Name: Dumisani Gumbi

Student Number: GMBDUM002

Qualification Registered for: LLM Degree in Commercial Law

Dissertation Title:

'Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom'.

Supervisor's name: Professor Caroline Ncube

Word count: 24 500

Declaration

Research dissertation presented for the approval of Senate in fulfillment of part of the requirements for the Masters of Law (LLM) Degree in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of Masters of Law (LLM) Degree dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

Signed by candidate

19/02/2018

Mr. Dumisani Gumbi

Date

GMBDUM002

Keywords

Breach, broadband, board of directors, computer crime, conventions, cyber-attack, cybercrime, cyber terrorism, cyber espionage, cybersecurity, cyber warfare, cyber risk management, cyber liability, cyber insurance, common law, critical information infrastructure, directors, fiduciary duty, internet access, illegal access, internet crime, legislation, jurisdiction, policy, personal information, Companies Act, Cybercrimes and Cybersecurity related matters Bill.

Acknowledgments

I would like to acknowledge and appreciate the supervision and guidance of Professor Caroline Ncube, without whom this study would not have seen the light of day. Thank you also to my sponsors, Parliament of South Africa and the Sanlam Group for the financial backing and support needed to undertake and complete these studies. To my manager and coach, Johan Marnewick, I am so grateful for your teachings and mentorship. Thank you to all my family and friends for being relentless cheerleaders, I hope to have done you proud.

Lastly, to Busisiwe and Rorisang-Morena Gumbi, thank you for bearing with me throughout this journey and for the constant reassurance and understanding. This is the product of you unwavering love, prayers, and sacrifices.

Phakama Gumbi!

Nkabanhle,

Luvun’a baliwayo,

Skhende,

Jele,

Ngubo yengwe.

Somkhanda, wena owakhanda amadoda,

Wena ka-Mathumb'ayiphanyeke,

Ntongande, Mdakane,

Mehl'enkomo, Ntini,

Nozingelayo,

Wena kaNgoni,

Mlotshwa!

Ndandayi,

Somkhanda kanomo,

Malila ngomkhonto abanye belila ngezinyembezi,

Siguguda senyathi,

Wena kaKhokhozela njengeQhinakazi,

Msimbithi kawuwelwa.

ABSTRACT

As broadband infrastructure investments in developing nations intensify and barriers to accessing the internet diminish, the more they increasingly become the quintessential destination for cybercrime. For their lax cyber laws and general cybercrime illiteracy, developing nations such as South Africa, Kenya, and India have become the destination of choice for cybercriminal enterprises.

The focus of this dissertation is to comparatively analyse South Africa's ICT regulatory framework against those of developing and developed nations and to determine its effectiveness in addressing the threat posed by cybercrime. This dissertation hopes to contribute towards establishing a greater understanding and appreciation of the scourge of cybercrime by studying the frameworks, structures, and arrangements, installed to safeguard against cybercrime in developing nations, namely Kenya and India, and developed nations, namely the United States and the United Kingdom.

Some of the key challenges identified in the dissertation, arising from the analysis of South Africa's cyber laws and policy framework, point to legislation that is out of date and in desperate need of revision; a lack of definitional clarity for cybercrime-related terminology; jurisdiction limitations for international cybercrimes investigations, no harmonisation with international laws, standards, and a poor record of implementing strategy and policies.

The dissertation concludes that the battle against cybercrime cannot be won without first understanding what cybercrime is. Developing a common understanding of cybercrime and related terminology, the implementation of the necessary Information and Communication Technology (ICT) strategies, policies, and regulatory frameworks, are thus recommended. Concluding international cooperation and mutual assistance agreements to assist with transnational cybercrime investigations and prosecutions is paramount. Establishing cross-sector, intra-ministerial, public-private, and multinational partnerships is also vital to managing the threat of cybecrime. Lastly, this dissertation recommends the development of dedicated cybersecurity and cybercrime mechanisms for the prosecution and safeguarding of the nation's critical information infrastructure, the mission critical

information of corporates and the personal information of citizens against cybercrime.

1. INTRODUCTION

1.1 Purpose of the research

The purpose of this work is to establish an understanding of the world of cybercrime and the threat it poses to citizens, corporations, and nation states. This dissertation examines the definition of cybercrime and associated, distinct terminology commonly used with it or in relation to it. It also looks at the cybercrime system and analyses the role players concerned, their motives, and their primary targets. The legislation, policies, and information communications and technology (ICT) regulatory frameworks, especially formulated to address the threat of cybercrime in developing nations (Kenya and India) and developed nations (the United States and the United Kingdom), are comparatively analysed throughout this dissertation and used to determine South Africa's readiness to combat and safeguard against cybercrime.

1.2 Problem Statement and Research question

The chosen countries that form the basis of the comparative analysis have legal systems that mainly consist of combinations of English law, common law, and constitutional law. These laws apply to traditional crimes such as harassment, assault, theft, and fraud. When applied to technology-enabled criminal offences, these traditional laws fall short and are inadequate to address the myriad of evolving computer offences. This has led to the introduction of new legislation to keep abreast of technology-enabled crimes.

The objective of this dissertation is to comparatively analyse South Africa's ICT regulatory framework against those of developing and developed nations in order to determine whether it adequately addresses the risk of cybercrime. This analysis considers the definitions of the cybercrime lexicon, the duties of boards of directors to safeguard corporate mission-critical information, the safeguarding of national critical information infrastructure by nation states, and the reparation of the victims of cybercrime.

1.3 Chapter outline

This dissertation comprises six chapters, the first establishing the state and importance of provision of internet and broadband access within South Africa. The second chapter lays the foundation for the remainder of the dissertation and explores the various terms and definitions associated with cybercrime, namely: computer crime, cybersecurity, cyber espionage, cyber terrorism, and cyber warfare. Having established what cybercrime is not, the third chapter unpacks the concept of cybercrime further by exploring its classification, categories, various forms, perpetrators and how to quantify the cost of cybercrime. Chapter four considers the measures and arrangements in place to safeguard against cybercrime. The duty of a nation to protect its critical information infrastructure is explored, furthermore, the fiduciary duty of a board of directors to protect its corporations mission critical data against cyber risks is also discussed. Chapter five discusses some of the key challenges contributing to the current state of South Africa's ICT regulatory frameworks and level of preparedness to address the risk of cybercrime. The dissertation culminates in chapter six which considers some recommendations and possible ways forward.

1.4 Context: Internet and Enabling Technologies

To herald the dawn of the internet era, Thomas M Siebel equates the meteoric rise to prominence of the world wide web to a watershed moment for humankind and writes in *Cyber Rules: Strategies for excelling at e-business (*1999*):*

> [E]very so often an event occurs that is so startling in its economic implications that it may reasonably be considered a watershed in the way we do business. By "watershed" we mean an abrupt and irrevocable turning point, one that signals a shift in historical direction by obliterating an established set of business practices and replacing them with a new commercial paradigm.[1]

As predicted by Siebel, the invention and uptake of the internet was truly a digital watershed moment. It surpassed all expectations and revolutionised most industries.

---

[1] T Siebel and P House *Cyber Rules: Strategies for excelling at e-business* (1999) 1.

Many believe that the internet is the precursor that will usher in the fourth industrial revolution.

> 'The first industrial revolution used water and steam power to mechanize production. The *Second* used electric power to create mass production. The *Third* used electronics and information technology to automate production. Now a *Fourth Industrial Revolution* is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.'[2]

As with any of the great technological inventions, the internet may be used positively for the advancement of humanity or misused to bring about human and systemic loss and suffering. Gilbert Ryle[3] uses the term 'ghost in the machine' to dispute the notion of the mind being distinct from the body and that mental states are separable from physical states. In the same vein as argued by Ryle, there seems to be a ghost in the World Wide Web machine that has resulted in the internet becoming the *de-facto* primary domain for cybercrimes. Over time the internet has 'developed' an alternate, ulterior, and parallel personality in the form of the Dark Web[4] where encrypted, unlawful services and markets between organisations and individuals, can thrive under the cloak of secrecy and anonymity. When compared to older generation technologies like the railway, television, telephone, automobile, and airplane, the transformative role that the internet has played in fostering the exchange and flow of licit and illicit activities across countries is unprecedented. The invention of the internet has greatly profited criminal enterprises in much the same way modern weaponry has previously 'facilitated the implementation of large-scale mass murders.'[5]As cyberspace[6] is borderless, interconnected and filled with unsecured content from unsuspecting users, it has become an attractive platform for criminals to spread their criminal enterprises onto the internet.

---

[2] K Schwab 'The Fourth Industrial Revolution: what it means, how to respond*' World Economic Forum*, 2016, available at *http://bit.ly/1pBfye4*, accessed on 02 April 2017.
[3] G Ryle *The Concept of the Mind* (2002) 12.
[4] D Glance 'What is the Dark Web?*',* available at *http://theconversation.com/explainer-what-is-the-dark-web-46070*, 2017, accessed on 12 December 2017.
[5] N Kshetri *Cybercrime and Cybersecurity in the Global South* (2013) 5.
[6] Term coined by William Gibson in 1982 and applied to the internet by Howard Rheingold. Cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.

The continual evolution of technologies, particularly the internet, inadvertently, breeds newer forms of computer-enabled crimes, targets, and perpetrators. Newer and more specialised, computer-crime[7] laws are now needed to fend off the modern day criminals and the unconventional crimes they carry out over the internet and computing technologies.

Cybercriminal activity is said to be at its highest on the African continent, due to the limited understating of information technologies, the naivety and absolute trust in the safety of transacting on the internet owing largely to high levels of illiteracy. There are few suitable laws to effectively deal with cybercrimes in many of the countries on the Africa continent[8]. As a continent that is primarily focussed on overcoming the HIV/aids pandemic, poverty, rising unemployment, basic service delivery, crime, and eradicating corruption[9], developing cyberlaws receives secondary attention, thus leaving the continent susceptible to malicious cyber-criminal activities.

The current set of laws and policies dealing with cyber security in South Africa are inadequate and ineffective. They have not kept up with cyber-threats and suffer implementation challenges due to a lack of administrative will, poor coordination of inter-governmental mandates and ineffective implementation programmes.[10] It is not only the laws that will need to be modernised and brought in line with the advances of technology. Industries and professionals must also evolve if they are to survive and still benefit society.

1.5 State of Internet Access and the ICT Policy Framework in South Africa

Given the rate of contribution to South Africa's gross domestic product (GDP), access to the internet is a key stimulus for job creation and a faster contributor than the offline economies, contributing up to 5.5% per annum (on average) to the overall

---

[7] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrimes: a comparative study' (2009) 12 *Potchefstroom Electronic Law Journal* 37.
[8] International Telecommunication Union 'Global Cybersecurity Index 2017 Africa Report', 2017, available at *http://bit.ly/2C3zrRn*, accessed on 29 December 2017.
[9] F Cassim 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012) 15 *Potchefstroom Electronic Law Journal* 394.
[10] D Mangena 'Will legislation protect your virtual space? Discussing the draft Cybercrime and Cyber Security Bill' (2016) *De Rebus*.

GDP growth[11]. Elsie Kanza of the *World Economic Forum (WEF)*, recently reported the following about the potential of the internet in South Africa:

> 'Forty-eight percent of South Africans between the ages of 15 and 34 are unemployed... The Fourth Industrial Revolution offers South Africa, and Africa - a continent where 70% of the population is under 30 - a real opportunity to use digital technology to leapfrog growth and to emerge as key players in the technology sector.'[12]

Although the South African government has undertaken to invest in the ICT sector and through it, to improve the quality of lives and prospects of its citizens, its efforts fall short. Some of the government's key ICT Policy frameworks, strategies and/or related programmes for realising its ICT intentions are discussed below.

1.5.1 The National Development Plan

The National Development Plan, 2030 (NDP) launched in 2012 by the National Planning Commission, is a blueprint for how the country can eliminate poverty and reduce inequality by the year 2030. The medium term target of the NDP, from 2015 to 2020, is that there should be 100 percent broadband access to all schools, health facilities, and similar social institutions whilst ensuring that individual citizens have access to affordable information and voice communication services.[13] The NDP's hopes for 2030 are, to lead South Africa to becoming a connected information society that fully participates in a vibrant, innovative, prosperous, and inclusive knowledge economy.[14] It is hoped that this society will be realised through the provisioning of universally accessible, reliable, and affordable broadband access that will empower all and unlock mass access to global ICT commercial opportunities.

The Infrastructure Development Act 23 of 2014, through which the strategic integrated projects were realised, resulted in the commencement of the Strategic Integrated Project 15 (SIP15): Expanding Access to Communication Technology. This project aims to prioritise the establishment of national backbone infrastructure

---

[11] Ibid.
[12] E Kanza 'How universal internet access could reboot South Africa' (16/062017) *World Economic Forum*, available at *http://bit.ly/2z9sgcx*, accessed on 15 November 2017.
[13] National Planning Commission '*National Development Plan 2030*' (2011) 178.
[14] Ibid.

and to provide connectivity to e-health, e-schools and e-government facilities. Some of the key mid-term targets of the SIP (15) are to provide broadband access to all households, to migrate from analogue to digital national TV broadcasting and to improve regulation and competition within the sector.[15]

1.5.2 The New Growth Path

Complimentary to the NDP is the New Growth Path (NGP) which came about because of the Industrial Policy Action Plan (IPAP). The NGP's target is the creation of 100 000 new jobs by the year 2020 in the knowledge-intensive sectors of ICT, higher education, healthcare, mining-related technologies, pharmaceuticals, and biotechnology[16]. These targets are informed by the belief that a functional information and technology sector will greatly enable substantial employment creation.

The long-term year (2030) IPAP targets are as follows:

- ✓ 100% of population to have internet (broadband) access of 10mbps speed;
- ✓ 80% of population to have internet (broadband) access of 100mbps speed;
- ✓ 100% of schools to have internet (broadband) access of 1gbps speed;
- ✓ 100% of health facilities to have internet (broadband) access of 1gbps speed;
- ✓ 100% of government facilities to have internet (broadband) access of 100mbps speed.

1.5.3 South Africa Connect: Creating Opportunities, Ensuring Inclusion. South Africa's Broadband Policy (South Africa Connect)

The National Broadband Policy of 2013 (also referred to as South Africa Connect), has the following vision for 2020: that all citizens must have access to broadband

---

[15] Presidential Infrastructure Coordination Commission 'A summary of the South African infrastructure plan', 2012, available at *http://bit.ly/2EdBjJy*, accessed on 31 October 2017.
[16] N Nattrass 'The new growth path: Game changing vision or cop-out?'107 *South African Journal of Science* (2011) 4.

and related services at a cost of 2,5% or less of the population's average monthly income[17].

The broadband access targets that South Africa has set for itself are comparable to the global targets set by the International Telecommunications Union's (ITU) Connect 2020: Global telecommunication/information and communications technology goals and targets[18]. The target set for household access to the internet by the year 2020 is 55% and the target for access to the internet by individuals is 60%. The targets set by South Africa therefore, are in line with global standards, if not slightly more ambitious.

Despite the various government strategies, policies, frameworks, and targets set by the South African government for itself, universal access to broadband and related services remains a challenge as essential targets and deadlines are consistently missed. According to the World Bank[19], the GDP in developed nations can be grown by up to 1.21% from a 10% increase in fixed broadband penetration. The same broadband penetration can benefit the GDP's of developing economies by as much as 1.38%. SA only has 20% broadband penetration. The number of internet users in South Africa has grown beyond 21million, meaning that roughly 40% of the population now has access to the internet. With the world average for internet penetration currently at 46%, South Africa is not far behind.[20]

---

[17] Ellipsis 'Policy direction on effective competition in broadband markets', 2016 available at *http://bit.ly/2BiUouT*, accessed on 21 August 2017.
[18] Plenipotentiary Conference of the International Telecommunication Union '*International Telecommunications Union resolution 'Connect 2020 Agenda for global telecommunication/information and communication technology development*' adopted in Busan ,2014, available at *http://bit.ly/2FXvRLa*, accessed on 11 December 2017.
[19] M Minges 'Exploring the Relationship Between Broadband and Economic Growth' *World Development Report 2016: Digital Dividends*, 2016, available at *http://bit.ly/2lZTn4p*, accessed on 7 December 2017.
[20] G Van Zyl 'Ripe for a digital revolution: 40% of SA now has internet access – study' ,2017, available at *https://www.biznews.com/tech/2017/07/19/sa-internet-access-study/*, accessed on 17 November 2017.

The WEF's Network Readiness Index[21] assesses countries using the following four categories:

1. The overall environment for technology use and creation;
2. Networked readiness in terms of ICT infrastructure, affordability, and skills;
3. Technology adoption/usage by the three groups of stakeholders (government, the private sector, and private individuals); and
4. The economic and social impact of the new technologies.

South Africa, ranked 65th, is behind 5th ranked United States of America (USA), and the United Kingdom (UK) in position eight. South Africa did however rank higher than Kenya, 86th and India at 91.

Despite the Constitution[22], polices, strategies, and plans of the South African government to provide all with access to quality, responsive internet access, the South African government with Russia, China, Saudi Arabia, and India, voted against the United Nations Human Rights Council non-binding resolution on 'the promotion, protection and enjoyment of human rights on the internet'[23] in June 2016. This resolution condemns countries that intentionally take away or disrupt its citizens' internet access. It stresses that people must be allowed to enjoy the same rights they have offline when online. The right of freedom of expression is protected by Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The RSA government has acted contrary to Article 19 and the Covenant on Civil and Political Rights.

---

[21] World Economic Forum 'Global Information Technology Report 2016', 2016, available at *http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index,* accessed on 15 November 2017.

[22] Section 16 (1) of the Constitution of the Republic of South Africa, 1996, does not explicitly protect internet freedom but states that everyone has the right to 'freedom to receive or impart information or ideas'. This is a right for everyone and it is not just a freedom from interference but is a right to communicate with other and to also be reached by others.

[23] United Nations Human Rights Council '32nd session of the Human Rights Council (13 June to 1 July and 8 July 2016', 2016, available at *http://bit.ly/1rK70TS,* accessed on 30 November 2017.

As the number of internet connections increases in South Africa, so too will the risk of cybercrime. These gains cannot simply be undone and jeopardised by cyber criminals seeking to compromise and limit the positive change that stand to be realised through the increased internet access. This access will need to be reliable, secured and trustworthy.

