions after the attack.[85] For this reason, IRMs ease and accelerate the process of recovering information or data lost after attacks to CIIs.[86] It is important, however, that the structure of IRMs should not be such as to interrupt the appropriate functioning of CIIs.[87]

Incident recovery measures can establish the extent of the attacks to CIIs. The rationale for such investigation is to consider existing attack(s) trends. Such scrutiny may lead to the ability to forecast future threats to CIIs.

81 Rittinghouse and Hancock *Cybersecurity Operations* 327.
82 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
83 Principles V and VIII of the G8 Principles (G8 2003 http://bit.ly/128xThV).
84 Principle X of the G8 Principles (G8 2003 http://bit.ly/128xThV).
85 Chandrasekhar "Living With Disasters" 195.
86 Anderson *et al* 2005 *IEEE Transactions on Power Systems* 1924.
87 Anderson *Information Infrastructure* 51-52.

3.2 The South African approach

3.2.1 Background to the study

CII security in South Africa is needed in order to safeguard e-systems and networks from outside attacks. In particular, South Africa proposes that we should have a "vigilant and proactive approach" to the CII security structure.[88] Such an approach requires a constant, regular assessment and forecasting of attacks on CIIs.[89]

It is argued that the requirement for the regular assessment of attacks on CIIs in South Africa is analogous to the identification and verification procedure which is practised by *FICA*.[90] *FICA* requires certain institutions, that is, accountable institutions,[91] to undertake the identification and verification process before establishing a business relationship[92] or concluding a transaction between parties[93] or a single transaction[94] with other persons or institutions.[95] Such a process has to be recurrent and continuous.[96] The purpose of the process is twofold. Firstly, enables accountable institutions to detect any changes in the activities or behaviour

88 The South African Cybersecurity Policy 11 (GN 118 GG 32963 of 19 Feb 2010).

89 The South African Cybersecurity Policy 11 (GN 118 GG 32963 of 19 Feb 2010).

90 See s 21 *Financial Intelligence Centre Act* 38 of 2001 (hereinafter referred to as *FICA*).

91 Accountable institutions are those listed in Schedule 1 of *FICA*. Included in the list are attorneys, boards of executors or trust companies, estate agents, financial instruments traders, management companies, persons who carry on the business of banks, mutual banks, persons who carry on long-term insurance businesses, persons who carry on business in respect of which a gambling licence is issued, persons who carry on the business of dealing in foreign exchange, persons who carry on the business of lending money, persons who carry on the business of rendering investment advice or investment-broking services, persons who issue, sell or redeem travellers' cheques, money orders or similar instruments, Postbanks, members of the stock exchange, the Ithala Development Finance Corporation Limited, persons who have been approved or who fall within the category of persons approved by the Registrar of Financial Markets, and persons who carry on the business of a money remitter.

92 *FICA* defines a business relationship as an arrangement between two or more parties which is entered into for the purpose of concluding transactions on a regular basis (s 1 *FICA*).

93 A transaction is a transaction which is concluded by or between two or more parties in accordance with the type of business relationship carried out (s 1 *FICA*).

94 Section 1 *FICA* defines a single transaction as a transaction other than a transaction which is concluded in the course of a business relationship.

95 Sections 21(1) and (2) of *FICA*.

96 *Columbus Joint Venture v Absa Bank Ltd* 2002 1 All SA 105 (SCA); *Energy Measurements (Pty) Ltd v First National Bank of South Africa* 2000 2 All SA 396 (W); *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* 1992 1 All SA 411 (A).

of the person or people it has established business relationships with.[97] Secondly, it identifies any alterations or modifications in the pattern of concluding transactions or single transactions.[98] It is therefore inferred that the *FICA* approach to assessing transaction or single transactions on a continuous basis has shaped the framework that South Africa is adopting to evaluate CII protection measures.

An overview of the South African structure to safeguard CIIs is set out below. The section below describes in general terms the approach that South Africa is adopting to assess and forecast attacks on CIIs.

3.2.2 The Chapter IX structure

Chapter IX of the *ECT Act* provides and/or seeks to provide measures for the deterrence of attacks on CIIs. In particular, sections 53, 54 and 55 of the *ECT Act* grant the Minister extensive powers to design measures to avert cyber-attacks. For example, the Minister decides on the data that should be identified and classified as essential to the protection of the national security of South Africa.[99] The Minister furthermore sets out measures to ascertain and classify the data that are fundamental to the protection of the economic and social wellbeing of South African citizens.[100] Lastly, the Minister establishes procedures for the identification of such data.[101]

In other cases, the Minister prescribes rules for the registration and management of CIIs.[102] Firstly, the rules provide for the registration of the full names, address and contact details of the critical database administrator;[103] the location of CIIs or their

97 *LIoyds Bank Ltd v The Chartered Bank of India, Australia and China* 1928 All ER 285 297A-F.
98 *LIoyds Bank Ltd v The Chartered Bank of India, Australia and China* 1928 All ER 285 297A-F.
99 Section 53(a) *ECT Act*.
100 Section 53(a) *ECT Act*.
101 Section 53(b) *ECT Act*.
102 Sectionss 54 and 55 *ECT Act*.
103 A critical database administrator is a person who is responsible for the management and control of a critical database. See s 1 *ECT Act.*

component parts; and the general description of the information stored on CIIs.[104] A description of the information stored on CIIs must, however, exclude the actual contents of a CII.[105] The information that forms the basis of CIIs must be maintained by the Department[106] or any institution specified by the Minister for that purpose.[107] The Department or institution must therefore refuse to disclose the information, subject to certain exceptions.[108] More specifically, the information should be accessible only to the employees of the Department or institutions.[109] For purposes of the disclosure of critical information, the term "employees" excludes "general employees".[110] The employees refer to as being able to hold the information are those are responsible for the keeping of the register.[111]

Secondly, the rules regarding the management of CIIs relate, amongst other things, to the accessing, transferring and controlling of CIIs; infrastructural and procedural rules and requirements for securing the integrity of CIIs; procedures and technological methods to be used in storing and archiving CIIs; disaster recovery plans in the event of the loss or destruction of CIIs or their component parts, and any other matter required for the adequate protection, management and control of CIIs.[112]

Section 55(2) of the *ECT Act* furthermore introduces a procedure or mechanism for the management of other CIIs. These other CIIs include databases administered by public bodies. Section 55(2) states that such management should be performed in consultation with the members of the Cabinet affected by Chapter IX of the *ECT Act*. Examples of these members include, amongst others, the Minister of Defence, the Minister of Police and the Minister of State Security.

---

104 Section 54(2)(a)-(c) *ECT Act*. The recording of these particulars may, however, be waived at the Minister's discretion in terms of s 55(2)(a) and (b) *ECT Act*.

105 Section 54(2)(c) *ECT Act.*

106 In terms of the *ECT Act* this is the South African Department of Communications. See s 1 *ECT Act*.

107 Section 54(2) *ECT Act.*

108 Section 56(1) *ECT Act*. For an interesting study of the exceptions to the rule that information contained in the register should be kept secret, see s 56(2)(a)-(e) *ECT Act.*

109 Section 56(1) *ECT Act.*

110 Section 56(1) *ECT Act.*

111 Section 56(1) *ECT Act.*

112 Section 55(1)(a)-(f) *ECT Act.*

It is argued that an approach to secure CIIs functions adequately in an environment where a risk-based or sensitive framework is adopted. This risk-based framework is recognised *inter alia* by the OECD. More specifically, the OECD principles or guidelines contain provisions related to the conducting of a risk-assessment-based analysis.[113] The risk-assessment-based analysis assists in ascertaining the degree and extent of the risks to critical information security measures.[114] Section 4 below therefore reviews the risk-based theory. In addition, section 4 examines the approaches to the risk-assessment-based analysis which are adopted by the OECD and, to some extent, by South Africa. More specifically, Chapter IX of the ECT Act embodies the South African structure to protect critical databases. The Chapter IX structure to secure CIIs or databases is supported by certain provisions of the Draft Cybersecurity Policy of South Africa.[115]

4 The risk-based theory

4.1 The nature of the risk-based theory

The risk-based theory of regulation was developed recently. Other theories developed recently are, *inter alia,* the codes-based theory of regulation,[116] the institutionalist theory of regulation, the systems theory of regulation[117] and the "Good Regulator Theorem."[118] The risk-based theory of regulation is referred to in fields such as internal auditing as the risk management process.[119] The risk management process is normally associated with "precautionary logic",[120] which posits that the state should extend "freedom and security by intervening in ways