2. DEFINITIONS (COMPUTER-RELATED CRIMES, CYBERCRIME, CYBERSECURITY, CYBERWAR, CYBER-ESPIONAGE AND CYBER TERRORISM)

Technological advances, though positive and inspirational by nature, also create opportunities for criminals and introduce newer types of crimes. Considering that criminals do not need a computer to commit fraud, traffic in child pornography, commit intellectual property fraud, steal an identity, or violate someone's privacy, these traditional crimes have now become easier to carry out in the digital era. Stevenson, when explaining how ethical definitions involve a wedding of descriptive and emotive meaning, argues that '[t]o choose a definition is to plead a cause'[1], meaning that definitions in and of themselves, can encourage future actions.

Before a comparison and evaluation of the various legislative frameworks in question can be undertaken, it is essential to establish an understanding of, and to distinguish between, the following terms: cybercrime, cybersecurity, cyber-espionage, cyberterrorism, and cyberwar(fare). These terms are commonly used to refer to varying criminal acts involving computers, mobile devices, communication networks and the internet. They remain misunderstood and increasingly misused in common parlance and in academia.

2.1 Cybercrime

Cybercrime is commonly described as the criminal use of computer technology and is said to be a form of crime that happens in the world of computers and the internet, known as cyberspace. As coined in 1995 by Sussman and Heuston, the term 'cybercrime' is best considered as a series of criminal acts, 'based on the material offence object and modus operandi that affect computer data or systems.'[2]

---

[1] G Kisicek & IZ Zagar 'What do we know about the world? Rhetorical and argumentative perspectives',2013, available at *http://bit.ly/2C6f2LD*, accessed on 20 April 2017.
[2] R Sabillon et al 'Cybercriminals, cyberattacks and cybercrime. Privacy, security and control' (2016) *Institute of Electrical and Electronics Engineers* 3.

There appears to be no precise definition for cybercrime or 'computer crime'.[3] Nor does there seem to be a globally accepted standardised definition for cybercrime. It is argued that the term is a misnomer that describes criminal behaviour where the computer or computer networks may be a source, tool, target, or a place of criminal activity.[4] The term is also used interchangeably with computer crime, electronic crime, high-technology crime, information age crime, cybernetic crime, computer-related crime, or digital crime.

The development of a common language to facilitate sound collaboration and further research on this subject matter requires clearly defined and understood cybercrime terminology.[5] Although it is essential to develop a common definition for cybercrime, at a country level, this process is subject to sovereign decisions and an object of international cooperation and application.

2.1.1 Computer Crime

Computer crime has been described as 'any violation of criminal law that involves knowledge of computer technology by the perpetrator, investigator or prosecution'[6]. Cybercrimes differ from computer crimes in that they most often involve connectivity between software and/or the flow of information. Conversely, computer-related crimes encompass offences committed without the presence of a computer network, affecting only stand-alone computer systems.[7]Cybercrime is thus a sub-category of computer crime.

The following section considers the definitions of the cybercrime terminology in question, by subject country, starting with east and southern Africa and then proceeding to the USA and the UK.

---

[3] Internet Safety Campaign Africa *'*Cybercrime Definition' available at *http://cybercrime.org.za/definition* accessed on 29 March 2017.
[4] R Arora 'Introduction to Cyber-crimes, cyber security, and legal aspects', available at, *http://bit.ly/2FZPB0S,* 2013, accessed on 07 April 2017.
[5] S Gordon & R Ford 'On the definition and classification of cybercrime' (2006) 2 *Journal of Computer Virology and Hacking Techniques* 17.
[6] Cassim op cit (n7) 36.
[7] M Gercke 'Understanding Cybercrime: Phenomena, challenges, and legal responses.' 2012, available at, *http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*, accessed on 5 April 2017.

i. Eastern and South(ern) African Definitions of Cybercrime

Papadopoulos defines cybecrime as 'any unlawful conduct involving a computer or computer system or computer network, irrespective of whether it is the object of the crime or instrumental in the commission of the crime.'[8]

Kenya's primary legislation for cyber security and related matters, the Information and Communications Amendment (ICA) Act of 2013, fails to tender a definition of cybercrime. The National Cybersecurity Strategy is also silent on the definition of cybercrime. The 2017 Computer and Cybercrimes Act, defines cybercrime offences and is a powerful tool for the investigation and prosecution of cybercrimes, but it also does not define cybercrime.

Section 10 of South Africa's 2012 Electronic Communications and Transactions Act (ECTA), Amendment Bill[9], defines cybercrime as 'any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the internet or any one or more of them.'[10] The Cybersecurity Policy Framework for South Africa of 2015 further defines cybercrime as 'illegal acts, the commission of which involves the use of information and communication technologies.'[11] There is no definition of cybercrime in the 2017 Cybercrimes and Cybersecurity (CAC) Bill.

The ITU & African Union (AU) cybercrime model law[12] contains provisions relating to cybercrime, but leaves the defining of the cybercrime to the individual jurisdictions to develop. Similarly, the 2008 East African Community (EAC) Legal

---

[8] M Watney *Cybercrime and the investigation of cybercrime* in S Papadopoulos & S Snail (eds) *Cyberlaw@SA* 3ed (2012) 336.
[9] Bill may not be passed. Has laid fallow for six years and due to be replaced by Cybercrimes and Cybersecurity Bill, 2017.
[10] s10 of ECTA, Amendment Bill,2012.
[11] National Cybersecurity Policy Framework for South Africa (2015).
[12] Harmonisation of ICT Policies in Sub-Saharan Africa (HIPSSA) 'Computer Crime and Cybercrime SADC Model Law' 2008 *International Telecommunications Union*.

Framework for Cyberlaws[13], the 2010 Common Market for Eastern and Southern Africa (COMESA) Model Law on Electronic Transactions**,** the 2011 Common Market for Eastern and Southern (COMESA) Africa Cyber Crime Model Bill and the 2014 African Union Convention on Cybercrime and Data Protection, all do not furnish their member states with a definition for cybercrime either.

ii.International Definitions of Cybercrime

Kshteri defines cybercrime as 'criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations.'[14]

India's Information Technology (IT) Act of 2000 and its 2008 amendment, do not define the term cybercrime. Section 43(j)(i) of the Act however, introduces the following term 'computer contaminant'[15] together with cybercrime offences and penalties. There is also no definition of cybercrime in the 2013 National Cyber Security Policy of India.

The UK National cyber security strategy of 2016, categorises cybercrimes into cyber-enabled and cyber-dependant cybercrimes, without defining cybercrime. The Computer Misuse Act of 1990 and the arsenal of cyber laws[16] in the UK, create cybercrime offences and penalties but none offer a definition for cybercrime**.**

The European Commission defines cybercrime for the region as follows: 'Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems.'[17] The WEF's definition of

---

[13] Not intended to create legal obligations for member states but designed to serve as inspiration or models for the development of national legislative provisions.
[14] N Kshteri *Cybercrime and Cybersecurity in the Global South* 2013 6.
[15] '(i) Computer contaminant' means any set of computer instructions that are designed– (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network.
[16] 'Cyber Crime – Legal Guidance' *The Crown Prosecutors* 2017, available at *https://www.cps.gov.uk/legal-guidance/cybercrime-legal-guidance,* accessed on 17 December 2017.
[17] 'Cybercrime' *European Commission*, 2017, available at, *https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en*, accessed on 19 April 2017.

cybercrime adds to the definition supplied by the European Union (EU) in that cybercrimes are also those criminal activities that are traditional crimes but are further enabled or aggravated by the internet.[18]

In the USA, federal computer offences are defined in and dealt with through the United States Code[19], the Uniting, and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT) Act[20], the Racketeer and Influenced Corrupt Organisation Act[21], and the Computer Fraud and Abuse Act[22], none of which contain a definition for cybercrime.

The United Nations (UN) defines cybercrime in two ways. Narrowly - as the 'illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them'[23] and more broadly defined, cybercrimes is 'any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.'[24]

Although there is still no universally acceptable definition for cybercrime, those jurisdictions that have defined this term seem to have the same goal of criminalising trans-border cybercriminal activities perpetuated by or directed at data, computers, and/or computer networks through the internet. The journey towards effective regulating, prosecuting and the combating of cybercrime begins with the ability to accurately define and distinguish cybercrimes from related incidents such

---

[18] J Vez 'Recommendations for Public-Private Partnerships against Cybercrime' *WEF*, 2016, available at *http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf*, accessed on 19 April 2017.
[19] A Rees 'Cybercrime Laws of the United States' *US Department of Justice: Computer Crime and Intellectual Property Section* 2006 available at *https://www.oas.org/juridico/spanish/us_cyb_laws.pdf* accessed on 10 February 2018.
[20] The Uniting, and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.
[21] 18 U.S.C §1961-68.
[22] 18 U.S.C §1830.
[23] 'Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders' *United Nations* 2000, available at *http://bit.ly/2kjJFXN* accessed on 19 December 2017.
[24] Ibid.

as cyber espionage, cyber warfare, and cyber terrorism. This distinction is essential and may be the difference between an investigation being undertaken in the interest of local law enforcement or national security for instance.

2.2 Cybersecurity

The next commonly misused and misunderstood term is 'cybersecurity'. The common technical definition means to safeguard and prevent incidents of cybercrime. Failure to accurately define this term means failure to task the relevant functions to ensure protection from, and/or prosecution of incidents of cybercrime. This term was initially used to refer to officials responsible for addressing security concerns emanating from the internet or cyberspace. Cybersecurity, is often incorrectly referenced as a synonym for the terms 'IT security', 'ICT security' or 'information security'. There appears to be no precise definition for cybersecurity either. Many jurisdictions and regional economic communities have legislative provisions relating to cybersecurity but none provide a definition for the term.

i. Eastern and South(ern) African Definitions of Cybersecurity

Both South Africa's (ECTA) Amendment Bill of 2012 and the (CAC) Bill,2017, contain provisions related to cybersecurity, but provide no definition for the term. The National Cybersecurity Policy Framework of 2015, defines cybersecurity as the securing of 'networks that constitute cyberspace against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.'[25] Like South Africa, the Southern African Development Community (SADC) model law for cybercrime[26] also has provisions addressing cybersecurity, but does not define the term, leaving it to the member states to develop in their own jurisdictions.

---

[25] Ibid.
[26] HIPSSA (2008) '*Computer Crime and Cybercrime SADC Model Law.'*

Section 2(c) of Kenya's ICA Act defines cyber security as a 'collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment.'[27]. Neither the 2008 EAC Legal Framework for Cyberlaws, the 2010 Common Market for Eastern and Southern Africa (COMESA) Model Law on Electronic Transactions, nor the 2011 Common Market for Eastern and Southern Africa (COMESA) Cyber Crime Model Bill, define 'cybersecurity' for the East African region. They only contain cybersecurity related provisions. The 2014 African Union Convention on Cybercrime and Data Protection[28] also fails to provide a definition for cybersecurity.

ii. International Definitions of Cybersecurity

The ITU describes the objective of cybersecurity as securing the assets of a corporation or nation against cyber threats and risks.[29]

India's Information Technology Amendment (ITA) Act of 2008 defines cybersecurity as 'protecting information, equipment, devices, computing, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.'[30]

The US National Initiative for Cybersecurity Career and Studies' extended definition of cybersecurity is as follows:

> 'Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass the full range of threat reduction, vulnerability reduction, deterrence, 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.'[31]

---

[27] s2(c) of Information Communication and Technology Amendment Act of 2013, Kenya.
[28] Although adopted, this convention is not yet in force as the requisite ratification has not yet been achieved. In accordance with article 36, a minimum of 15 ratifications are required for the convention to enter force. available at *http://bit.ly/2nVb9Es*, accessed on 5 February 2018.
[29] ITU 'Definition of Cybersecurity' 2017, available at, *http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx* accessed on 24 May 2017.
[30] s2(D)(b) of ITA Act of 2008, India.
[31] National Initiative for Cybersecurity Career and Studies 'A Glossary of common cybersecurity terminology' US Department of Homeland Security 2017, available at *https://niccs.us-cert.gov/glossary#C* accessed 24 May 2017.

The UK Computer Misuse Act of 1990 does not define 'cybersecurity'. The United Kingdom's National Cyber Security Strategy defines 'cybersecurity' as 'the protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse.' [32]

The EU Agency for Network and Information Security's definition of cybersecurity is the 'protection of information, information systems and infrastructure from those threats that are associated with using ICT systems in a globally connected environment.'[33].

Cybersecurity governance measures include technical, organizational, policy, and legal aspects. Promoting good cyber security also involves the creation of laws that prohibit all acts that are contrary to the confidentiality, integrity and availability of information, systems, and critical information infrastructure. These laws enacted to bolster cyber security should not only concern themselves about the securing systems and networks but should also criminalise computer enabled criminal acts.[34]

---

[32] UK National Cyber Security Strategy 2016 – 2021 (2016) 33.
[33] U Helmbrecht 'ENISA at the service of the EU's cyber security*' European Union Agency for Network and Information Security* 2015, available at *http://bit.ly/2BBWUed* accessed on 24 May 2017.
[34] UJ Orji, 'Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?' *NATO Cooperative Cyber Defence Centre of Excellence* 2015, available at, *https://ccdcoe.org/cycon/2015/proceedings/08_orji.pdf*, accessed on 29 August 2017.

2.3 Cyber espionage

Where the target of cybercrime activities ranges from competitors, key infrastructure or utilities providers, large enterprises, military, governments, and the motive of the attack is to illegally acquire private information for industrial, economic, political, or military gain, then it is more than ordinary acts of cybercrime. They are illicit intelligence gathering acts of cyber espionage, aimed at acquiring intellectual property or government secrets and may further lead to industrial, economic or political espionage. It is essential therefore, to be able to define, identify and distinguish instances of cyber-espionage from incidents of cybercrime so that the appropriate actors can be deployed. Failure to do this may result in incidents of cyber-espionage being classified as standard cyber-attacks.

i. Eastern and South(ern) African Definitions of Cyber-Espionage

Cyber-espionage or related terms have not been defined in South Africa's ECTA Amendment Bill, 2012 nor the CAC Bill,2017. However, the latter defines the term 'restricted computer system'[35], which sufficiently defines and criminalises acts of cyber-espionage within South Africa. The National Cybersecurity Policy Framework for South Africa defines cyber-espionage as 'the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage.'[36]

For SADC member states, the 2008 cybercrime model law contains provisions related to 'data espionage', but offers no definition for the term 'cyber-espionage'.

---

[35] Means any data, computer program, computer data storage medium or computer system under the control of, or exclusively used by—(i) any financial institution;(ii) an organ of state as set out in section 239 of the Constitution; or (ii) a Critical Information Infrastructure.
[36] National Cybersecurity Policy Framework for South Africa (2015) 8.

Similarly, Kenya's ICA Act, does not contain a definition for cyber-espionage. The 2017 Computer and Cybercrimes Act on the other hand, only contains a definition for 'protected computer system'[37] but has provisions criminalising cyber-espionage, although the term is not defined therein.

The East African Economic Community model laws and frameworks such as the 2008 EAC Legal Framework for Cyberlaws, the 2011 COMESA Cyber Crime Model Bill and the 2010 COMESA Model Law on Electronic Transactions**,** contain provisions related to cyber-espionage, such as unauthorised access to computer programs, computer data and traffic data, but offer no definition for 'cyber-espionage'.

The AU Convention on Cybercrime and Data Protection 2014 does also not offer the continent a definition for cyber-espionage in its model law.

ii. International Definitions of Cyber-Espionage

The Tallinn Manual defines cyber-espionage as 'any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather information) with the intention of communicating it to the opposing party.'[38] Sabillon defines it as 'acts that involve exfiltration, unauthorized access, interception, and acquisition of data.'[39] Cyber-espionage may constitute cyber-attacks aimed at illegally obtaining sensitive information and data from financial, government and utility providers. Scholars of information warfare often use the terms cyber espionage and computer operations interchangeably. Depending on the

---

[37] s10(2) - means a computer system used directly in connection with, or necessary for (a), the security, defence or international relations of Kenya: (c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically; (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

[38] MN Schmitt 'Tallinn Manual 2.0 on the International Law Applicable to Cyberwarfare', 2013, Rule 66.

[39] R Sabillon et al (2016) 4.

context, computer operation can either mean the intelligence and data collection from a target or adversary computer systems, or alternatively mean, as defined by the United States Joint Chiefs of Staff, to 'attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.'[40]

India's IT Act does not provide a definition for the term 'cyber-espionage'. The closest the Act and the 2008 Amendment Act, come to defining cyber-espionage is the criminalising of unauthorised access to 'protected systems'[41].

The Homeland Security Act[42], the PATRIOT Act, and the US Code all contain the phrase 'protected computer'[43] and all have cyber-espionage provisions for the protection of not only federal computers and their information but extends to computers used in interstate or foreign commerce. The US Code[44] and the Economic Espionage Act of 1996 also outlaw unauthorised access to trade secrets by way of computer in a commercial setting. Although the listed acts regulate and criminalise cyber-espionage, none of them define the term.

None of the UK IT laws studied contain a definition for 'cyber-espionage'. The National Cyber Security Strategy uses the phrase 'cyber network exploitation' interchangeably with 'cyber espionage', which it defines as 'the use of a computer network to infiltrate a target computer network and gather intelligence.'[45]

---

[40] D Weissbrodt 'Cyber-Conflict, Cyber-Crime And Cyber-Espionage' 2013, available at *http://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_*articles accessed on 29 August 2017.
[41] s70 India Information Technology Act of 2000.
[42] The Homeland Security Act of 2002.
[43] [T]he term 'protected computer' means a computer—(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government or (B) which is used in interstate or foreign commerce or communication, *including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States*, 18 U.S.C §1030(*e*)(2).
[44] 18 U.S.C §1832(a).
[45] UK National Cyber Security Strategy 2016 – 2021 (2016) 74.

2.4 Cyber-Terrorism

Cyber-terrorism is a term that is also often used out of context and not defined. The term 'terrorist' is mainly used in association with extremist militia whose modus operandi is to use grand scale acts of violence and fear to further their political or religious ideologies. Shackleford explains that: 'cyber-terrorists, use cyberspace to disrupt computer or telecommunications services to illicit widespread disruptions and loss of public confidence in the ability of government to function effectively.'[46]

As a recognised form of cybercrime, cyber-terrorism, is said to be about organised crime and terrorist groups using sophisticated computer technology to bypass government defences and carry out destructive acts of violence. The target of these attacks range from information infrastructures, computer systems, computer programmes to data.