113 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
114 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.
115 See Procl R118 in GG 32962 of 19 February 2010 (hereinafter referred to as the Draft Cybersecurity Policy of South Africa).
116 The codes-based theory of regulation was developed by Lessig. See Lessig *Code and Other Laws of Cyberspace*; Lessig 1995 *Yale L J* 17-46.
117 The institutionalist and the systems theories of regulation were promoted by Morgan and Yeung. See in general, Morgan and Yeung *Law and Regulation* 53-75.
118 The "Good Regulator Theorem" is favoured by Conant and Ashby. See Conant and Ashby 1970 *Int J Syst Sci* 89.
119 Spencer *Internal Auditing Handbook* 175.
120 Bowling, Marks and Murphy "Crime Control Technologies" 52.

that pre-empt wrongdoing."[121] Accordingly, risk management is a forceful process that seeks to:

Identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation's objectives. [122]

The risk management framework depends and/or relies on establishing the source or sources of the risks and/or threats.[123] It extends to identifying *inter alia* the type of risks at issue, and asking if the risks could affect a specific event or process.[124] Furthermore, risk management enables organisations and sometimes individuals to direct or allocate organisational and individual resources to high-risk areas.[125]

The notion "risk" derives from the Italian verb *risicare*,[126] which means "to dare".[127] The verb *risicare* is used in the Italian proverb *chi non risica, non rosica* which translates in English into "nothing ventured, nothing gained".[128] Some scholars believe that the idea of risk was seriously considered during the Italian Renaissance,[129] when the concept of risk was developed as mathematically astute gamblers sought to "unlock the mysteries of dice throwing".[130]

This paper submits that the structure of the risk-based theory is comparable to the risk management framework. For example, the risk-based theory discards a one-size-fits-all approach to regulation and accepts that a holistic and elastic regulatory framework is indispensable. This framework focuses on the number and degree of risks related to a particular event. It presupposes that certain facts or circumstances are unknown, and that the unknown facts should be evaluated by means of a risk-

121 Bowling, Marks and Murphy "Crime Control Technologies" 52.
122 Griffiths, O'Callaghan and Roach *Internal Relations* 251.
123 Somsen "Cloning Trojan Horses" 223.
124 Spencer *Internal Auditing Handbook* 179.
125 For an interesting study on the "fundamentals of the framework for risk criteria", see Vrijling *et al* 2004 *Journal of Risk Research* 570-574.
126 Deuchars *International Political Economy* 7.
127 Deuchars *International Political Economy* 7.
128 Griffiths, O'Callaghan and Roach *Internal Relations* 251.
129 Griffiths, O'Callaghan and Roach *Internal Relations* 251.
130 Griffiths, O'Callaghan and Roach *Internal Relations* 251.

assessment-appraisal process[131] which encompasses, *inter alia,* risk identification, risk classification and risk analysis.[132] The risk-assessment-appraisal process accordingly is opposed to the idea of relying on "intuition and guesswork" as the basis for assessing risks.[133]

Lastly, the risk-based theory presupposes that a fitting method of regulating facts or circumstances is to investigate and scrutinise those facts or circumstances.[134] This scrutiny is commonly made by applying measures (preventative or otherwise) notwithstanding the absence of facts to determine the outcome.[135] The foundation for such a scrutiny is to strike equilibrium between the taking of the measures and the identification of the imminent risks.[136] In other words, a balance should be maintained or sought to be maintained between the number and extent of the measures and the number and degree of the risks. Therefore, in cases where the risks are high, stricter measures to prevent or deter the risks should be applied.

The OECD and to some extent, the South African structures to safeguard CIIs reveal that a risk-assessment-based analysis is indispensable to the general scheme to protect CIIs. The sections below, namely sections 4.2 and 4.3, will therefore examine both the OECD and the South African approaches to the risk-assessment-based analysis.