The global rise of terrorism-related activities has led to an increased fear and broader coverage of cyber-terrorism. This has resulted in the blurring of the distinctions between what constitute acts of hacktivism and which are cyber terrorism, thus the need to distinctly define the term 'cyber-terrorism'.

i. Eastern and South(ern) African Definitions of Cyber-Terrorism

Watney defines cyber-terrorism 'as the unlawful attack or threat of attack on computers and networks and the information stored in them for intimidation or coercion of a government or its people for the furtherance of a political or a social goal.'[47]

---

[46] SJ Shackelford 'Towards Cyber-peace: Managing Cyberattacks through Polycentric Governance' (2013) 62 *American University Law Review* 1301
[47] Watney op cit (n8) 337.

South Africa's current set of cyber laws[48] and the regional cybercrime model law[49] do not offer a definition for 'cyber-terrorism' but they do contain provisions relating to cyber-terrorism, such as the protection of critical databases, protection of critical information infrastructure, unauthorised access to data, interception of or interference with data, unlawful acts in respect of software or hardware tools. The term finds definition in the National Cybersecurity Policy Framework for South Africa where it is described as 'the use of internet based attacks in terrorist activities by individuals and groups, including acts of deliberate large scale disruptions of computer networks, especially computers attached to the internet.'[50]

Kenya's Information Technology Act and its 2013 Amendment Act are silent on the definition of cyber-terrorism. It is in the 2017 Computer and Cybercrimes Bill that related provision pertaining to the protection of critical databases and the protection of national critical information infrastructure, are found. The 2008 EAC Legal Framework for Cyberlaws, the 2010 COMESA Model Law on Electronic Transactions and the 2011 COMESA Cyber Crime Model Bill all do not provide a definition for the term cyber-terrorism for the East African region.

The 2014 AU Convention on Cybercrime and Data Protection also does not provide a working definition for cyber-terrorism that its member states can reference.

ii. **International Definitions of Cyber-Terrorism**

Pollit, authoritatively describes cyber-terrorism as a 'premeditated, politically motivated attack against information, computer systems, computer programmes, and data which result in violence against non-combatant targets by sub national groups or

[48] ECT Amendment Act of 2012, Regulation of Interception of Communications and Provision of Communication related Information Act 70 of 2002; Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004; Financial Intelligence Centre Act 38 of 2001; Prevention of Organised Crime Act 38 of 1999 and the Cybercrimes and Cybersecurity Bill of 2017
[49] HIPSSA (2008) 'Computer Crime and Cybercrime SADC Model Law'.
[50] National Cybersecurity Policy Framework for South Africa (2015) 9.

clandestine agents'[51]. Cyber-terrorism encompasses attacks against life and electronic infrastructure which are targeted at national security establishments and critical infrastructure. The main aim of the cyber-terrorism attacks is to cause panic in society.[52] Acts of cyber-terrorism are distinguishable from other forms of cybercrime in that they generally disrupt essential services of a nation, can result in violence against persons or property, or at least cause enough harm to generate fear and the attacks can lead to bodily injuries, loss of lives, explosions, plane crashes, water contamination, or even severe economic loss.

Section 66(F) of India's 2008 Amended IT Act contains provisions that criminalise acts of cyber-terrorism and corresponding penalties for the crime. There is no outright definition within the Act, nor is it defined in the 2013 National Cyber Security Policy.

Close inspection of the USA's PATRIOT Act of 2001 reveals no definition for the term 'cyber-terrorism' within it. This despite the act being very pronounced on cyber-terrorism and containing provisions such as, deterrence and prevention of cyber-terrorism, development, and support of cybersecurity forensic capabilities. The Act also calls for the amendment of the Critical Infrastructures Protection Act of 2001 and parts of title 18 of the United States Code in relation to cyber-terrorism.

Analysis of the UK legislation, namely, the UK Terrorism Act of 2000, the various pieces of cyber legislation[53] and the National Cyber Security Strategy suggests that there is no official legal definition for the term 'cyber-terrorism' in the UK. There are however provisions within these laws that regulate 'cyber-terrorism'.

---

[51] S Krasavin 'What is Cyber-Terrorism' 2002, available at *http://bit.ly/1Lnsjm5*, accessed on 20 December 2017.
[52] Cassim op cit (n9) 384.
[53] Anti-Terrorism, Crime, and Security Act 2001; Terrorism Act of 2006; Computer Misuse Amendment Bill 2002; UK National Cyber Security Strategy 2016 – 2021.

Regionally, the Council of Europe's (COE) 2011 Convention on Cybercrime also does not provide a definition for its member nations to adopt.

The UN Global Counter-Terrorism Strategy fashions the definition of cyber-terrorism to be the:

> '[I]ntentional use or threat of use of electronic information systems for the perpetration of terrorist acts inspired by certain motives with the aim to cause death or serious bodily injury, serious material damage, create a state of fear, compel a government or an international organization to do or to abstain from doing any act.'[54]

2.5 Cyber-war(fare)[55]

Defence of national security has evolved over the years from being predominantly concerned with protecting tangible physical structures into fifth domain of military warfare[56], namely 'information, the veritable lifeblood of our modern economy and culture'[57]. The protection of a nations proprietary information is now deemed a vital component of its defence strategy.

Acts of war are no longer limited to physical military-versus-military engagements but now comprise attacks on the most critical national infrastructure, which if attacked, could disable a nation without physical exchange of fire.[58] The extension of the notion of war into the digital or cyber environment, has direct consequences for the extent and application of rule of law, the protection of persons, preservation of state authority, and stability of the international system. Concise understanding of this area of the law is thus essential to prevent overreach and the limitation of civil liberties in the name of 'war' or 'attacks' against the sovereign state.[59]

---

[54] UN 'Global Counter-Terrorism Strategy' 2011, available at, *https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf* accessed on 30 August 2017.
[55] In this dissertation '*cyber war*' means an act of war and '*cyber warfare'* is how the cyberwar is carried out.
[56] D Hughes & A Colarik 'The Hierarchy of Cyber War Definitions' *Massey University* 2017
[57] ITU 'Cybercrime and Espionage' United Nations 2015 available at *www.igmun.org/wp-content/uploads/2015/10/6-ITU-Synopsis.pdf*, accessed on 4 February 2018.
[58] Global Information Assurance (GIAC) Certification Paper 'Information Warfare: Cyber Warfare is the future warfare (2004) at 4.
[59]JD Ohlin et al, '*Cyber War: Law and ethics for virtual conflicts'* (2015) 74

i. Eastern and South(ern) African Definitions of Cyberwar(fare)

Watney's definition of cyberwar or information warfare may be defined as "the actions taken to infiltrate, corrupt, disrupt or destroy the information systems of an adversary."[60]

South Africa's ECTA Amendment Bill and CAC Bill,2017contain provisions pertaining to cyber warfare. None of them however contain a definition for the term. Cyberwar is defined in the National Cybersecurity Policy Framework as: **'**actions by a nation or state to penetrate another nation's computers and networks for purposes of causing damage or disruption.'[61]

Like South African's cyber laws, Kenya's IT laws[62] regulate cyber war without it being defined in in law. The regional legal instruments and model law, also contain provisions related to cyber warfare, but offer no definition.

ii. International Definitions of Cyberwar

There are various definitions for cyberwar internationally. The scholarly understanding of the term is: 'an attack by one hostile nation against the computers or networks of another to cause disruption or damage, as compared to a criminal or terrorist attack involving private parties.'[63]

As cyberwar is a type of information warfare, it is thus paramount to start with defining what information warfare is. Information warfare is about 'actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer based networks while defending one's own.'[64]

---

[60] Watney op cit (n8) 337.
[61] National Cybersecurity Policy Framework for South Africa (2015) 8.
[62] IT Act, ICA Act, Computer and cybercrimes Bill 2017.
[63] Shackelford op cit (n46) 1297.
[64] I Porche et al 'Redefining Information Warfare Boundaries, for an army in a wireless world', 2013 available at *https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf,* accesses on 10 February 2018 xvi.

Cyberwar on the other hand can be defined as the acts of a nation state to penetrate another nation's computer or network to cause it harm or disruption[65]. Cyberwarfare on the other hand, may be defined as 'the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state.'[66]

Cyberwarfare can take one of two forms: it can either be the offensive[67] or defensive[68] kind of cyberwar operations. With the offensive form, intelligence about the cyberspace capabilities, configuration, and operations of a country, is regularly collected and used against them to disrupt, destabilise and degrade their cyber defence arrangements. Conversely, defensive cyberwarfare is mainly about countries bolstering their national cyberspace defence capabilities to proactively detect, analyse and mitigate against threats to national security- in so doing, designated networks and critical infrastructure will be protected.

The term 'cyber war' is not used nor defined within both of India's IT laws and the National Cyber Security Policy. However, there are provisions that directly regulate cyber war.

In the USA, the US Penal Code[69] does not include cyberwar amongst the list of actions that may be deemed an act of war. The US Code also does not define what cyberwar is, nor is the term defined by any of the current sets of laws regulating cybercrime. Thus far, the waging of cyberwarfare has been a prerogative of the

---

[65] D Hughes and A Colarik (2017) 26.
[66] Ibid.
[67] JE Cartwright 'Cyberspace Operations Lexicon' *US DoD* 2011, available *at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf* accessed on 12 December 2017 Para 34.
[68] Ibid Para 11.
[69] 18 U.S.C §12331(4).

executive in terms of the War Powers Resolution[70]and the Department of Defence's Strategy for Operating in Cyberspace[71]. Efforts to legislate the declaration of cyber war as an act of war are underway as per the proposed Cyber Act of War Bill of 2017[72] is before the Senate. Once enacted it will contain provisions related to regulating cyber war and hopefully a definition of the term.

The UK National Cyber Security Strategy and cyber laws[73], does not define the term 'cyber war' although there are provisions dedicated to dealing with national cyber-attacks and state-sponsored threats.

Similarly, UN Article 2(4): prohibition on the use of force, and Article (51): inherent right to self-defence, both contain provisions relating to and deemed by the International Court of Justice[74] to be applicable to 'cyber war'. The UN Charter does not define the term 'cyber war' nor does Article 36 of the 1977 additional protocol to 1949 Geneva conventions.

2.6 Cyber Lexicon

The two tables below have been inserted to assist in identifying and distinguishing between the various types of computer-based crimes. Table 1 seeks to enable correct identification of the category of crime based on three factors, namely the motive, target and method of attack deployed by the perpetrator whereas Table 2 assists in identifying the type of computer-based crime by determining the actors involved, namely the perpetrator of the crime and their chosen target.

---

[70] J Healey and A.J. Wilson 'Cyber Conflict and the War Powers Resolution' *Georgetown Journal of International Affairs* 2012.
[71] US DoD Strategy for Operations in Cyberspace 2015 Available at *http://bit.ly/2mpJ0Yd* accessed on 24 December 2017 p5.
[72] Cyber Act of War Bill of 2016.
[73] Communications Act of 2003; Civil Contingencies Act 2004; Computer Misuse Amendment Bill 2002; Data Protection Act 1998; European Union - General Data Protection Regulation; European Union - The Network and Information Security Directive 2016/1148.
[74] International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996, para 39.

	Motivation	Target	Method
Cyber crime	Economic gain	Individuals, companies	Malware for fraud, identity theft, DDOS for blackmail
Cyber Espionage	Economic and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber Terrorism	Political or social change	Innocent Victims	Computer-based violence or destruction
Information War	Political or military gain	Infrastructure, information technology systems and data (private or public)	Range of techniques for attack or influence operations

Table 1: Identifying computer-based crimes by target and motivation[75]

Actors: Perpetrator→ Target ↓	Government	Business	Individual/Consumer
Government	- Cyberwarfare - International spying activities	- Organised cybercrime groups targeting government networks	- Computer-based violence or destruction
Business	- Spying activities on business - Government attacks on business websites	- Industrial cyber espionage - Online extortions targeting businesses	- Intrinsically motivated cybercrimes - Fighting for ideology Malware for fraud, identity

[75] Kshteri op cit (n14) 25.

			theft, DDOS for blackmail
Individual/Customer	- Spying on citizens - Cyberattacks targeting citizens (sending virus-infected emails to dissidents)	- Illegitimate companies targeting individuals - Online extortions targeting individuals - Sending email spam	- Intrinsically motivated cybercrimes (e.g. cyber-bullying) - Extrinsically motivated cybercrimes

Table 2: Identifying computer-based crimes by category of actors involved.[76]

Defining cyber-criminal terms is not only essential from the perspective of a local jurisdictions but it is equally essential for international harmonisation of terms and laws.[77]

The primary focus of lawmakers around the world, when developing cyber laws, has largely been on criminalisation: creating new offences and penalties or adapting existing offences to address the broader challenges of cybercrime. The secondary objective has been to pronounce investigation and prosecution procedures following cyber incidents.

The study of the various nations' primary IT laws revealed that only South Africa's ECT Amendment Act defined the term 'cybercrime'. The analysis also uncovered that apart from India's IT Act, none of the subject countries' primary IT laws contained a definition for 'cybersecurity'. Similarly, none of the reviewed IT

[76] F Kramer et al '*Cyberpower and National Security'*,2009 439.
[77] J Clough 'A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation' (2014) 40 (3) *Monash University Law Review* 698.

laws of the subject nations contained definitions for ‘cyber-espionage’, ‘cyber-terrorism’ and ‘cyber war’.

As already reported, India’s IT Act does not provide a definition for ‘cybercrime’ and ‘cyber espionage’, nor does the US Code provide a definition for ‘cyber espionage’. As alternates, India’s IT Act offers the following definitions for ‘computer contaminant’ in the place of cybercrime and the term ‘protected systems’ for cyber espionage. The US Code defines ‘protected computer’ as an alternate term in the place of cyber espionage.

Where applicable, the IT laws specially drafted to combat cybercrimes, were also analysed for the definitions of cyber-criminal terminology. India and the UK exempted, none of the special cyber laws studied provided definitions for any of the terms in question. The special cyber laws all offered an alternate term for cyber espionage. South Africa’s CAC Bill defines ‘restricted computer system’ in the place of cyber espionage. Kenya’s Computer and Cybercrimes Act defines ‘protected computer system’ in the place of cyber espionage, where the US PATRIOT Act defines ‘protected computer’ as an alternative definition for cyber espionage

The search for legal definitions for cyber-criminal terminology extended to the national cybersecurity strategies and/or policies of the subject nations. In direct contrast to the primary IT laws and specialised cyber laws and owing largely to being more recent, most definitions were found therein. South Africa’s National Cybersecurity Policy Framework and the UK’s National Cyber Security Strategy both provide definitions for ‘cybercrime’, ‘cybersecurity’, ‘cyber espionage’ and ‘cyber war’. Only the South African cybersecurity framework defines ‘cyber terrorism’. Kenya’s national cybersecurity strategy and India’s National Cyber Security Policy don’t provide any definitions for the cyber-criminal technology in question. The US does not have a national cybersecurity strategy and definitions are mainly defined at an agency level. For comparative purposes, the Department of Defence’s Cyber Strategy was considered. It too contained none of the definitions.

Whether it is necessary to define what cybercrime is and what it is not, is a domestic matter for nation states to resolve. Where the purpose of defining cybercrime is for investigating and prosecuting purposes, defining the activities that constitute cybercrimes may be more worthwhile, regardless of whether the crimes are considered real world crimes or cybercrimes in that jurisdiction. Conversely, where the purpose is to create distinction between acts of cybercrime and other malicious activities, it may then be worthwhile to define cybercrime and its expanding range of cyber threats at a policy level. Communicating a clear definition of cybercrime is essential for all stakeholders and various agencies involved.[78] The lack of definitional clarity is problematic and retards prevention and remediation efforts.

As the body of literature grows and more jurisdictions provide definitions for cybercrime related terms, understanding and awareness of what constitutes cybercrime will also increase.

[78]K Finklea and C Theohary 'Cybecrime: Conceptual Issues for Congress and U.S. Law Enforcement' *Congressional Research Services* 2015, available at *http://bit.ly/2m4DhDX* accessed on 28 December 2017.

3. WHAT IS CYBERCRIME?

The term 'cybercrime' has increasingly found its way into modern every day parlance with various meanings and interpretations attached to it. It has become a widely and loosely used term to refer to just about any criminal activity of an electronic nature that involves computing devices, electronic networks, the internet, and cyberspace. It is essential, for purposes of this dissertation, to define precisely what is meant and understood by this term, its origins, and its intended use within our context. Thus far, this dissertation has attempted to offer definitions for these key terms chapter two.

Through the various definitions analysed, it is apparent that as it relates to cybercrime, '[t]he computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime.'[1] This section will examine: the types of cybercrime; classifications of cybercrime; categories of cybercrime; the various forms of cybercrime; the perpetrators of cybercrime and what motivates them to commit act of cybercrime.

3.1 Types of cybercrime

Furnell[2], Gordon and Ford[3] classify cybercrime into two distinct groupings, namely those of a predominantly type I (also referred to as computer-focused) and type II (also referred to as computer-assisted) nature. Type I cybercrimes are almost entirely technological in nature. They are committed using computer-related and enabled technologies, they take place on computer-related and enabled platforms and rely primarily on computer-related and enabled technologies for their successful execution. Type II group of cybercrimes can be said to be more deceptive as they are almost always people-related. Although these types of crimes are committed using computer-related and enabled platforms and take place on computer-related and enabled platforms, their success is dependent on human frailty, susceptibility, and potential errors in judgements.

---

[1] Gordon & Ford op cit (n5) 14.
[2] M Ngafeeson (2009) 2.
[3] Gordon & Ford op cit (n5) 13.

3.1.1 Type I cybercrimes

These are computer-focused as they depend on the installation, modification, and/or manipulation of 'crimeware' which can be defined as malicious software designed to facilitate the commission of fraud, theft of personal information, from internet users, required to access, authorise or grant entry into programs and systems requiring valid identification and authentication for use. Malware is also written to perform unauthorised online transactions using the ill-gotten personal credentials and identities[4]. These cybercrimes generally exhibit the following characteristics: a once-off, singular occurrence or discrete incident from the perspective of the victim; often facilitated through the introduction of 'crimeware' which may have been successfully installed onto the user's computer systems a result of various vulnerabilities exploited by the perpetrator. Examples of this type of cybercrime include forms of phishing, theft or manipulation of data or services via hacking or viruses.