4.2 The OECD approach to the risk-assessment-based analysis

The OECD encourages awareness of the risks to CII security.[137] This awareness is, according to the OECD, to be sustained in circumstances where a risk-assessment-based analysis is carried out. The OECD therefore demands that such an analysis should be broad-based. In other words, the risk-assessment-based analysis must

131 Afzal, Rohaniand and Roshana 2011 *ISBEIA* 320.
132 Afzal, Rohaniand and Roshana 2011 *ISBEIA* 320.
133 See Macaulay 2009 http://bit.ly/14AqrQM.
134 Spedding *Due Diligence* 40.
135 Spedding *Due Diligence* 40.
136 Spedding *Due Diligence* 40.
137 OECD 2008 http://bit.ly/11cZ1xh; OECD 2002 http://bit.ly/14Ar0tG.

encompass the relevant internal and external factors that have an impact on CIIs.[138] These factors include, amongst others, technology, physical and human factors, policies, and third-party services with security implications.[139] Furthermore, the risk-assessment-based analysis is required to include information components supporting CIIs; information infrastructures supporting the essential components of a nation's business; and information infrastructures indispensable to a country's national economy.[140]

The awareness of the risks to CIIs must therefore encourage the developing of preventive measures.[141] Furthermore, the requisite awareness must promote the undertaking of steps to enhance the security of information systems and networks.[142] Put differently, the risk-assessment-based analysis must assist in determining the levels of risks and must also aid in the selection of suitable risk management controls.[143] An ongoing or periodic review structure must therefore be developed. This structure must assist in re-examining and revaluating the measures developed to safeguard CIIs.[144] The review procedures must be structured in a manner that adequately addresses the risks or threats associated with the constant developments in modern ICTs.

4.3 The South African approach to the risk-assessment-based analysis

The South African structure to secure CIIs seems to diverge from that which is championed by the OECD. For example, no clear and/or ascertainable measures are set out by South Africa regarding the risk-assessment-based analysis. South Africa, it further appears, favours and/or adopts a generalised view in respect of the risk-assessment-based analysis. This paper, on the contrary, argues that a risk-assessment-based analysis should be a necessary component of any model designed

138 OECD 2008 http://bit.ly/11cZ1xh.
139 OECD 2002 http://bit.ly/14Ar0tG.
140 OECD 2002 http://bit.ly/14Ar0tG.
141 OECD 2002 http://bit.ly/14Ar0tG.
142 OECD 2002 http://bit.ly/14Ar0tG.
143 OECD 2002 http://bit.ly/14Ar0tG.
144 OECD 2008 http://bit.ly/11cZ1xh.

to protect CIIs in the provisions of the South African National Cybersecurity Policy. For example, South Africa provides that relevant tools, policies, security concepts and safeguards, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment, organisations and user assets should be collected. Consequently, policies and procedures facilitating such collection should be developed. The framework and ambit of the abovementioned policies and procedures should, however, be to secure the South African cyberspace structure. This structure should include physical or non-physical terrains which are created or composed of computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users.[145]

Notwithstanding the abovementioned, this paper argues that there are a number of barriers to South Africa's progress towards establishing a risk-assessment-based analysis as part of its scheme to safeguard CIIs. Firstly, the fact that the Cybersecurity Policy is still in its drafting phase obstructs South Africa's overall agenda to curb cybercrime. Secondly, the general provisions contained in the Cybersecurity Policy could be thought to support the adoption of a one-size-fits-all framework. Consequently, South Africans could be falsely persuaded that CIIs could be protected by merely ticking boxes.[146]

5 Conclusion

South Africa has made great strides to protect CIIs. The South African approach is one that encourages the adoption of a model which requires the regular assessment of attacks or threats of attacks to its CIIs. Accordingly, it is argued that this approach is a representation of the identification and verification procedure that is found in *FICA*. Nevertheless, it is argued that the South African approach is rule-based as opposed to risk-based. Put differently, it implicitly promotes an inflexible and incongruous culture of protecting critical databases. For example, it is submitted

145 The South African National Cybersecurity Policy (GN 118 GG 32963 of 19 Feb 2010).

146 The proposal for a one-size-fits-all approach to a process to identify and classify CIIs is implicitly advocated by Von Solms. See Von Solms "Securing the Internet" 2-3.

that the evolution of attacks or threats of attacks to CIIs is linked to developments in contemporary technologies. Accordingly, the emergence of new technology brings about or can bring about the emergence of new attacks or threats of attacks on CIIs. Fixed rules or regulatory frameworks will fail to deal adequately with these regular developments. It is furthermore argued that South Africa should adopt a generalised approach in regulating the risks posed or potentially posed by outside attacks to CIIs. For example, no specific provisions can be found that to regulate the aforementioned. Only an inference can be drawn from various provisions that are contained in the Draft Cybersecurity Policy. Consequently, South Africa fails to follow the coordinated approach found in many instruments of the OECD.