Type I cybercrimes differ from Type II cybercrimes in that the kind of crimes that fall in this category come about as 'a direct result of computer technology and there is no direct parallel in other factors.'[5]

3.1.2 Type II cybercrimes

These types of cybercrimes have a more pronounced human element and are said to be computer-assisted or computer-facilitated in nature. They are dependent on exploiting human frailties, momentary errors in judgement and play on the human psyche for their success. The perpetrators usually commit these crimes using legitimate, familiar, and frequently used computer programs (such as e-mail and web-browsers), to lure their unsuspecting victims. Forms of Type II cybercrimes

---

[4] M Nyamanga 'A Layered Framework Approach to Mitigate Crimeware' (2010) Annual ADFSL Conference on Digital Forensics, Security, and Law. Available at *http://commons.erau.edu/adfsl/2010/thursday/7* accessed on 30 January 2018.

[5] W Hutchinson '*Survival in the economy: 2nd Australian information warfare & security conference 2001*' 2001, available at *http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7758&context=ecuworks#page=38, 200.1,* accessed on 8 November 2017.

include cyberstalking, cyber bullying, cyber harassment, child predation, extortion, and blackmail. In the case of Type II cybercrimes the underlying crime or offence either predates the emergence of computers or could be committed without them.

Distinguishing between the two types of cybercrimes will not always be possible, nor precise. Not all cybercrimes will present themselves as being purely Type I or Type II in nature, they represent either end of a continuum.[6]

3.2 Typology (Classification) of cybercrime

Based on the object of legal protection and the method used to commit the crime, the 2001 COE Convention on Cyber-crime lays down four criteria to be used for classifying cybercrimes. The convention's section on substantive criminal law, lists them as follows:

a. Offences against the confidentiality, integrity and availability of computer data and systems;
b. Computer-related offences;
c. Content-related offences;
d. Offences related to infringements of copyright and related rights.

The cybercrimes in the federal Computer Fraud and Abuse Act and the PATRIOT Act in the USA can, by deduction, be reasonably classified as those specified by the 2001 European Convention on Cyber-Crime. The same can be said about South Africa's ECT Act and CAC Bill.

These classification of cybercrimes is also adopted and referenced within East Africa's draft EAC legal framework for cyberlaws. Similarly, Article 29 of the African Union's Convention on Cyber Security and Personal Data Protection identifies four classifications of cybercrime, referred to in the convention as offences specific to information and communication technologies:

a. Attacks on computer systems;
b. Computerised data breaches;
c. Content related offences; and

---

[6] Gordon & Ford op cit (n5) 13.

d. Offences relating to electronic message security measures.[7]

3.3 Categories of cybercrime

Having classified cybercrimes, this section delves into the categorisation of these acts of cybercrime and their various forms and instances. There are, in general, four main categories of cybercrime that forms of cybercriminal activities may be categorised into.

3.3.1 Cybercrimes against persons:

This category of cybercrime involves cybercriminal attacks, through computers or computer networks, where the target of the attack is an identifiable individual or a group of persons. Examples of these crimes include insults[8], harassment, acts of a racist and xenophobic nature[9], assault by threatening[10] through to cyber-defamation.

3.3.2 Cybercrimes against property:

This second category of cybercrimes is cyber-attacks that cybercriminals direct at the property belonging to a person and involve varying degrees of violation[11] of, or, tampering with another's property. These cybercrimes are also known as crimes affecting the economy. They range from cyber-vandalism and cyber-squatting through to computer related fraud.

3.3.3 Cybercrimes against governments and/or organisations

With this category of cybercrime, the attackers seek the critical information infrastructure and confidential military information of a country or the confidential mission-critical information that an organisation runs on. Crimes that make up this

---

[7] E Tamarkin 'Cybercrime: A complex problem requiring a multi-faceted response' *Institute for Security Studies* 2014, Available at, *https://issafrica.s3.amazonaws.com/site/uploads/PolBrief51Feb14.pdf* accessed on 10 April 2017.
[8] African Union Cybercrime Convention, Article 29(3)(1)(g) Date of Adoption 27 June 2014. Date of last signature 29 January 2018.
[9] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) Opening of the treaty, Strasbourg 28/01/2003.
[10] African Union Cybercrime Convention, Article 29(3)(1)(f).
[11] Ibid Article 30(1).

category are crimes such as cyber warfare, cyber espionage, industrial espionage, and cyber fraud.

3.3.4 Cybercrimes against society:

These unlawful acts of cybercrime are committed with the intention of causing harm to the broader society at large through using cyberspace to cause widespread harm, to disrupt societal balance and disharmonise the moral wellbeing of society. These offences include: possession and exchange of child pornographic materials, sale of illegal articles, illegal auctions on the internet and cyber terrorism.

As technology evolves, so too do the cyber-attack vectors.[12] By considering the following alternate categories of cybercrime, namely: 'device spoofing, location manipulation, identity fraud, and threats or bots'[13], newer forms of cybercrime and their interdependence and interconnectedness can be more accurately categorised. Table 3 below is inserted to illustrate the alternate categories and newer attack vectors and forms of cybercrime.

[12] R Hummel 'Securing against the most common vectors of cyber-attacks '2017 *SANS Institute* available at, *https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995*, accessed on 04 December 2017.
[13] E Burns 'Periodic table of cybercrime attacks: curing cybersecurity's tunnel vision'2017, available at, *https://www.cbronline.com/cybersecurity/business/periodic-table-cybercrime-attacks-curing-cybersecuritys-tunnel-vision/*, accessed on 03 December 2017.

Table 3: Alternate Cybercrime categories revised by attack vector .

3.4 Forms of cybercrime

3.4.1 COE Convention on Cybercrime.

Most of the cybercrime legislation developed and adopted by countries between the years 2000 and 2010 were based on the traditional principles of substantive cybercrime and as defined by the COE Convention on cybercrime. This cybercrime legislation commonly outlaws the following acts of cybercrime and regards them as offences:

a) illegal access;
b) illegal interception;
c) data interference;
d) system interference;
e) misuse of devices;
f) computer forgery;
g) computer fraud, and;
h) offences related to child pornography.

The convention, and subsequently the legislation that is based on it, does not address cater for the following new methods of cybercrime that must be covered by criminal

law, such as phishing, botnets, spam, identity theft, crime in social networks, internet of things, terrorist use of internet, and massive and coordinated cyber-attacks against information infrastructures.

3.4.2 AU Convention on cyber security and personal data protection.

Article 29 of the convention lists the following as cyber-criminal offences:

a) Attack on computer system;
b) Computerised Data Breaches;
c) Content related offences;
d) Offences relating to electronic message security;
e) Property Offences.

3.4.3 South Africa: Cybercrimes and Cybersecurity Bill 2017.

The second chapter of the CAC Bill lists the following offences as acts of cybercrime:

a) Unlawful securing of access;
b) Unlawful acquiring of data;
c) Unlawful acts in respect of software or hardware tool;
d) Unlawful interference with data or computer program;
e) Unlawful interference with a computer data storage medium or computer system;
f) Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices;
g) Cyber fraud;
h) Cyber forgery and uttering;
i) Cyber extortion;
j) Theft of incorporeal.

3.4.4 Kenya: The Computer and Cybercrimes Bill 2017.

a) Unauthorised access;
b) Access with intent to commit further offence;
c) Unauthorised interference;

d) Unauthorised interception;
e) Illegal devices and access codes;
f) Unauthorised disclosure of passwords or access code;
g) Cyber espionage;
h) False publications;
i) Child pornography;
j) Computer forgery;
k) Computer fraud;
l) Cyberstalking and cyber-bullying; and
m) Offences committed through computer systems.

3.5 Perpetrators of cybercrime:

The word hacker has been around since the 1960s, initially used to describe well-meaning and disciplined software and hardware experts. Lately, the term has taken on a more sinister and lessor constructive meaning and is used largely to refer to skilled computer experts who look to illegally gain access to systems and data.

Although neither of the terms, 'hacking' nor 'cracking' are defined in South Africa's ECT Act, its 2012 Amendment Bill, nor the CAC Bill of 2017, hacking can be described as unauthorised access to computers. The would-be perpetrator logs into a computer network, and gains entry to it without having the necessary authority to do so.[14] In South African law, hacking and similar computer-enabled criminal activities performed to gain illegal access to a computer, network, or data, are explicitly prohibited and outlawed by s86 and s87 of the ECT Act[15].

There is still no universally accepted definition for hackers and those that are adopted and used in common speak are inconsistent. Having regard for the core elements of hacking, namely innovative use of technology, eagerness to exploit

[14] B Gordon 'Internet Criminal Law' Available at, *http://www.legalnet.co.za/cyberlaw/cybertext/chapter15.htm*, accessed on 08 November 2017 para 426.
[15] Electronic and Communication and Transactions Act 25 of 2002.

systems vulnerabilities, and programming, the following definition of hacking is recommended:

> An activity which encompasses computer programming, circumventing security systems designed to protect computer networks and digital data stores, designing, and executing solutions to solve problems by combining software and hardware in unconventional ways, and modifying and re-purposing digital products of all kinds.[16]

3.5.1 Categories of hackers

Hackers, whether a lone hacker or affiliated to a group, can generally be categorised into three main categories, distinguished by their motivation, their intent and observed values when carrying out their cyber-attacks or circumventing cyber defence parameters.

White hats: This category of hackers are "ethical" hackers, driven by the need for good systems security. These individuals work within the laws of the hacker ethic (to do no harm), or as security experts. These are the so-called 'good guys' and are usually computer security experts or have extensive knowledge of that field.

Grey hats: This term was coined by L0pht – one of the best known old-school hacking groups. These hackers are reformed Black Hats, now working as security consultants. An alternate definition describes these hackers as those whose motives are unclear or may most likely change allegiance as they fall somewhere in between the White and Black hats.

Black Hats**:** Power, anger or hate motivates these hackers. They do not have any qualms about stealing or destroying data from networks that they penetrate. Their object is to illegally obtain access into systems and perform malicious and

---

[16] R Madarie, 'Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers' 11 (2017) *International Journal of Cyber Criminology*, 79.

criminal acts therein. These are the more sinister hackers who the term hacker generally applies to.

3.5.2 Why cyber-attack perpetrators commit acts of cybercrime

A study of cybercrime would not be complete without a cyber-criminal. To understand this calibre of criminal, it is essential to understand that, like many criminals who commit traditional crimes 'the production of crime requires the presence of both motivated offenders and suitable targets (individuals or their property), in the absence of effective guardians'[17]. Successful combating and prevention of cybercrime relies heavily on understanding the profile and motivation of the perpetrator seeking to overcome cyber defences. This is known as psychological incident handling.[18]

The driving and motivating factors that compel would-be perpetrators of cyber-attacks to carry out their illicit acts are complex, varied and not absolute. Various bodies of work were considered, but it was the 2001 hacker motivation table model[19] developed by Furnell that was preferred ahead of that of Ngafeeson, Herzberg and Cohen & Felson[20].

	Cyber-terrorists	Cyber Warriors	Hack-tivists	Malware Writers	Industrial	Phreakers	Samurai	Script Kiddies	Warez doodz
Challenge				✓		✓	✓		✓
Ego				✓		✓		✓	✓
Espionage		✓		✓	✓				
Ideology	✓	✓	✓						✓
Mischief				✓		✓		✓	

[17] M Ngafeeson ' Cybercrime Classification: A Motivational Model', 2009, available at *http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf* accessed on 10 November 2017.
[18] S Atkinson '*Psychology and the hacker – Psychological Incident Handling'*, 2015 available at *https://www.sans.org/reading-room/whitepapers/incident/psychology-hacker-psychological-incident-handling-36077* para 2 accessed on 10 November 2017.
[19] Hutchinson op cit (n5).
[20] Ngafeeson op cit (n17).

Money		✓		✓	✓	✓	✓		✓
Revenge	✓		✓	✓				✓	

Table 4. Adaptation of Furnell's - Hacker motivation table

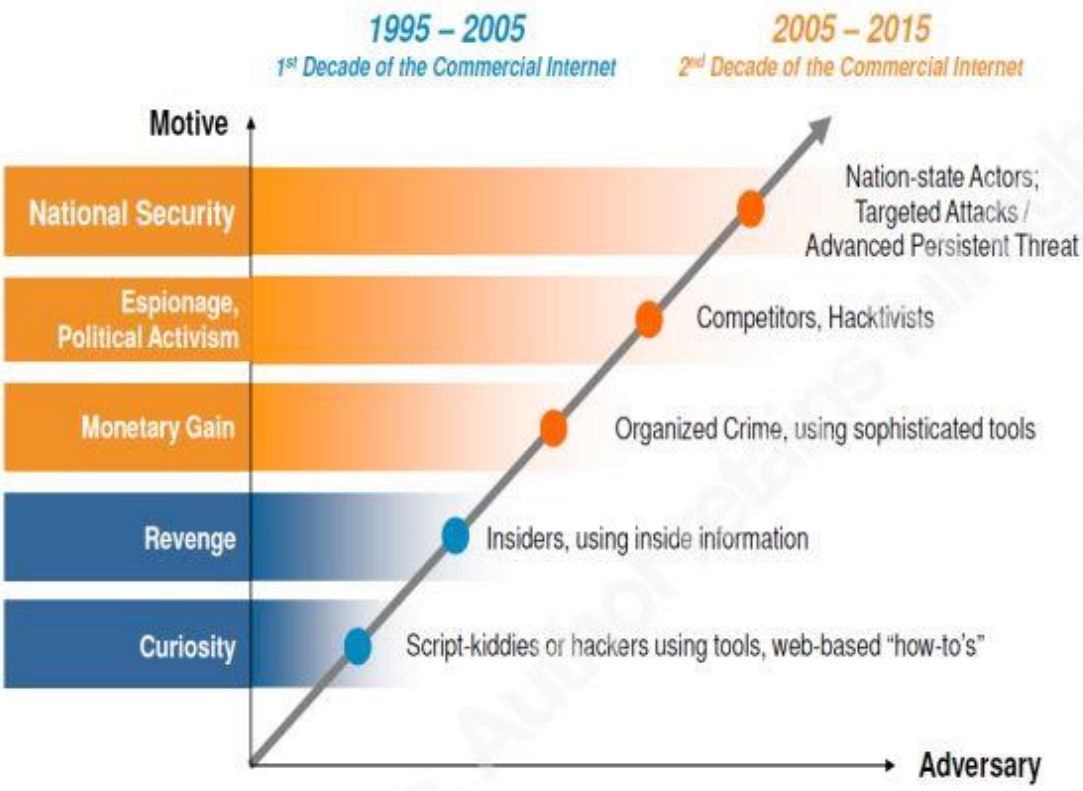
Having considered the driving values and factors that motivate cyber-attackers to carry out their cybercriminal activities, it is clear to see that there is seldom an attempted or completed cyber-attack without a motive. The following formula seeks to categorise and quantify the cost -versus -benefit decision evaluation considerations that a cyber-attack perpetrator will typically apply when deciding whether or not to proceed with a cyber-attack. For purposes of this dissertation, motive can be equated to a form of benefit in the following formula.

CI = (BV * AL) – (DV * RL)

'The equation looks at Criminal Intent (CI) equals the attained likelihood (AL) of a benefit value (BV) minus the realization likelihood (RL) for the anticipated disadvantage value (DV).'[21]

Graph 1 below, depicts how the hacker's motives and sophistication are evolving over time as the world becomes more persistently and ubiquitously connected.

[21] Atkinson op cit (n18) 14.



Graph 1: Evolving hacker motives[22]

3.5.3 Industries most targeted by cyber-attack perpetrators

A large extent of combating, preventing, or reducing the scourge of cybercrime in the digital era, has to do with understanding what it is that the cyber-criminals are after. Information is the lifeblood of nations, societies and organisations today. The format, reliance and value of the information may differ from country to individual to organisation but what is important to note is that not all the information will have the same value. Some will be deemed more important and useful than others. This is when the information becomes a critical asset and the organisation's 'crown jewels'[23] that are highly sought after by very motivated and well-funded adversaries ranging from competitors, nation states, and organised crime groups.[24]

---

[22] Atkinson op cit (n18)
[23] The Information Security Forum defines "Crown Jewels" as information assets of greatest value and would cause major business impact if compromised.
[24]Information Security Forum 'Protecting the Crown Jewels'2016, available at *https://www.securityforum.org/uploads/2016/09/ISF_Protecting-the-Crown-Jewels-Executive-Summary-final.pdf* accessed on 13 November 2017.

Personal information is the most sought after form of data. Incidents of identity theft are constantly rising (refer Table 5 below) from personally identifiable information, personal health information to personal finance information[25]. An assessment of the reported data breaches of the past three years indicates that the services and finance, insurance and real estate sectors[26] suffered the most breaches and that the leading form of data breach is theft of data[27].

Data breaches, 2014-2016

While the number of data breaches in 2016 remained fairly steady, the number of identities stolen increased significantly.

Year	Breaches	Identities stolen	Average per breach	Mega breaches
2014	1523	1,226,138,929	805,081	11
2015	1211	563,807,647	465,572	13
2016	1209	1,120,172,821	926,528	15

Table 5: 2016 Data Breaches[28]

The following is a list of the most traded illegally obtained personal information artefacts in the criminal underground economy for 2016, thanks to publicly accessible underground forums and Dark Web Tor sites:

1. Account details to access online entertainment and media platforms such as Netflix and Spotify;
2. Restaurant gift cards information;
3. Hotel bookings information;
4. Airline frequent flyer programme information;
5. Online banking account details;
6. PayPal account details;
7. Retail shopping accounts details (Amazon and Walmart);

---

[25] Symantec '2016 Internet Security Threat Report', 2017, available at *https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf*, 46 accessed on 18 November 2017.
[26] Ibid p48.
[27] Ibid p47.
[28] Ibid p45.