Therefore, it is recommended that South Africa should adopt the four essential principles or elements that form the basis of the OECD's structure to safeguard CIIs. The adoption of these OECD principles would enable South Africa to undertake a process to forecast, identify, assess, monitor, and recover from, attacks or threats of attacks to its CIIs. Furthermore, South Africa should accept that risks of attacks differ in terms of their degree and size. Consequently, a method to forecast, identify, assess, monitor and recover from, risks of attacks will generally diverge according to their pervasive or critical nature. It is furthermore recommended that regulations, ordinances or guidelines should be suited to the nature of the threats as described above. The aim should be to alleviate the impact of new attacks or threats of attacks to CIIs, owing to the constant developments in technologies. The regulations, ordinances or guidelines should generally promote a culture of protecting CIIs which examines the foreseen and unforeseen, or foreseeable and unforeseeable risks of attacks to CIIs.

Bibliography

Afzal, Rohaniand and Roshana 2011 *ISBEIA*

Afzal AZ, Rohaniand EI and Roshana T "Contractor's strategic approaches to risk assessment techniques at project planning stage" 2011 *ISBEIA* 318-323

Anderson *et al* 2005 *IEEE Transactions on Power Systems*

Anderson G *et al* "Causes of the 2003 Major Grid Blackout in North America and Europe, and Recommended Means to Improve System Dynamic Performance" 2005 *IEEE Transactions on Power Systems* 1922-1928

Anderson *Information Infrastructure*

Anderson RH *Securing the US Defense Information Infrastructure: A Proposed Approach* (RAND Washington 1999)

Baocun and Fei "Information Warfare"

Baocun W and Fei L "Information Warfare" in Pillsbury M (ed) *Chinese View of Future Warfare* (National Defence University Washington 1997) 327-342

Bendisch *et al* "Towards a European Agenda"

Bendisch U *et al* "Towards a European Agenda for CIIP - Results from the CI^2 RCO Project" in Lopez J and Hämmerli BM (eds) *CRITIS 2007: Second International Workshop on Critical Information Infrastructures Security* (Springer Berlin 2008) 1-12

Bolzoni and Etalle "Approaches in Anomaly-based Network Intrusion Detection Systems"

Bolzoni D and Etalle S "Approaches in Anomaly-based Network Intrusion Detection Systems" in Di Pietro R and Mancini LV (eds) *Advances in Information Security: Intrusion Detection Systems* (Springer Verlag London 2008) 1-15

Botma *et al Navigating Information Literacy*

Botma T *et al Navigating Information Literacy: Your Information Society Survival Toolkit* 2nd ed (Pearson Cape Town 2008)

Bowling, Marks and Murphy "Crime Control Technologies"

Bowling B, Marks A and Murphy C "Crime Control Technologies – Towards an Analytical Framework and Research Agenda" in Brownword R and Yeung K (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Oxford 2008) 51-78

Brazzoli "Future Prospects of Information Warfare"

Brazzoli MS "Future Prospects of Information Warfare and Particularly Psychological Operations" in Le Roux L (ed) *South African Army Vision 2020*: *Security Challenges Shaping the Future South African Army* (Institute for Security Studies Pretoria 2007) 217-232

Carcano *et al* "State-based Network Intrusion Detection Systems"

Carcano A *et al* "State-based Network Intrusion Detection Systems for SCADA Protocols - A Proof of Concept" in Rome E and Bloomfield B (eds) *Critical Information Infrastructures Security: CRITIS 2009* (Springer Verlag Berlin 2010) 138-150

Chandrasekhar "Living with Disasters"

Chandrasekhar D "Living with Disasters – A Planning Approach to Critical Incidents" in Schwester RW (ed) *Handbook of Critical Incident Analysis* (Sharpe New York 2012) 186-200

Conant and Ashby 1970 *Int J Syst Sci*

Conant RC and Ashby WR "Every Good Regulator of a System Must be a Model of That System" 1970 *Int J Syst Sci* 89-97

Deuchars *International Political Economy*

Deuchars R *The International Political Economy of Risk: Rationalism, Calculation and Power* (Ashgate Aldershot 2004)

Durrani *Information and Liberation*

Durrani S *Information and Liberation: Writings on the Politics of Information and Librarianship* (Library Justice Duluth 2008)

Granova and Eloff 2005 *Computer Fraud and Security*

Granova and Eloff "A Legal Overview of Phishing" 2005 *Computer Fraud and Security* 6-11

Griffiths, O'Callaghan and Roach *Internal Relations*

Griffiths M, O'Callaghan T and Roach SC *Internal Relations: The Key Concepts* 2nd ed (Routledge London 2008)

Kapoor *Computerised Banking*

Kapoor N *Computerised Banking System in India* (Sublime Jaipur 2008)

Katyal 2001 *U Pa L Rev*

Katyal NK "Criminal Law in Cyberspace" 2001 *U Pa L Rev* 1003-1114

Lessig 1995 *Yale L J*

Lessig L "The Path of Cyberlaw" 1995 *Yale L J* 1743-1755

Lessig *Code and Other Laws of Cyberspace*

Lessig L *Code and Other Laws of Cyberspace* (Basic Books New York 1999)

Milone 2002 *Business Lawyer*

Milone MG "Hacktivism - Securing the National Infrastructure" 2002 *Business Lawyer* 383-413

Morgan and Yeung *Law and Regulation*

Morgan B and Yeung K *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press Cambridge 2007)

Myers "Introduction to Phishing"

Myers S "Introduction to Phishing" in Jakobsson M and Myers S (eds) *Phishing and Counter-Measures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley Hoboken 2007) 1-30

Nickolov 2005 *Information & Security*

Nickolov E "Critical Information Infrastructure Protection - Analysis, Evaluation and Expectations" 2005 *Information & Security* 105-119

Okhravi *et al* 2012 *IJCIP*

Okhravi H *et al* "Creating a Cyber Moving Target for Critical Infrastructure Applications Using Platform Diversity" 2012 *IJCIP* 30-39

Rittinghouse and Hancock *Cybersecurity Operations*

Rittinghouse JW and Hancock WM *Cybersecurity Operations Handbook* (Elsevier Amsterdam 2003)

Sieber "Emergence of Information Law"

Sieber U "The Emergence of Information Law - Object and Characteristics of a New Legal Order" in Lederman E and Shapira R (eds) *Law, Information and Information Technology* (Kluwer The Hague 2001) 1-30

Somsen "Cloning Trojan Horses"

Somsen H "Cloning Trojan Horses – Precautionary Regulation of Reproductive Technologies" in Brownword R and Yeung K (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Oxford 2008) 221-242

Spedding *Due Diligence*

Spedding LS *Due Diligence and Corporate Governance* (LexisNexis Coydon 2004)

Spencer *Internal Auditing Handbook*

Spencer PKH *The Internal Auditing Handbook* 3rd ed (John Wiley Chichester 2010)

Taylor *SQL for Dummies*

Taylor AG *SQL for Dummies* 7th ed (Wiley Hoboken 2010)

Taylor "Hacktivism"

Taylor PA "Hacktivism - In Search of Lost Ethics?" in Wall D (ed) *Crime and the Internet* (Routledge New York 2001)

Van Niekerk and Maharaj 2011 *South African Journal of Military Studies*

Van Niekerk B and Maharaj MS "Relevance of Information Warfare Models to Critical Infrastructure Protection" 2011 *South African Journal of Military Studies* 52-75

Von Solms "Critical Information Infrastructure Protection"

Von Solms B "Critical Information Infrastructure Protection – Essential During War Times, or Peace Times or Both?" in Phahlamohlaka J *et al* (eds) *IFIP TC9 Proceedings on ICT Uses in Warfare and the Safeguarding of Peace* (CSIR Pretoria 2008) 36-40

Von Solms "Securing the Internet"

Von Solms B "Securing the Internet - Fact or Fiction?" in Camenisch J, Kisimov V and Dubovitsknya M (eds) *Open Research Problems in Network Security* (Springer Verlag Heidelberg 2011) 1-8