8. (Money laundering as a service) Illegal money transfer services, where inflated money transfers are made for nominal Bitcoin payments; and
9. Credit cards details

As at June 2017, more data had been lost or stolen in the first half of 2017 than in all of 2016. 'In total, 1.9 billion records were compromised as of the end of June 2017, compared to 1.37 billion in 2016.'[29] Table below illustrates this rise in breaches from 2013-2017[30]

BREACH SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Accidental Loss	8,488,082	6,580,674	4,523,689	305,300,000	33,976,668	231,233,179	258,617,400	33,302,653	1,627,637,633
Malicious Outsider	502,709,463	1,578,575,971	305,090,925	1,569,453,283	175,502,519	99,259,842	370,439,884	686,490,243	254,017,085
Malicious Insider	1,150,087	9,221,723	108,770,712	76,968,030	2,006,460	62,785,175	13,460,128	479,618	20,211,893
Hacktivist	777,216	98,730	7,000,096	1,182,007	561,918	30,011,904	11,453,685	918,179	0
State Sponsored	38	165,015	3,016,499	506,912,064	104,009,225	4,067,411	10,355,381	442,200	0
Unknown	72,780	4,745	1,307	0	391	200	950,000	0	0
TOTALS	513,197,666	1,594,646,858	428,403,228	2,459,815,384	316,057,181	427,357,711	665,276,478	721,632,893	1,901,866,611

Source: BREACHLEVELINDEX.COM

The second half of 2017 also saw South Africa experience it's largest data breach to date. It has been referred to as the Deeds-Master-Data-Breach and involved a breach of up to 66.3 million records of South African citizens' personal information. The latest assessment[31] indicates that of these 66.3 million records, 57 million were related to people marked as 'alive' and 9.3 million to people marked as 'deceased'. Worryingly, the data that was breached seems to indicate that the personal information of minors was also included.

Hacker Motive Summary

---

[29] L Irwin 'More data was lost or stolen in the first half of 2017 than all of 2016' *IT Governance Institute* 2017, available at *http://bit.ly/2EPoU1L*, accessed on 13 November 2017.
[30] Gemalto '2017 First Half Breach Level Index'2017, available at *http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf* accessed on 13 November 2017.
[31] T Hunt 'Questions about the Massive South African "Master Deeds" Data Breach Answered'2017, available at *https://www.troyhunt.com/questions-about-the-massive-south-african-master-deeds-data-breach-answered/* accessed on 13 November 2017.

The following decision chart[32] seeks to visually illustrate the process a cyber attacker typically follows before carrying out an attack and lists the considerations they would have to undertake before arriving at their ideal target by considering their motives, expertise and chosen target.

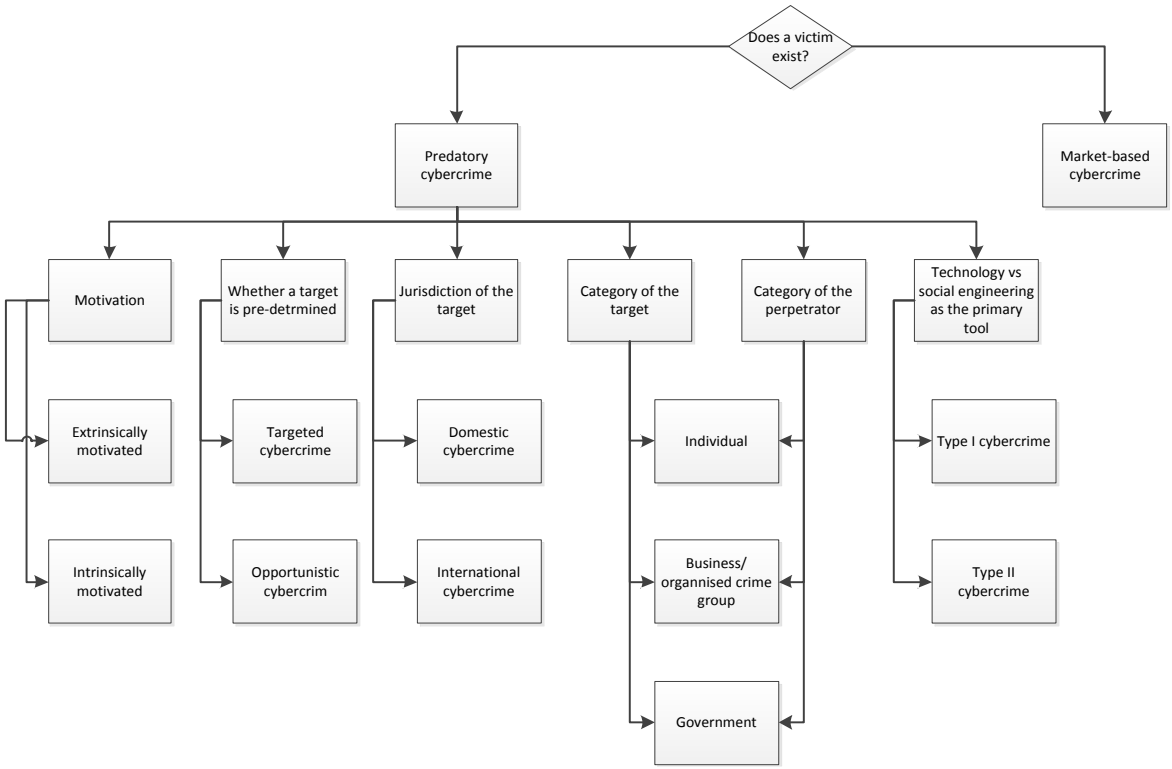


Diagram 1: Hacker attack decision chart by expertise, motive, and target.

[32] Kshteri op cit (n14) 45.

3.6 Counting the cost of cybercrime

Where there is a growing economy, bounds of capital infrastructure investments and a population explosion, cybercriminals are never far behind. They prey on developing countries where the risks presented by cybercrime are second to the need for connectivity and internet access. Typically, in nations such as these, the awareness to the threat of cyber risks ranges from low to non-existent due to the lax regulatory environment and low risk of prosecution. Cybercrime losses in the region have been on the rise as broadband connectivity increases. The lure of low-hanging fruits to be had explains the shift in cybercrime towards developing nations and emerging economies. The fact that the internet is now ubiquitous and easily accessible, means that countries, organisations and citizens alike, will generate volumes of personal, corporate, national, and military data that organised crime bodies will be drawn to. These cybercriminal outfits will stop at nothing and spare no costs in their pursuit of personal data, money, and intellectual property. The impact of cyber-criminal activities on the global economy is believed to equal that of that of counterfeit goods or the narcotics trade.[1]

According to the Norton Cybersecurity Insights Report of 2016[2] 8.8 million South African's fell victim to cybercrime that amounted to around R5.7 billion. In 2014, South Africa had the most cyber-attacks in Africa[3] and the centre for Strategic and International Studies[4] estimates that 0.14% of the South African GDP was lost to cybercrime related activities. It is no wonder then that cybercrime statistics recently posted by the South African Banking Risk Information Centre[5] report that South

---

[1] E Tamarkin, 'The AU's cybercrime response A positive start, but substantial challenges ahead'2015, available at, *https://issafrica.s3.amazonaws.com/site/uploads/PolBrief73_cybercrime.pdf* accessed on 19 April 2017.

[2] G Van Zyl '8.8 million South Africans hit by cybercrime - study' 2016, available at,*http://www.fin24.com/Tech/News/88-million-south-africans-hit-by-cyber-crime-study-20160707* accessed on 01 August 2017.

[3] N Davids 'SA is the leading target in Africa for cybercrime, warns legal firm' 2017, available at,*https://www.businesslive.co.za/bd/world/africa/2017-02-13-sa-is-the-leading-target-in-africa-for-cyber-crime-warns-legal-firm/* accessed on 01 August 2017.

[4] B O'Connor & V Moodley 'The Growing Need For Cybercrime Insurance In South Africa' 2016, available at,*https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2016/dispute/downloads/Dispute-Resolution-Alert-10-August-2016.pdf* accessed on 07 November 2017.

[5] Pay U 'SA companies under cyber-attack?' 2015, available at, *https://www.payu.co.za/press-room/sa-companies-under-cyberattack* accessed on 01 August 2017.

Africans lose in excess of R2.2 billion due to internet fraud and phishing attacks annually. 'Forbes has estimated the combined spending on cyber security of just a few major banks (J.P. Morgan, Bank of America, Citibank and Wells Fargo) was to the tune of US $500 billion in 2016.'[6] In 2013, Kenya lost an estimated $36 million to cybercrime (0.05% of GDP), which rose to $150 million in 2015. McAfee and the Center for Strategic and International Studies, reported in 2014 that the annual cost to the global economy from cybercrime is more than [US]$445 billion.[7]

Falling victim to cybercrime has become a real and costly threat to all so much so that business and consumers worry more about cybercrimes than about physical crimes.[8] The now retired former US director of the National Security Agency, Keith B Alexander, referred to loss of industrial information and intellectual property through cyber espionage as 'the greatest transfer of wealth in history.'[9] Even the most trusted system, once deemed impenetrable and totally secure, used to move trillions of dollars daily between banks (SWIFT) fell victim to cybercrime when one of its terminals[10] was hacked and $81million was stolen from Bangladesh central bank.

3.6.1 Analysing the cost of cybercrime

The phenomenon of cybercrime is new to most and still unfamiliar territory for many nations and industries. The details of how the cost and financial and/or fiscal impact of incidents of cybercrime is arrived at, is seldom disclosed, and/or

---

[6] India Ministry of Finance 'Report of The Working Group For Setting Up of Computer Emergency Response Team In The Financial Sector (Cert-Fin)' 2017, available at, *http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf* accessed on 18 November 2017.
[7] McAfee 'McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies' 2014 available at, *https://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx* accessed 20 November 2017.
[8] ThreatBrief 'Consumers worry more about cybercrime than physical crime' 2017, available at,*http://threatbrief.com/consumers-worry-cybercrime-physical-crime/* accessed on 04 December 2017.
[9] J Rogin 'NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history', 2012 available at,*http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/* access on 04 December 2017.
[10] T Bergin 'Costs of bank cyber thefts hit SWIFT profit last year' 2017, available at,*https://uk.reuters.com/article/us-banks-swift-cybercrime/costs-of-bank-cyber-thefts-hit-swift-profit-last-year-idUKKBN1910FX* accessed on 04 December 2017.

shared. This is largely because the methodologies and frameworks followed are still inconsistent, rudimentary, and ad hoc at best. Where organisations and countries have suffered from incidents of cybercrime, that data is seldom made public nor the details of what they considered when quantifying the impact and costs of the cybercrimes they have encountered. It is thus extremely difficult to arrive at a de facto and universally adopted framework or methodology without first concluding information sharing agreements, so that countries and/or organisations can develop their own bespoke models and algorithms to determine the actual or would be costs of incidents of cybercrime. Without industry/national data to model around and benchmark against, this is near impossible. It is for this reason that this dissertation will, through consideration of two different frameworks, determine how the cost of cybercrime is derived.

Analysing the cost of cybercrime: Model 1 - Academia

Driven by a desire to develop a framework that can be used to differentiate cybercrime costs from costs of other more traditional crimes and produce a more reliable, sound methodology that can be relied on for more accurate estimates of cybercrime losses using publicly available data, a team of information security economists from universities across the UK, Denmark, Netherlands, and the USA developed the 'measuring the cost of cybecrime' framework[11] which is referred to as Model 1.

Model 1 arrives at the cost or impact quantum of cybercrime by taking the following four categories and their components into consideration:

1. Criminal revenue**:** Gross receipts from a crime, where criminal revenue may comprise:
    a. Money withdrawn from victim accounts;
    b. Revenue to spammer for sending phishing mails
2. Direct losses: Losses, damage, or other suffering experienced by the victim as a consequence of a cybercrime. These may be:

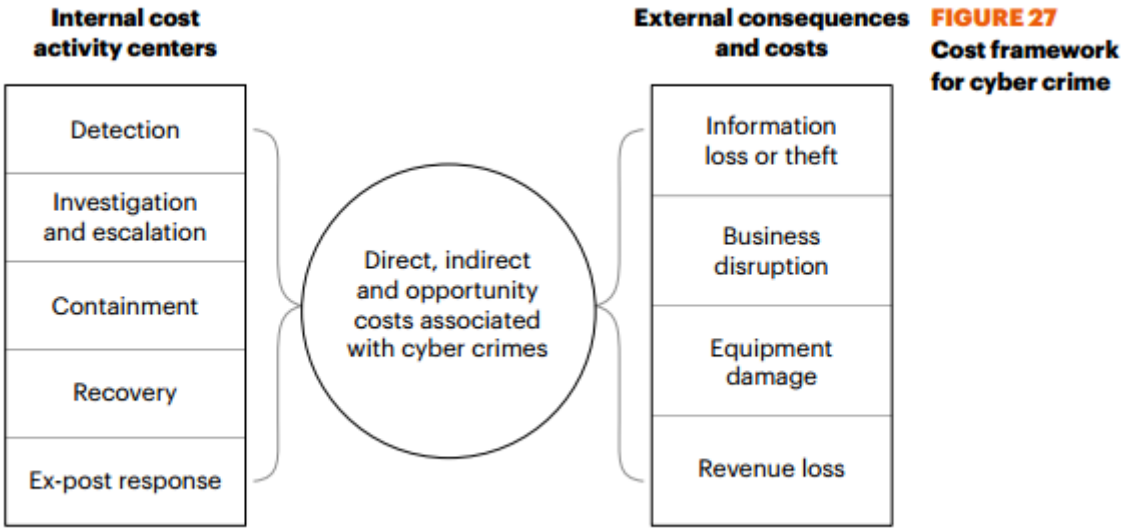
[11] R Anderson et al 'Measuring the cost of cybercrime' 2012, available at, *http://www.econinfosec.org/archive/weis2012/presentation/Moore_presentation_WEIS2012.pdf*, accessed on 04 December 2017.

   a. Criminal revenue loss;
   b. Time and effort to reset account credentials;
   c. Secondary costs of overdrawn accounts (deferred purchases);
   d. Lost attention and bandwidth caused by spam messages;
3. Indirect losses**:** losses and opportunity costs imposed on society as a result of an incident of cybercrime include:
   a. loss of trust in online banking;
   b. lost opportunity for banks to communicate via email;
   c. efforts to clean-up PCs infected with malware
4. Defence costs**:** the costs associated with of preventing future incident of cybercrime
   a. security products (spam filters, antivirus);
   b. services for consumers (training) & industry (‘take-down’);
   c. fraud detection, tracking, and recuperation efforts;
   d. law enforcement costs

Analysing the cost of cybercrime: Model 2 - Industry

Following up on the model developed by the Anderson and Moore, the Ponemon Institute and Accenture’s 2017 ‘Cost of cybercrime study’ framework (see Figure 1 below) will be considered as an alternate model to analysing and determining the cost of cybercrime. This model will be referred to as model 2**.** Unlike Model 1 which was develop using publicly available and published data of 2010/11, this model was developed by conducting field-based research that involved interviews with senior industry personnel about actual cybercrime incidents in 2017.

Figure 1: Cost of Cybercrime Framework



Like Model 1 the dimensions considered by Model 2 are centred around determining the direct costs, indirect costs, and opportunity costs as a result of, and associated with an incident of cybercrime. Model 2 will also consider the internal and external costs to be incurred after an incident of cybercrime. The internal costs consist of the costs associated with the detection of the incident and end with the costs related to the final agreed upon response to the incident, which involves quantifying the costs of the lost business opportunities and the business disruption.

External costs comprise the loss of information assets, business disruption costs, extent of equipment damage and revenue loss as captured using shadow-costing methods. Unlike model 1, model 2 assigns costs to the following discernible cyber-attack vectors[12]: viruses, worms, trojans; malware; botnets; web-based attacks; phishing and social engineering; malicious insiders; stolen or damaged devices; malicious code (including SQL injection); and denial of services. Figure 2 below refers.

[12] Accenture 'Cost of Cyber Crime Framework',2017 available at *https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf* accessed on 12 December 2017 p24.

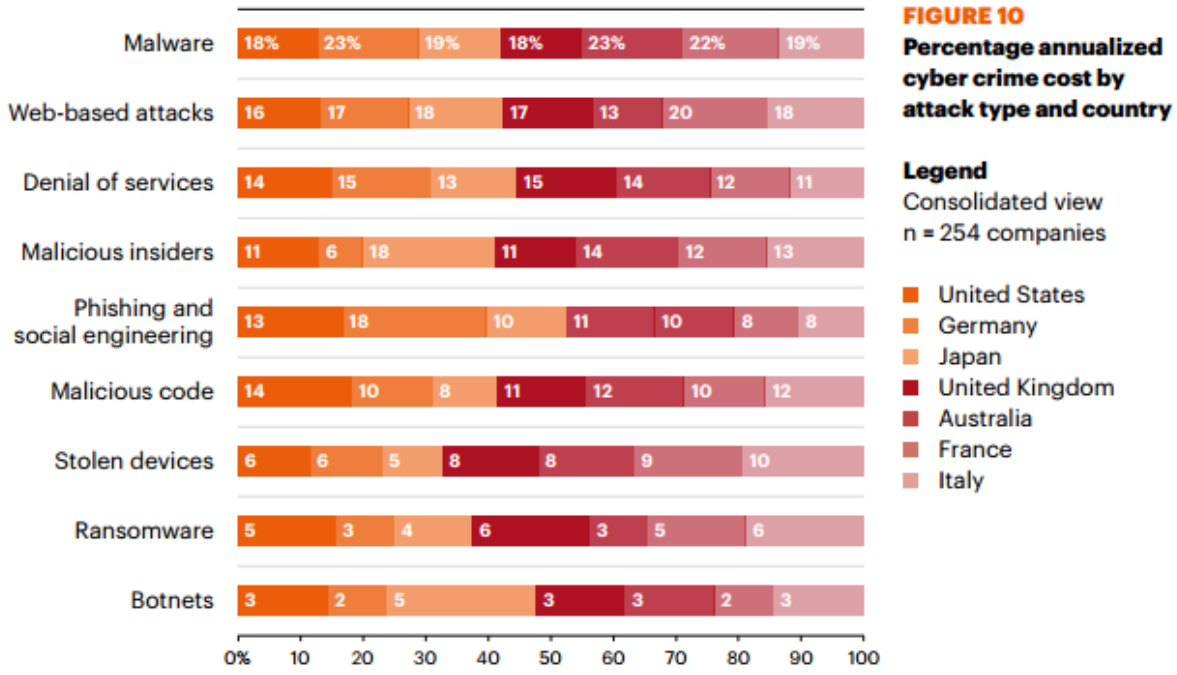


Figure 2: Cost of cybercrime by attack type and country

The five internal cost activity centers to consider as per this framework are as follows costs of early detection, investigation and escalation, containment activities associated with stopping or reducing the extent of a cyber incident or the advanced threat thereof, repairing and remediating the organization's systems and core business processes. These costs include the restoration of damaged information assets and other physical IT infrastructure assets. The costs of activities to help reduce the chances of a suffering from a similar cyber-attack in future are also borne in mind. They range from the costs of minimising business disruption and information loss, to future cybersecurity spend to enable newer technologies and strengthen controls systems.