Vrijling *et al* 2004 *Journal of Risk Research*

Vrijling JK *et al* "A Framework for Risk Criteria for Critical Infrastructures – Fundamentals and Case Studies in Netherlands" 2004 *Journal of Risk Research* 569-579

Webster *Theories*

Webster F *Theories of the Information Society* (Routledge London 2006)

West "Preventing System Intrusions"

West M "Preventing System Intrusions" in Vacca JR (ed) *Computer and Information Security Handbook* (Morgan Kaufmann Amsterdam 2009) 39-51

Register of cases

Columbus Joint Venture v Absa Bank Ltd 2002 1 All SA 105 (SCA)

Energy Measurements (Pty) Ltd v First National Bank of South Africa 2000 2 All SA 396 (W)

Indac Electronics (Pty) Ltd v Volkskas Bank Ltd 1992 1 All SA 411 (A)

LIoyds Bank Ltd v The Chartered Bank of India, Australia and China 1928 All ER Rep 285

United States v Morris 928 F2N 504 (2nd Circuit Court 1991)

United States v Robert J Riggs 739 FSupp 414 (North District of Illinois 1990)

Register of legislation

Computer Fraud and Abuse Act, 1986

Cyber Security Enhancement Act, 2002

Cyber Security Research and Development Act, 2002

Defence Act 42 of 2002

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications Security Pty (Ltd) Act 68 of 2002

Financial Intelligence Centre Act 38 of 2001

National Key Points Act 102 of 1980

National Strategic Intelligence Act 39 of 1994

Protection of Personal Information Bill, 1998

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercepting and Obstructing Terrorism Act, 2001

Register of government publications

GN 118 GG 32963 of 19 February 2010

Procl R1 in GG 21951 of 1 January 2001

Procl R118 in GG 32962 of 19 February 2010

Register of international conventions

Council of Europe's Convention on Cybercrime (2001)

Council of the European Union Framework Decision on Attacks against Information Systems (2005)

Register of internet sources

Brown, Bryan and Conley 1999 http://bit.ly/16rT8h8

Brown, Bryan and Conley "Database Protection in a Digital World" 1999 *Richmond Journal of Law and Technology* http://bit.ly/16rT8h8 [date of use 13 Jul 2012]

Commission of the European Communities 2006 http://bit.ly/Z497fe

Commission of the European Communities 2006 *Proposal for a Directive of the of the Council Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection* http://bit.ly/Z497fe [date of use 13 Jul 2012]

Council of the European Union and Commission of the European Communities 2000 http://bit.ly/YZQlMX

Council of the European Union and Commission of the European Communities 2000 *E-Europe 2002 – An Information Society for All* http://bit.ly/YZQlMX [date of use 13 Jan 2012]

Cukier 2005 http://bit.ly/179q6UO

Cukier K 2005 *Critical Information Infrastructure Protection – Ensuring (and Insuring?) Critical Information Infrastructure Protection* http://bit.ly/179q6UO [date of use 13 May 2012]

Denning 2000 http://bit.ly/16rUw3i

Denning DE 2000 *Cyberterrorism Testimony before the Special Oversight Panel of Terrorism* http://bit.ly/16rUw3i [date of use 14 Jan 2012]

Fikle and Rothacker 2012 http://reut.rs/179qwdK

Fikle J and Rothacker R 2012 *Iranian Hackers Target Bank of America, JPMorgan, Citi* http://reut.rs/179qwdK [date of use 12 Nov 2012]

Francis 2012 http://abcn.ws/ZwFUJH

Francis E 2012 *Hackers, Possibly from Middle East, Block US Banks' Websites* http://abcn.ws/ZwFUJH [date of use 12 Nov 2012]

G8 2003 http://bit.ly/128xThV

G8 Justice and Interior Ministers 2003 *G8 Principles for Protecting Critical Information Infrastructures* http://bit.ly/128xThV [date of use 15 Jul 2012]

ICS-CERT 2009-2011 http://1.usa.gov/16fCWxp

ICS-CERT 2009-2011 *ICS-CERT Incidence Response Summary Report* http://1.usa.gov/16fCWxp [date of use 13 Oct 2012]

Macaulay 2009 http://bit.ly/14AqrQM

Macaulay T 2009 *US Critical Infrastructure Interdependency Wheel (CIIW) – Executive Summary* http://bit.ly/14AqrQM [date of use 13 Jun 2012]

Marsh 1997 http://bit.ly/Z4cWkx

Marsh RT 1997 *Critical Foundations – Protecting America's Infrastructures* http://bit.ly/Z4cWkx [date of use 13 Mar 2012]

McAfee Date unknown http://bit.ly/11d0cwJ

McAfee Date unknown *White Paper on Identity Theft* http://bit.ly/11d0cwJ [date of use 11 Jul 2011]

OECD 2002 http://bit.ly/14Ar0tG

OECD 2002 *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* http://bit.ly/14Ar0tG [date of use 18 Mar 2012]

OECD 2008 http://bit.ly/11cZ1xh

OECD 2008 *Recommendations of the Council on the Protection of Critical Information Infrastructures* http://bit.ly/11cZ1xh [date of use 16 Mar 2012]

Perlroth 2012 http://nyti.ms/13M0EWG

Perlroth N 2012 *Cyberattack on Saudi Firm, US Sees Iran Firing Back* http://nyti.ms/13M0EWG [date of use 12 Nov 2012]

Scarfone and Mell 2007 http://1.usa.gov/ZwIkbb

Scarfone K and Mell P 2007 *Guide to Intrusion Detection and Prevention Systems*: *Recommendations of the National Institute of Standards and Technology* http://1.usa.gov/ZwIkbb [date of use 12 May 2012]

US-Canada Power System Outage Task Force 2004 http://1.usa.gov/10t19NH

US-Canada Power System Outage Task Force 2004 *Final Report on the August 14 2003 Blackout in the United States and Canada – Causes and Recommendations* http://1.usa.gov/10t19NH [date of use 11 Nov 2012]

US Department of Energy 2012 http://1.usa.gov/XmvVwl

US Department of Energy 2012 *Special Report – Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex* http://1.usa.gov/XmvVwl [date of use 14 Nov 2012]

VandenBrink 2011 http://bit.ly/Yr6ok9

VandenBrink R 2011 *8 Years Since the Eastern Seaboard Blackout – Has It Been Long?* http://bit.ly/Yr6ok9 [date of use 6 Oct 2012]

List of abbreviations

CERTs	Computer Emergence Response Teams
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CSIRTs	Computer Security Incidence Response Teams
HEUMF	Highly Enriched Uranium Materials Facility
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
IJCIP	International Journal of Critical Infrastructure Protection
Int J Syst Sci	International Journal of Systems Science
IRMs	Incidence Recovery Measures
ISBEIA	IEEE Symposium on Business, Engineering and Industrial Applications
MPAs	Malicious Packet Alerts
OECD	Organisation for Economic Co-operation and Development
Richmond J Law	Richmond Journal of Law and Technology

Technol	
UN	United Nations
U Pa L Rev	University of Pennsylvania Law Review
Yale L J	Yale Law Journal

PROTECTING CRITICAL DATABASES – TOWARDS A RISK-BASED ASSESSMENT OF CRITICAL INFORMATION INFRASTRUCTURES (CIIS) IN SOUTH AFRICA

MN Njotini*

SUMMARY

South Africa has made great strides towards protecting critical information infrastructures (CIIs). For example, South Africa recognises the significance of safeguarding places or areas that are essential to the national security of South Africa or the economic and social well-being of South African citizens. For this reason South Africa has established mechanisms to assist in preserving the integrity and security of CIIs. The measures provide *inter alia* for the identification of CIIs; the registration of the full names, address and contact details of the CII administrators (the persons who manage CIIs); the identification of the location(s) of CIIs or their component parts; and the outlining of the general descriptions of information or data stored in CIIs.

It is argued that the measures to protect CIIs in South Africa are inadequate. In particular, the measures rely on a one-size-fits-all approach to identify and classify CIIs. For this reason the South African measures are likely to lead to the adoption of a paradigm that considers every infrastructure, data or database, regardless of its significance or importance, to be key or critical.

KEYWORDS: Critical databases; critical information infrastructures; national security; social and economic well-being

* Mzukisi N Njotini. LLB (Vista), LLM (*cum laude*) Information Technology Law, (UNISA), LLD Candidate, (UNISA). Senior Lecturer, Department of Jurisprudence, College of Law. UNISA, South Africa. Email: njotim@unisa.ac.za.