In addition to the costs above, Model 2 also suggests consideration of the following external consequences or costs associated with the aftermath that sets after a successful cyber-attacks:

a) Quantifying the value of the lost sensitive and confidential information, and the costs of notifying the relevant parties and authorities about the data breach and extent of information wrongfully acquired.

b) The costs to recover from business disruptions or unplanned outages that prevent the organisation from meeting its data processing requirements.
c) Costs of restoring equipment and other IT assets, information resources and critical infrastructure.
d) Overall value of revenue lost and damage caused due to system delays or shutdowns.

An exact understanding of cybercrime is necessary in the fight against this epidemic. It is vital to know the difference between types of cybercrime, the classifications of cybercrime and the various categories of cybercrime. Without this knowledge and understanding it will be nearly impossible to correctly classify cyber incidents, to criminalise the ever changing forms of cybercrime and to sufficiently empower parties tasked with investigating and prosecuting the incidents of cybercrime.

It is equally important to understand the role players in the cyber-criminal arena and the markets they service with their ill-gotten gains. A definition of a hacker will go a long way in identifying common attributes and characteristics to be identified by. Understanding what motivates which cyber-attackers, their ideal targets, preferred attack conditions and their modus operandi is paramount to proactively thwarting their exploits or speedily resolving cyber-incidents. The age old business adage commonly attributed to Peter Drucker, “If you can’t measure it, you can’t manage it” rings especially true in the fight against cybercrime. Details of breaches and incidents of cybercrime are seldom released and made public for peer corporations, nations, and members of the public to improve their safeguards against this threat. It becomes extremely difficult to establish which sectors or nations are most at risk without information sharing. It is thus essential that incidents be costed and reported against. This will not only improve cyber security awareness postures but will also reduce the chances of success for cyber-attacks. Another benefit of reporting incidents of cybercrime is that the data can be used to establish whether the battle against cybercrime is indeed being won or not. The more nations, corporations and citizens report their breaches and incidents the more accurate the cost impact

frameworks will be and the more reliable the threat indicators and cyber resilience strategies will become over time.

4. SAFEGUARDING AGAINST CYBERCRIME

The Institute of Risk Management defines *'cyber risk'* as 'any risk of financial loss, disruption, or damage to the reputation of an organisation from some sort of failure of its information technology systems'[1]. Chapters two and three have thus far established that the likelihood and probability of a cyber-attack does not only threaten private corporations and businesses but that countries and sovereign states are equally susceptible to the threat.

4.1 Safeguarding the national critical information infrastructure from cyber risks

The government of Australia's definition of critical infrastructure is most appropriate for this dissertation. It progressively defines critical infrastructure as

> '[T]hose 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.' [2]

Systems, structures and physical places or areas that are of strategic interest to a country and are deemed vital to the country's safety, security, and the wellbeing of its citizens, are known as critical infrastructure. Disruption of a nation's critical infrastructure has the potential to undermine public safety, social order, and the fulfilment of key government responsibilities.[3] Such damage would generally be catastrophic and far-reaching. Sources of critical infrastructure risk could be natural (ie earthquakes or floods) or man-made (ie terrorism or sabotage).

---

[1] Institute of Risk Management 'Cyber risk and risk management' 2018, available at, *https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/* accessed 13 November 2017.

[2] The information sharing network 'What is critical infrastructure?' *Australian National Security* 2018, available at, *https://www.tisn.gov.au/Pages/Critical_infrastructure.aspx*, accessed on 18 November 2017.

[3] Organisation for Economic Co-operation and Development (OECD) 'Protection of 'Critical Infrastructure' And The Role Of Investment Policies Relating To National Security'2008, Available at,*https://www.oecd.org/investment/investment-policy/40700392.pdf* accessed on 18 November 2017.

Critical information infrastructure is a subset of a country's critical infrastructure that consists of vital interconnected information networks and systems that if disrupted or destroyed, the health, safety, security, and financial well-being of a country and the effective functioning of a government or economy would be severely hampered.[4]

4.1.1 National Policies, Strategies and plans to protect critical information infrastructure

It is paramount for the effective running of a country that the critical infrastructure be protected against all possible known risks. To achieve this will require the countries to adopt a risk management approach towards protecting their critical infrastructure. This approach will ensure that governments identify their key security assets, assessing their exposure to associated risks and develop appropriate controls to mitigate the risks. Protection of a nations critical information infrastructures, using the risk management approach, will require prevention, preparedness, response and recovery plans from the nations, their relevant agencies, and private sector operators of critical infrastructure facilities.[5]

When countries develop their national policy frameworks for critical infrastructure protection, they must ensure that the frameworks satisfactorily address all the major threats and ensure the coordination amongst all respondents (public and private, different levels of government and different sectoral responsibilities, diverse expertise). Countries should heed the UN General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other similar relevant resolutions, as they greatly assist with the development of strategies to secure national critical information infrastructure.[6]

---

[4] MN Njontini 'Protecting Critical Databases – Towards a risk based assessment of critical information infrastructures in South Africa' 2013(16) *Potchefstroom Electronic Law Journal* 453.
[5] OECD op cit (n3) 2.
[6] P Paganini 'G7 Declaration on responsible state behaviour in Cyberspace', para 6-7 2017, available at *http://securityaffairs.co/wordpress/57932/cyber-warfare-2/g7-declaration-responsible-states-behavior-cyberspace.html* accessed on 05 December 2017.

4.1.2 Critical Information Infrastructure Protection Structures: National Computer Security Incident Response team (nCSIRT)

In its 2015 report, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), encouraged states to establish a national Computer Emergency Response Team (CERT), a Computer Security Incident Response Team (CSIRT) or to officially designate an organisation to fulfil this role. These response teams are often the primary national point of contact for cyber incident response as they are tasked by the nation's cyber defence policy to issue alerts, warnings and to handle all matters relating to cyber threats and incidents, including the training of government constituents and cybersecurity stakeholders.[7]

National CSIRTs help coordinate cyber incident response at the national and international levels and are involved in devising and implementing national cybersecurity strategies. Their role is key in protecting the country's government networks, critical information infrastructure and critical infrastructure networks and facilitating information sharing and dissemination with all relevant stakeholders. Some act as a default operational response team that national and international stakeholders can turn to, when there is no other known contact in a country. The way in which the national CSIRT's are structured in terms of their authority, authorisation, functions and funding [8], varies by country. Some are positioned within governmental ministries, whilst others exist as non-governmental organisations or even independent governmental organisations. The ITU reported that in 2015 there were 102 countries that had either setup or formally recognised nCSIRTs.[9]

4.1.3 Critical Information Infrastructure Protection Structures: National cybersecurity centres

---

[7] India Ministry of Finance op cit (n6) 76.
[8] R Morgus et al 'National CSIRTs and Their Role in Computer Security Incident Response' 2015, available at http://bit.ly/2BDskCP accessed on 05 December 2017 5.
[9] Ibid, p8.

In line with the UN's creation of a global culture of cybersecurity and the protection of critical information infrastructures resolution 58/199, countries are setting up dedicated national cybersecurity centres (NSCS) or network security agencies that will mainly host the national cyber security incident response teams (nCSIRT) and all role-players required for the collective defence of the nation's cybersecurity. These centres are being setup as structures promised within the national cyber security policies.

4.2 Protection of national critical information infrastructure arrangements – SOUTH AFRICA:

4.2.1 National Strategy, Policy, and Regulatory Framework

The South African government has put in place the following policies for the safeguarding of it's critical information infrastructure:

i. South African Cybersecurity Policy;
ii. National e-Strategy; and
iii. National Cybersecurity Policy Framework as per Gazette No.39475 of December 2015

The safeguarding of critical information infrastructure is protected in law as codified in the following proposed and enshrined laws:

i. Section198 & s210 Constitution of RSA Act 108 of 1996;
ii. Section 17 Critical Infrastructure Protection (CIP) Bill 2016 –powers and duties of persons in control of critical infrastructure;
iii. Section 20,57 &58 Cybercrimes and Cybersecurity Bill 2017;
iv. Disaster Management Act 57 of 2002;
v. Section 53 Electronic Communications and Transactions Act 25 of 2002;
vi. Financial Intelligence Act 38 of 2001;
vii. Interception of Communications and Provision of Communication related Information Act, 2002;

viii. National Key Point Act 102 of 1980;
ix. National Strategic Intelligence Act 39 of 1994;
x. Non-Proliferation of Weapons of Mass Destruction Act 97 of 1993;
xi. Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; and
xii. Trespass Act 6 of 1959.

4.2.2 National Critical Information Infrastructure Security Structures

The following structures and arrangements in relation to the creation and operation of national critical information infrastructure structures for the South African government are in place:

i. Critical Infrastructure Council – as proposed by section 4 of the CIP Bill
ii. Cyber Response Committee – as proposed by section 53 of 2017 CAC Bill
iii. Cyber Security Centre – as proposed by per section 12(8) of CIP Bill
iv. Cyber Security Hub – as proposed by section54 of Cybercrimes Bill
v. The Electronics Communications Security – Computer Security Incident Response Team (ECS-CSIRT) – established by the State Security Agency in 2003
vi. National Computer Security Incident Response Teams - as proposed by section 52 of Cybercrimes Bill
vii. Private sector Computer Security Incident Response Teams - as proposed by section 55 of Cybercrimes Bill

4.3 Protection of national critical information infrastructure arrangements - KENYA:

4.3.1 National Strategy, Policy, and Regulatory Framework

The government of Kenya has the following strategy and policy framework in place for the protection of its national critical information infrastructure against the threat of cybercrime:

i. Kenya Vision 2030;
ii. National Cybersecurity Strategy, 2014;

iii. National Cybersecurity Masterplan;
iv. National Cybersecurity Framework, 2014;
v. National Certification Authority Framework;
vi. National Public Key Infrastructure Policy;
vii. Kenyan Information and Communications Technology Policy, 2006

The safeguarding of Kenya's critical information infrastructure is protected in law as codified in the following proposed and enshrined laws:

i. Information and Communications Act 2013;
ii. Kenya's National Security Intelligence Service Act 11 of 1998;
iii. Cybersecurity and Protection Bill 2016;
iv. Computer and Cybercrimes Bill 2016;
v. Critical Infrastructure Protection Bill;
vi. Data Protection Bill 2015;
vii. Finance Bill 2016.

4.3.2 National Critical Information Infrastructure Security Structures

The structures responsible for the cyber security and effective operation of Kenya's national critical information infrastructure structures are:

i. Communications Authority of Kenya;
ii. Kenya ICT Authority;
iii. National Security Council;
iv. The Kenya Computer Security Incident Response Team (CSIRT-Kenya);
v. National Computer Incident Response Team Coordination Centre (KE-CIRT/CC);

4.4 Protection of national critical information infrastructure arrangements – USA:

The USA has installed the following strategy, policy and regulatory frameworks have been installed to ensure the protection of national critical information infrastructure from cybercrimes:

4.4.1 National Strategy, Policy, and Regulatory Framework

i. Computer Fraud and Abuse Act of 1986;
ii. Cybersecurity Information Sharing Act of 2015;
iii. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001;
iv. Cyber Security Enhancement Act of 2002;
v. Cyber Research and Development Act of 2002;
vi. Homeland Securities Act of 2002;
vii. Federal Advisory Committee Act;
viii. Executive Order (EO) 13636[10] Improving Critical Infrastructure Cybersecurity;
ix. Presidential Policy directive (PPD) – 21;
x. Presidential Policy directive (PPD) – 24;
xi. Presidential Policy directive (PPD) – 41;
xii. National Information Infrastructure Protection Act of 1996;
xiii. National Infrastructure Protection Plan[11] : Partnering for Critical Infrastructure Security and resilience;
xiv. The Physical Protection of Critical Infrastructures and Key Assets;
xv. Framework for Improving Critical Infrastructure Cybersecurity;

4.4.2 National Critical Information Infrastructure Security Structures

It is from within the following structures and arrangements that the national critical information infrastructure of the US is situated and operated:

i. National Operations Center
ii. National Cybersecurity and Communications Integration Center (NCCIC)
    a. US Cyber Emergency Response Team (US-CERT)
    b. Industrial Control Systems CERT

---

[10] 'Improving Critical Infrastructure Cybersecurity Executive Order 13636' 2013, available at, *http://www.cyberriskinsuranceforum.com/sites/default/files/preliminary-cybersecurity-framework.pdf* accessed on 14 November 2017.
[11] 'National Infrastructure Protection Plan' *Department of Homeland Security* 2017, available at, *https://www.dhs.gov/national-infrastructure-protection-plan* accessed on 14 November 2017.

iii. Critical Infrastructure Cyber Community Voluntary Program (C^3VP)
iv. National Infrastructure Coordinating Center

4.5 Protection of national critical information infrastructure arrangements – UNITED KINGDOM:

To safeguard the national critical information infrastructure of the UK from cyber risks, the following strategy, policy, and regulatory frameworks have been developed:

4.5.1 National Strategy, Policy, and Regulatory Framework

Strategies and Policies

i. Counter Terrorism Strategy
ii. National Security strategy
iii. National Cyber Security Strategy
iv. National Risk Register
v. Financial Conduct Authority - CBEST Vulnerability Testing Framework

Legislation

i. Emergency Powers Act of 1920
ii. Computer Misuse Act of 1990
iii. Civil Contingencies Act of 2004
iv. Communications Act 2003
v. Security Services Act of 1989

Directives

i. The Network and Information Security Directive (NIS Directive)
ii. General Data Protection Regulation (GDPR)
iii. Payment Services Directive 2 (PSD 2)

4.5.2 National Critical Information Infrastructure Security Structures

It is from within the following structures and arrangements that the national critical information infrastructure of the UK is situated and operated:

i. National Cyber Security Centre
ii. Centre for the protection of National Infrastructure

4.6 Protection of national critical information infrastructure arrangements - INDIA

Efforts to protect India's national critical information infrastructure from cybercrimes are captured in the following strategy, policy, and regulatory frameworks:

4.6.1 National Strategy, Policy, and Regulatory Framework

Legislation

i. Information Technology Act 2000
ii. IT Amendment Act 2008
iii. The Data (Privacy and Protection) Bill, 2017

Strategies and Policies

i. National Cyber Security Policy 2013
ii. National Information Security Policy & Guidelines 2013
iii. Security and Privacy framework for Smart Cities 2016
iv. State Cyber Security Policies - Telangana and AP 2016
v. Guidelines for the protection of National Critical Information Infrastructure

4.6.2 National Critical Information Infrastructure Security Structures

The following structures and authorities are responsible for the protection of India's national critical information infrastructure from cybercrimes:

i. National Critical Information Infrastructure Protection Centre (NCIIPC)
ii. National Security Council (NSC)
iii. Indian Computer Emergency Response Team (CERT-In)

4.7 Safeguarding corporate mission critical information assets from cyber risks

4.7.1 Definition of Cyber Risks:

Having defined cyber risks from a point of view of nation states and their duty to protect their country's critical information infrastructure, the term is now defined for boards of directors and those entrusted with the duty of protecting a company's mission critical information assets from cybercrime. 'Cyber risk' is defined as 'the operational risk to information and technology assets that may affect the confidentiality, availability, or integrity of information or information systems.'[12] The incidents of cyber risks range from unauthorised access to the use or disclosure of regulated, protected or sensitive data.[13] Cyber risks may be categorised into four classes: 1) actions of people, 2) systems and technology failures, 3) failed internal processes, and 4) external events.[14]

An organisation that suffers a cyber risk incident may find itself liable for the costs and penalties associated with business disruption, financial loss, loss to stakeholder value, reputational harm, trade secret disclosure, competitive harm, legal non-compliance liability and civil liability to customers, business partners and other persons.

Despite the rise in reporting of high profile incidents of cyber risks around the world, directors remain uninformed about cyber risk management and their cyber risk responsibilities towards their companies. Studies in the UK reveal that only 5% of company boards regularly and thoroughly review their key information and data assets. Whilst only 1% are said to be fully informed and skilled in respect of cyber security.[15] Cyber risk events can halt operations, expose critical intellectual property,

---

[12] C Biener et al 'Insurability of Cyber Risks: An empirical analysis' (2015) *Institute of Insurance Economics* available at *http://bit.ly/2FeD6if* accessed on 28 December 2017 4.
[13] B Gervais 'Cyber Risk Management Guidance for Corporate Directors', 2017 available at, *https://www.lexology.com/library/detail.aspx?g=800d6480-500a-424d-839f-68879eb98637* accessed on 16 November 2017.
[14] Biener op cit (n12) 4.
[15] F Flockhart 'Cyber risk and directors' liabilities: an international perspective' 2016, Norton Rose Fulbright available at, *http://www.nortonrosefulbright.com/knowledge/publications/145122/cyber-risk-and-directors-liabilities-an-international-perspective* accessed on 16 November 2017.

and adversely affect the reputation of a company and its board. Furthermore, equity funds and companies considering acquisition and investment now take cyber preparedness into consideration, and a lack of planning can impact a company's value and potential sale price.

Duties of directors[16] are to be found in a company's memorandum of incorporation, the common law, codes of practice, and the Company's Act and other statues.

These duties owed to the company by the directors, as imposed by the common law are a fiduciary duty, requiring reasonable care skill and diligence.

A fiduciary duty simply means that a director of a company must exercise the powers and perform the functions of director in good faith and in the best interest or benefit of the company.[17] The director owes the duty to the company itself and not to shareholders or other stakeholders, and fault is not required to prove breach of duty. There are four fundamental fiduciary duties of director in common law. These are that directors may not (a) exceed their powers; (b) exercise their powers for an improper or collateral purpose; (c) fetter their discretion; or (d) place themselves in a position in which their personal interests conflict with their duties to the company.[18]

Where a director is in breach of a fiduciary duty, the company can remedy the breach through restitution to the company for the loss suffered by the company or the benefit gained by the director.[19]

Similarly, section 76 of the Company's Act requires a fiduciary duty, and a duty of reasonable care from directors. These are not all the duties expected of directors by the Companies Act but are the most applicable to the scope of this

---

[16] Director means any member of the board of a company, as contemplated is s66 or an alternate director of a company and includes any person occupying the position of a director or alternate director, by whatever name delegated, as defined in s1 Companies Act.
[17] W Geach 'Statutory, Common Law And Other Duties Of Directors' Available at *https://www.chartsec.co.za/documents/speakerPres/WalterGeach/GeachStatutoryCommonLawAndOtherDutiesOfDirectors.pdf* , 2009, accessed on 11 February 2018.
[18] Duties of Directors and Officers Fiduciary Duties (4) *SALJ* 2
[19] N Bouwman 'An Appraisal of the Modification of the Director's Duty of Care and Skill' 4 *SA Mercantile Law Journal* 21 (2009) 510-511.

dissertation. The directorial duties pertaining to conflict of interest (s75) and indemnities and insurance (s78) will not be discussed further. The duties regarding directors' liability (s77) will be discussed in later sections to follow.

The key functions of a governing body, according to the King IV Code[20] are 1.) to steer the organisation and set its strategic direction; 2.) to approve policy and planning that give effect to the set strategy and direction; 3.) to oversee and monitor implementation and execution by management and 4.) to ensure that there is accountability for organisational performance.

4.7.2 Common law duty of care

The common law duty of care requires directors to act with the required degree of care and skill. The standard of 'care' and 'skill' is not prescribed in the common law. Establishing that a director acted with required 'care' can to some degree be proven objectively whereas establishing the discharge of the required 'skill' will vary depending on the nature of the business, obligations assigned, and if they are an executive or a non-executive director. Directors are expected to exercise the care that can reasonably be expected of a person with their knowledge or expertise and as such are justified in trusting and rely on the judgment, information, and advice of management, provided due consideration was given to the information and their own judgment applied accordingly.[21]

In Terms of s60[22] of the Banks Act of 1990[23] and the banking regulations[24], the directors of a bank owe a greater duty of skill and care than that owed, under the

---

[20] Institute of Directors in Southern Africa (IODSA) '*King IV Report on Corporate Governance for South Africa*' (2016) 21.
[21] Bouwman op cit (n19) 510-511.
[22] S60 Banking Act "fiduciary relationship" must be interpreted as acting in the "best interests and for the benefit of the bank and its depositors".
[23] The Banks Act 4 of 1990.
[24] The Banks Regulations (published in Government Gazette no. 21726 of 8 November 2000.

common law, by the directors of other companies. The fiduciary duty and duty of skill and care owed by the directors of a bank is also owed to its depositors.[25]

Where a director is charged with a breach of the common law duty of care in the discharge of his duties, the company's cause of in delict. This action requires the company to satisfactorily establish the existence of the following elements of delict: conduct (can either be an act or an omission), wrongfulness, fault (in the form of intent or negligence), causal connection between the wrongful act or omission and the damage suffered, and the resulting loss or damage suffered because of the conduct of the director. The remedy for breach of the duty of care is delictual damages recoverable by the company and not based on restitution in *integrum*. [26]

4.7.3 Duty to discharge the duty of care and skill

Section 76(3) of the Companies Act of 2008 partially codifies the common law duty of care and skill and in so doing leaves room for the common law to still be developed further and even apply to matters not foreseen by drafters at time of codification. Determining a breach of duty of skill and care has come a long way from the lenient approach under the common law that relied on subjectively proving the director's intelligence and experience. The shortfall of this test was that nothing less than the most gross or negligence would lead to a finding that a director was in breach of his duties. This test has since been revised to be inclusive of both the objective and subjective elements to suit the partially codified dispensation.[27]

Section 77(2)(a) of the Act state that a director of a company may be held liable (in accordance with the principles of the common law relating to the breach of a fiduciary duty) for any loss, damages or costs sustained by the company due to a

---

[25] C Tucker 'Greater duty of skill by the directors of a bank' 2003, available at *http://www.bowmanslaw.com/insights/greater-duty-of-skill-by-the-directors-of-a-bank/*, accessed on 12 February 2018.
[26] Ibid.
[27] Bouwman op cit (n19) 532.

consequence of any breach by the director of the duties contemplated, inter alia, in s76.

Similarly, section 77(2)(b) Act[28] provides that a director of a company may be held liable based on common law principles relating to delict for any losses or damages which the company may suffer due to a breach of the duty of care and skill in terms of s76(3)(c), losses due to a breach of a provision of the Act not mentioned in s77 and losses due to the contravention of any provisions of the memorandum of incorporation (MoI) of the company.[29]

The basis of the liability of a director to the company for injuries suffered to its interests, listed in s77(3)(a)- (e) in some instances combine consequences for violations of both a fiduciary duty and a duty of care, skill, and diligence. South African law allows the same facts to give rise to a claim for damages in delict as well as in contract and allows the plaintiff to choose which to pursue. [30]This is known as a *concursus actionum* which only exists where the independent requirements of both a contractual and a delictual action are present. In the case of *Loureiro v iMvula Quality Protection (Pty) Ltd*[31] the Constitutional Court unanimously upheld both claims in contract and delict holding that the defendant had acted negligently and wrongfully in a delictual sense.[32]

These cyber risk management duties of the board may also stem from stock exchange listing requirements, industry regulators, self-regulatory organisations or even codes of practice. Where the views expressed by regulators, organisations and associations might not have the force of law, they may be relied on by courts in determining the standard of reasonable care, skill and diligence required of corporate

---

[28] S76 -77, Companies Act 71 of 2008.
[29] R Stevens 'The legal nature of the duty of care and skill': Contract or Delict', 2016, 19 *PER* 42.
[30] B Mupangavanhu 2016 '*Directors' Standards of Care, Skill, Diligence, And The Business Judgment Rule In View of South Africa's Companies Act 71 of 2008: Future Implications For Corporate Governance*' 192.
[31] *Loureiro v iMvula Quality Protection (PTY) Ltd 2014 3 SA 394 (CC).*
[32] A Price 'The contract/delict interface in the Constitutional Court' 2014 25 *Stellenbosch Law Review* 501.

directors regarding the management of a corporation's cyber risk. Similarly, the King IV Code on Corporate Governance charges the governing body 'to govern risk in a way that supports the organisation in setting and achieving its strategic objectives'[33] and to oversee that the 'integration of technology and information risks into organisation-wide risk management.'[34]

4.7.4 Consequences of breach of duty of care by directors

The scope of this discussion on the consequence that may befall a director found to have breached their duty of care and skill in terms of the Companies Act does not include discussions of penalties applicable to a director of a company that is insolvent, entering business rescue or that was liquidated.

Directors of a company may be removed, statutorily, by shareholders, directors, and other parties catered for in law and/or the company's memorandum of incorporation (MOI)[35] such as the Companies Tribunal (Tribunal).

Section 71(1) allows for company directors elected to the board and found to have failed in their discharge of the duty of care and skill to be removed. Their removal may be by way of an ordinary resolution of shareholders in a general meeting. *Ex-officio* directors can only be removed by the board or the Companies Tribunal (Tribunal) provided they were given prior notice of the meeting and an opportunity to make representations.[36] A director may also be removed at the insistence of directors according to s71(3). The allegations against him must satisfy the board.

---

[33] IODSA (n20) Principle 10.
[34] Ibid, Principle 12.
[35] 'Removing a Director Under the Companies Act 71 of 2008' 2015, available at, *http://www.polity.org.za/article/removing-a-director-under-the-companies-act-71-of-2008-2015-06-30*, accessed on 11 February 2018.
[36] S71(2) of Companies Act.

Directors who have been appointed to the board by specific persons, can only be removed only by those persons, the board or the Tribunal[37]. Shareholder-appointed directors can be removed by the shareholders, the board, or the Tribunal. s71(8) provides that Tribunal removals are available only where the board consists of 'less than three members', whilst s71(3) provides that board removals are available only where the board has more than two members.[38]

Removal of directors at the instance of directors or a shareholder alleging ineligibility or disqualification[39] in terms of s69, may take place where the grounds for disqualification are a court order prohibiting a person from being a director or a declaration that they are delinquent as per s162. In the case of *Msimang NO and another v Katuliiba and others*[40] and that of *Cape Empowerment Trust Limited v Druker and others*[41], the courts confirmed the requirements for directors to be declared delinquent as contemplated in section 162 (5)(c)(iv)(aa). Furthermore, the court held in the case of *Kukama v Lobela and Others*[42] that once a director has been declared a delinquent the court does not have to order their removal, it follows automatically. Other grounds for removal due to insistence of directors or a shareholder are, inability to perform a director's functions, negligence (determined using s76) or dereliction of duties.[43]

Although the plaintiff faces high costs and difficulty in accessing to company information required to support the claim[44], a derivative action is one of the ways a shareholder, or a person listed in s165(2) of the Act, may redress the wrongs committed against the company when those in control of the company refuse to do

---

[37] Ibid at Section 66(4)(a)(i).
[38] C Ncube 'You're Fired! The removal of directors under the Company Act 71 of 2008' *SALJ* (2014) 39.
[39] S71(3)(a)(i) Companies Act.
[40] Msimang NO and another v Katuliiba and others [2013] JOL 30522 (GSJ).
[41] Cape Empowerment Trust Limited v Druker and others [2016] JOL 36987 (WCC).
[42] Kukama v Lobelo and Others (38587/2011) [2012] ZAGPJHC 60.
[43] Ncube op cit (n38) 39.
[44] MF Cassim 'The statutory derivative action under the Companies Act of 2008: Guidelines for the exercise of the judicial discretion' (2014) available at *https://open.uct.ac.za/bitstream/item/13147/thesis_hum_2014_cassim_mf.pdf?sequence=1*, accessed on 12 February 2018.

so. It also acts as a deterrent for directors not to abuse their duties to the detriment of a company. Public enforcement is a remedy for a person without the financial means a claim that can be used to bring the claim by a person without the financial means to access the courts and to secure access the required company information.[45]

For a derivative action, a minority shareholder/s or other stakeholder/s must serve a demand on a company. The case of *Mouritzen v Greystone Enterprises (Pty) Ltd and another*[46] held that any legally recognisable manner of service of any court process or document initiating proceedings shall be adequate service.

If the company does not challenge the demand or when the court does not set aside the demand, the company must appoint an independent person or committee to investigate the demand. Within 60 days of being served, the company must either initiate or continue legal proceedings, protect the legal interests of the company as contemplated in the demand, or serve a notice on the person who made the demand, refusing to comply with it.[47]

The court will thereafter exercise its discretion as per s165(5) to grant the person who served the demand the right to institute or continue legal proceedings.

Removal of directors by the Companies Tribunal as per s71(8) are restricted to companies which have between one and three directors. Any shareholder or director may apply to the Tribunal to decide whether a director should be removed on the grounds listed in s71(3).[48]

---

[45] Ibid 190.
[46] Mouritzen v Greystone Enterprises (Pty) Ltd & Another (10442/2011) [2012] ZAKZDHC.
[47] S Stadler & R Kok 'Protecting your rights as a minority shareholder in South Africa: The derivative action'(2015) available at *http://www.puleinc.co.za/publications/protecting-your-rights-as-a-minority-shareholder-in-south-africa-the-derivative-action/,* accessed on 12 February 2018.
[48] Ibid 44.

Criminal proceedings may be instituted against a company as per s332(1) of the Criminal Procedure Act[49]. A company can be prosecuted for any common law offence. This section 'caters for all types of criminal activities by corporations, including those that require *mens rea* in the form of negligence'[50], and it makes provision for acts or omissions instructed by a director or servant of that corporate body during the performance of their duties to further the interests of the corporate body. The act or omission is deemed to be performed by the corporate body and no intent is required.

4.7.5 Defences and remedies available to directors charged with breach of duty of care:

A director who is removed from office in terms of s71, by a board or the Tribunal, or person who had directly appointed him to the board, has 20 business days to take the matter on court on review. Any director who voted in favour of the resolution to remove or retain a director concerned, or any shareholder who has voting rights in the election of that director, can also bring matter to court on 'review'.

A director who has a fixed term appointment but is removed from office by an ordinary resolution of the shareholders before the expiry of that term and has not given the company cause to terminate the contract, may have a claim for damages against the company for breach of contract. As an executive director may resign from a directorship but still retain employment by the company a simultaneous termination of that director's employment would constitute a dismissal. In cases of unfair dismissal, the most appropriate remedy is usually an award of damages as the courts have stated that the remedy of reinstatement is unlikely to be granted.[51]

---

[49] Criminal Procedure Act 51 of 1977.
[50] DM Farisani 'Corporate Criminal Liability for Deaths, Injuries and Illnesses: Is South Africa's Mining Sector Ready for Change?' 2015 available at *https://www.moneyweb.co.za/wp-content/uploads/2015/11/Corporate-Criminal-Liability-for-Deaths-Injuries-and-IllnessArticleby-DM-Farisani.pdf*, accessed on 12 February 2018.
[51] Ncube op cit (n38) 46-48.

Section 77(9) states that in any proceedings against a director, other than for wilful misconduct or wilful breach of trust, the court may relieve the director, either wholly or in part, from any liability, if it appears to the court that the director has acted honestly and reasonably.[52]

The business judgement rule (BJR) has been codified into South African law as per s76(4) of the Act. This rule, of American origin, states that an officer or director of a corporation is not liable for acts of mere negligence as the court will not interfere with the business judgement of directors where fraud, bad faith or lack of care is absent. However, the interpretation and application of this rule has not been tested by the courts.[53] The BJR thus seeks to ensure that decisions made by directors, provided they meet set criteria, are protected even though, the decisions prove to be erroneous. Courts have long maintained that 'directors may exercise their discretion bona fide in what they consider not what a court may consider is in the interests of the company.'[54]

In the event of a derivative action, s165 (3) provides that when a demand is served on the company, the company has 15 business days to apply to court to have the demand set aside on the basis that the demand is frivolous, vexatious or without merit.

A company is entitled to take out indemnity insurance to protect a director (barring the situation where the director is convicted of an offence or the director acted in the name of the company and signed on behalf of the company and

---

[52] 'Directors liability Booklet' *Werksmans Attorneys* 2013, available at, *https://www.werksmans.com/wp-content/uploads/2013/04/Werksmans-Directors-Liability-Booklet.pdf* , accessed on 12 February 2018.
[53] H Stoop 'The business judgment rule: how the Companies Act of 2008 is impacting on directors' duties'2012 129(3) *SALJ* 547.
[54] B Mupangavanhu 2016 'Directors' Standards of Care, Skill, Diligence, And The Business Judgment Rule in View of South Africa's Companies Act 71 of 2008: Future Implications For Corporate Governance' 58.

purported to bind the company without the necessary authority). The company may also indemnify itself against expenses advanced to a director in terms of such indemnity and accordingly, in terms of s78, indemnity also applies to former directors of the company and allows for restitution claims from directors.[55]

Cyber Risk Management Duty: Analysis by country.

The question being addressed by the table below is whether there exists a fiduciary duty, at director level to manage the cyber risks of a company and if directors may face liability from a failure to discharge such a duty according to the various company and IT laws, sector regulations and exchange requirements of the subject nations. The form of cyber risk used for comparison in the table is that of a data breach.

	FIDUCIARY DUTY OF REASONABLE CARE	BREACH DISCLOSURE REQUIREMENT	LISTING /SECTOR REQUIREMENT	LEGISLATION	SHAREHOLDER LITIGATION	CYBER-RISK CASE LAW
USA	Y	SEC – Cyber Disclosure Guide[56] FINRA[57]	43 cybersecurity requirements applicable to financial services[58]	s141 (a) Delaware General Corporation law Gramm-Leach Bliley Act	- Y – (s11) & (s15) Securities Act. (s14) & (s20) Securities Exchange	Stone v Ritter

[55] W Smit 'Companies Act 2008 – Directors' Responsibilities and Liability' 2011 available at *https://www.exceedinc.co.za/news/companies-act-2008-directors-responsibilities-and-liability/?id=8&entryId=13*, accessed on 12 February 2018.
[56] 'CF Disclosure Guidance: Topic No. 2', *U.S. Security and Exchange Commission* 2011, available at, *https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm* accessed on 16 November 2017.
[57] 'Cybersecurity, Financial Industry Regulatory Authority'2015, available at, *http://www.finra.org/industry/cybersecurity*, accessed on 20 November 2017.
[58] R Frierson, 'Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security' 2017, available at, *https://www.federalreserve.gov/SECRS/2017/May/20170518/R-1550/R-1550_021717_131709_429070260162_1.pdf* accessed on 16 November 2017.

	FIDUCIARY DUTY OF REASONABLE CARE	BREACH DISCLOSURE REQUIREMENT	LISTING /SECTOR REQUIREMENT	LEGISLATION	SHAREHOLDER LITIGATION	CYBER-RISK CASE LAW
			FFIEC[59] (s17) SEC Act FSSCC: Enhanced Cyber Risk Management Standards[60] NY: DFS Cybersecurity regulation[61]	Health Insurance Portability and Accountability Act (HIPAA) Health Information Technology for Economic and Clinical Health Act (HITECH)	Act. Securities class action - Y – Rule 23.1 Delaware Chancery Court Derivative action	
UK	Y	General Data Protection Regulation (*679/2016/EU*) (GDPR),	Network and Information Security Directive (*2016/1148/EU*) (NIS Directive)	(s172 & 174) - UK companies Act 2006 (s105A) Communications Act 2003	Y – Derivative Action	Google Inc v Vidal-Hall Penalty: [62] Sony

[59] 'Financial Institutions Examination Council' 2017, Available at, *https://www.ffiec.gov/* accessed on 16 November 2017.
[60] 'Enhanced Cyber Risk Management Standards' *Financial Services Sector Coordinating Council* 2017 Available at, *https://www.federalreserve.gov/SECRS/2017/February/20170221/R-1550/R-1550_021717_131709_429070260162_1.pdf* accessed on 13 December 2017.
[61] MT Vullo 'Cybersecurity Requirements For Financial Services Companies' *New York Department of Financial Services* 2017, available at,*http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf* accessed on 16 November 2017.
[62] 'ICO fines Sony £250,000 for failure to prevent hacking on Sony PlayStation Network Platform, by PLC IPIT & Communications', 2013 available at, *https://uk.practicallaw.thomsonreuters.com/5-523-7306?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&comp=pluk* accessed on 16 November 2017.

	FIDUCIARY DUTY OF REASONABLE CARE	BREACH DISCLOSURE REQUIREMENT	LISTING /SECTOR REQUIREMENT	LEGISLATION	SHAREHOLDER LITIGATION	CYBER-RISK CASE LAW
		Draft Payment services 2 Directive	Draft Digital Economy Bill in October 2016	Data Protection Act		
RSA	Y	(s22) Protection of Personal Information Act 3 of 2013 (POPI)	FSB[63] - Governance and operational standard for insures 3	- Companies Act 2008 - PoPI Act	- (s165) Derivative Action: Companies Act - (s77) Liability of directors: Companies Act	None – Holtzhausen v ABSA Bank Ltd
KENYA	Y	(s31) Cybercrime and Computer related crime Bill Data Protection Bill	Central Bank of Kenya [64]	(s145) - Kenya Companies Act 2015	(s165) Derivative Action: Companies Act	Ajay Shah v Trust Bank
INDIA	Y*common law duties excluded	Not required by national ITA 2011	IRDA[66] SEBI-Principle 17 of PFMI	- (s166) - India Companies Act 2013	- Y - (s245) Derivative Action Companies Act	None: C.M.Philip vs The Registrar

[63] Insurance Bill 2016: Proposed Governance and Operational Standards for Insurers.
[64] V Juma 'CBK tells banks to boost cyber crime protection' 2017, available at, *http://www.businessdailyafrica.com/news/New-cyber-crime-rule-for-commercial-banks/539546-3981762-12c4in7/index.html* , accessed on 21 November 2017.
[66] Guidelines on Information and Cyber Security for Insurers – issued as per s14(1) IRDA Act 1999

	FIDUCIARY DUTY OF REASONABLE CARE	BREACH DISCLOSURE REQUIREMENT	LISTING /SECTOR REQUIREMENT	LEGISLATION	SHAREHOLDER LITIGATION	CYBER-RISK CASE LAW
		or Data Privacy Rules[65]. Sectoral requirement for banking and insurance sectors.	FSDC	- (s14(1)) – IRDA Act - (s43A) – IT Act 2000	- Y – (s85) Information Technology Act 2000	Of Co-Operative Societies [67] Mobikwik[68]

An analysis of the subject nations IT laws and sectoral regulations regarding directors' duties and management of cyber risks, mainly data breaches, indicates that all the nations analysed have legislated the fiduciary duty for directors to manage their organisations cyber risks with the required reasonable care and skill. This duty of care extends to directors in all jurisdictions[69], except India, to disclose after occurrences of a data breach. In the case of India, the duty to disclose after a data breach is limited to and only regulated within the financial services, banking, and the insurance sectors. Provisions to hold directors liable after data breaches and similar instances where they failed to manage cyber risks, are available in the legislation of all countries studied. These range from securities class actions to derivative actions and common law liability. Despite having codified legislation to compel directors to manage cyber risks with all due care, very few nations have case law to this effect, where directors were prosecuted for breach of duty of care and skill over the

[65] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[67] Kerala High Court, C.M Philip vs The Registrar of Co-Operative, 2013, available at, *https://indiankanoon.org/doc/16257664/* accessed on 5 December 2017.
[68] Developing case involving mobile money platform and all banks in India, October 2017, available at *https://economictimes.indiatimes.com/small-biz/startups/mobikwik-glitch-cops-track-those-who-transferred-funds/articleshow/60898149.cms* accessed on 5 December 2017.
[69] Once fully enacted and in force, section 22 of the Protection of Information Act will require that the information regulator in South Africa, be notified of breaches involving personal information.

management of a company's cyber risks. It is only the USA and the UK where this precedent exists.

4.7.6 Board cyber risk oversight duties:

Discussed below are a set of recommended cyber risk duties for boards of directors to consider, as framed by leading scholars[70] of enterprise risk management:

Directors should, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives, and risk managers, are consistent with the company's strategy and risk appetite; that these policies and procedures are functioning as directed; and that necessary steps are taken to foster an enterprise-wide culture that supports appropriate risk awareness, behaviours and judgments about risk and recognises and appropriately escalates and addresses risk-taking beyond the company's determined risk appetite.

The board should be aware of the type and magnitude of the company's principal risks and should require that the CEO and the senior executives be fully engaged in risk management.

The board should regularly review court decisions, regulations, and keep abreast of industry standards and best practices. Boards must hold frequent meetings to analyse cyber risks and develop potential mitigating plans of actions. They should create or appoint a committee to review cyber issues and/or investigate data incidents and breaches. Boards must work with risk management to implement a monitoring, compliance, and risk management programme, oversee the execution of the programme, and investigate possible violations.[71]

Through its oversight role, the board can send a message to management and employees that comprehensive risk management is not an impediment to the conduct

---

[70] Lipton M, 'Risk Management and the Board of Directors', *Harvard Law School*, 2017 available at, *https://corpgov.law.harvard.edu/2017/02/15/risk-management-and-the-board-of-directors-4/* accessed on 02 November 2017.

[71] R Sarkar 'Four Key Cyber Risk Management Questions for Directors and Officers' 2017, available at, *http://www.rmmagazine.com/2017/09/01/four-key-cyberrisk-management-questions-for-directors-and-officers/* accessed on 15 November 2017.

of business nor a mere supplement to a firm's overall compliance programme. Instead, it is an integral component of strategy, culture, and business operations. The board should ensure that the company has comprehensive cyber liability insurance coverage. [72]

4.7.7 Failure to discharge the duty to manage cyber risks:

Where directors fall short of the expected standard of due care and fail to adequately address cyber risks facing their companies they may be subject to litigation, regulatory and shareholder criticism and exposure should a successful cyber-attack or breach occur.[73]

In the UK in 2015, shareholders of Home Depot, sued 12 company directors and officers in a derivative action lawsuit, for breaching their fiduciary duties of loyalty, good faith, and due care by knowingly and consciously disregarding their duties and failing to ensure that Home Depot took reasonable measures to protect its customers' personal and financial information. Should this action succeed Home Depot will need to change its governance structure, reorganise risk management entities, and pay the shareholders' attorneys more than $1 million, among other costly and time-consuming charges.[74]

---

[72] Ibid.
[73]'Cyber Risks: Board responsibilities' *Vorys* 2014, available at, *https://www.vorys.com/publications-1316.html* accessed on 15 November 2017.
[74] Sarkar op cit (n71).

Types of cyber liability exposure

As established in the section on 'counting the cost of cybercrime' and as advised by the Insurance Information Institute[75], businesses may in the event of cyber-attack, be exposed to the following costs against them and their directors:

1. Liability: Business may be liable for costs incurred by customers and other third parties as a result of a cyber-attack or another IT-related incident.
2. System and/or Data recovery: Repairing or replacing computer systems or lost data can result in significant costs. In addition, companies may not be able to remain operational while their systems are inaccessible, resulting in further revenue loss.
3. Breach notification expenses—In certain jurisdictions, if a business stores customer data, it is required to notify customers if a data breach has occurred or merely just suspected. This can be costly, especially if there are many customers.
4. Regulatory fines and Penalties: Several sector regulations require businesses and organisations to protect consumer data. If a data breach results from a business's failure to meet compliance requirements, the business may incur substantial fines.
5. Class action lawsuits: Large-scale data breaches have led to class action lawsuits filed on behalf of customers whose data and privacy were compromised.
6. Shareholder liability**:** for failing to prevent the data breach or properly disclosing the cyber risks.
7. Reimbursement and/or reissuance: to customers for fraudulent transactions
8. Businesses may also need to financially recover from reputational harm to their brand, theft of trade secrets, cyber extortion and network or business interruption depending on the form of cybercrime they suffered, its impact and the extent thereof.

[75] 'Cyber liability risks' 2017 *Insurance information Institute*, available at, *https://www.iii.org/article/cyber-liability-risks* accessed on 15 November 2017.

4.7.8 Cyber liability insurance

Cyber insurance taken out by business should at the least cover the business in terms of the cyber liabilities the business may be exposed to, as discussed above. The market for cyber insurance policies is still in its infancy and policies have not yet been standardised, care should be taken to find someone with experience, such as an insurance agent or attorney who can assist with the negotiation and review of the cyber insurance policies being considered.[76]

Types of cyber insurance policies:

There are in general, two types of cyber insurance policies that corporations may take out to cover themselves against liabilities that may come about due to realised cyber risks. A typical third party cyber insurance policy covers privacy liability, network security liability and intellectual property and media breaches. Insured losses covered by privacy liability include legal liability, vicarious liability, and crisis control. Network security liability coverage insures against costs from reinstatement and costs from legal proceedings, and intellectual property and media breaches cover insures against legal liability losses.[77]

A typical first party cyber insurance policy, on the other hand, will offer an organisation crisis management cover, business interruption data asset protection cover and cyber extortion cover. Costs to reinstate reputation, for notification of stakeholders and continuous monitoring, are covered by the crisis management cover. Business interruption data asset protection cover insures losses from costs for reinstatements, loss of profit, data replacement costs, and costs from reinstatement or replacement of intellectual property. Cyber extortion insures losses arising from extortion payments and costs related to avoid extortion. [78]

4.7.9 Cyber Risk Insurance – South Africa

---

[76] Vorys op cit (n73).
[77] Biener op cit (n12) 7.
[78] Ibid.

The management of cyber risks at board level is a critical component of the board's responsibilities and has become an integral part of enterprise risk management. Directors fiduciary duty of care cannot ignore cyber risks and must oversee the enforcement of appropriate and adequate controls to address and mitigate the potentially devastating impact of cybercrimes.

An increasing number of businesses in South Africa are taking out specialised cybercrime insurance cover. As cyber insurance is still in its infancy in South Africa insurers are encountering problems at risk assessment stage with predicting probability of a cybercrime occurring and determining its business impact and quantifying the financial impact of a cyber-attack as they can result in a myriad of negative business consequences. The insurance industry is still to develop standard methodologies and financial models to determine the appropriate price to adequately cover cybercrime risks. The lack of historical data is also problematic to insurance firms when deciding the rate at which to underwrite the risks. The lack of standard legal definitions of cyber liability across the world also impacts on the insurance of cyber risks. The geographic limitation of domestic laws creates difficulties when determining which country's laws are applicable when a cross-border cyber-attack occurs.[79]

[79] B O'Connor & V Moodley op cit (n4).

5. Challenges

Cybercrime is transnational, borderless in nature and does not require knowledge of or proximity to the target. It poses a unique set of challenges, namely: logistics, combating anonymity, accessing electronic information and transnational enforcement. Due to these challenges, existing criminal laws regulating cyberspace tend to result in few successful prosecutions.[1].

Cybercrimes are constantly evolving and taking on newer forms. This calls for a nimble and responsive approach to tackling this pandemic. The current laws used to prosecute cybercrimes have not kept up with these evolutions. They lack definitional clarity hence many of the cybercrimes are in fact not offences according to local statues and are prosecuted using laws of other countries or traditional criminal laws where possible. This lack of definition clarity also hampers the provision of cyber insurance as there is still no agreed on definition of 'cyber liability'. There are also some areas of our current cyber laws that fall short and should be reviewed:

- Criminalising crimes that relate to intangible data;
- Review of current procedural laws to support and facilitate intensive cybercrime investigations;
- There is no obligation on internet service providers to report cybercrimes.[2]

Our current cybersecurity laws spread across multiple ministries and lead to clashes in mandate in investigating or prosecuting cyber incidents[3]. As cybercrimes tend to be cross-border in nature, the absence of ratified conventions that extend jurisdiction,

---

[1] Cassim op cit (n7) 39.
[2] 'Cybercrime in South Africa: What's the Plan?' *Hooybeg Attorneys* 2016, available at *https://hooyberglaw.wordpress.com/2016/02/29/cybercrime-in-south-africa-whats-the-plan/ accessed* on 06 December 2017.
[3] 'Discussion of the cybercrime and cybersecurity' *Department of Justice*, 2016, available at *http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.*pdf, accessed on 01 August 2017.

makes it difficult to effectively deal with these forms of cybercrimes accordingly. Geographical limits thus restrict South Africa's country's cyber laws.

The domestic police force operates with limited resources and lacks specialist skills to take on the complex, multijurisdictional investigations.[4] relating to cybercrimes. Despite the National Director of Public Prosecutions reporting 289 prosecuted cases related to cybercrime in 2017, and a remarkable 97% conviction rate[5], very few of the cases test the ECT Act to develop much required precedent.[6] In comparisons with 4779 convictions for sexual offences, this figure confirms that not enough cases of cybercrime are being reported and prosecuted annually. Of the three[7] unreported cybercrime related cases cited in the annual report, it is only the case of *State v Mduduzi Mkhize* where the ECT Act was used to secure a conviction.

Harmonisation of cybercrime laws across ministries domestically and internationally with other sovereign states remains a challenge. It is made more complex when seeking to address matters such as substantive and procedural law, mutual assistance, and extradition. Noting that each country will come to the harmonisation table with its own perspective, influenced by its legal tradition(s) as well as cultural and historical factors. The object of harmonisation is to 'harmonise' and not to produce 'identical' copies. What is required is complementarity enabling enforcement mechanisms to work effectively while respecting national and regional differences.[8]

South Africa has signed but not yet ratified the Budapest Convention on Cybercrime. As a founding member of the association of five the major emerging national economies: Brazil, Russia, India, China, and South Africa (BRICS), there

---

[4] Ibid.

[5] National Prosecution Authority 'Annual Report National Director of Public Prosecutions 2016/17' available at *https://www.npa.gov.za/sites/default/files/annual-reports/NDPP-Annual%20Report-2016*-17.pdf, accessed on 13 February 2018

[6] K O'Riley 'South African law coming to grips with cybercrime' 2013 *De Rebus*

[7] *State v Mduduzi Mkhize; State v N Idediora and another; State v Matatu and 4 others*

[8] Clough op cit (n77).

seems to be a problem with ratifying a convention from the COE as BRICS members much prefer to ratify a 'more universal international instrument'[9]. Member states of BRICS consider the United Nations (UN) as *the* agency that has a central role in developing universally accepted norms of responsible state behaviour in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible, and equitable ICT environment. BRICS members are mostly concerned about the upholding of state sovereignty, political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms which they feel would be compromised by ratifying the COE convention on cybercrime.[10]

6. Conclusion, Recommendations, and future Research Areas

6.1 Conclusion

Even though the term 'cybercrime' has been around in legal system and parlance for some time now, there is overwhelming evidence to suggest that it is still misused, misunderstood, and ambiguously applied. This lack of understanding does not stop at the colloquial level but has crossed over into industrial, academic, and statutory nomenclature. The menace has instead intensified and taken on juggernaut-like proportions, getting stronger as it spreads and morphs into different attack vectors, making it harder to stop, comprehend and prosecute.

The battle against cybercrime cannot be won without first understanding the phenomenon. To arrive at this understanding multiple courses will need to be chartered. First a common understanding of all cybercrime and related terminology will need to be developed. Once the lexicon is in place, drafting of the necessary artefacts for the harmonisation of ICT strategy, policy and regulatory frameworks can be undertaken in earnest. With the cybercrimes, penalties and prosecutorial procedures codified, grand scale education, training and awareness of all stakeholders can begin in earnest. Cybercrimes are multi-jurisdictional in nature and

---

[9] LexInformatica – 2013 Cyberlaw Conference, A Nel *'Advancement of cyberlaw and information ethics in Africa and globally'* available at *http://www.justice.gov.za/cfw/confw.htm* accessed on 22 December 2017.
[10] DIRCO 'Xiamen Declaration' 2017 *BRICS* available at *http://bit.ly/2CWOiSs* accessed on 22 December 2017.

thus also call for a cross-sector, intra-ministerial, public-private and multinational partnering and working together.

6.2 Recommendations

6.2.1 Technical: Broadband and Infrastructure

The path to economic emancipation, employment opportunities and overall sustainable positive GDP growth in the digital era begins with access to reliable, secure and affordable broadband internet access. For the South African Government to realise its own broadband targets and gain improved infrastructure cybersecurity recommended:

a) Access to the internet must be deemed a human right by the RSA government by ratifying the UN Human Rights Council non-binding resolution on 'The promotion, protection and enjoyment of human rights on the Internet'[1];
b) Honour NDP commitment on implementing broadband by delivering on targets of the National Broadband Policy (SA Connect), SIP 15, MTSF (2014 – 2019) and the National e-Strategy.
c) The establishment of sectoral computer emergency response teams (CERT) starting with the development of a financial sector CERT as with the government of INDIA[2]. This Fin-CERT should work with the financial sector regulators, Central Bank, and national CSIRT to strengthen cyber security in critical national infrastructures and facilitate the development and implementation of internationally recognised cybersecurity standards, frameworks, and tools.
d) Establishment of or sectoral information sharing and analysis centres (ISACs)[3] for collecting, analysing and sharing of cyber threat intelligence

---

[1] '32nd session of the Human Rights Council' 8th July 2016 *United Nations Human rights council* available at at,*http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session32/Pages/32RegularSession.asp* x accessed on 30 November 2017.
[2] India Ministry of Finance op cit (n6).
[3] ISAC Available at *http://bit.ly/2AJZQD6* accessed on 28 December 2017.

and provision of tools to mitigate risks and improve resilience. The USA's FS-ISAC and SABRIC are great models that the rest of South Africa's critical infrastructure sectors can reference.

6.2.2 Cooperation: Agreements, Treaties and Conventions

As cybercrime is in its nature a global issue, it calls for coordinated ministerial, sectorial, and national approaches. South Africa's current jurisdictional challenges that limit and hamper cybercriminal investigations can be remedied by concluding international cooperation, mutual assistance, and enforcement agreements in tandem with harmonising of cybercrime legislation, standards, and procedures.

South Africa has the option to ratify the COE's Convention on Cybercrime, failing which the following is recommended to improve cooperation and establishment of mutual assistance:

a) National: Ensure coordination of the various laws dealing with cyber security that have overlapping mandates and responsibilities between different government ministries;
b) Continental Convention: Ratify and implement the African Union Convention on Cyber Security and Personal Data Protection adopted in 2014 and harmonize domestic IT laws and frameworks accordingly;
c) Economic Region: Implement the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs and the BRICS Intergovernmental Agreement on Cooperation in Ensuring Security in the use of ICTs as per the Xiamen Declaration[4];
d) International: Affiliate to the UN's 2011 UNODC led Global Programme on Cybercrime[5] mandated to assist member States with cyber-related crimes through capacity building and technical assistance;

[4] DIRCO op cit (n10).
[5] 'UNODC Global Programme on Cybercrime' available at *http://bit.ly/2AN6DvP* accessed on 04 January 2018.

e) International: Implement the ITU Global Cybercrime Agenda framework for international cooperation aimed at enhancing confidence and security in the information society[6].

f) International: Endorse the proposed 2015 UN International Code of Conduct for Information Security[7] drafted to strengthen international cooperation and formulate relevant international norms;

g) Mutual legal assistance treaties and inter-agency[8] agreements may also be concluded, in the absence of conventions and treaties that establish international corporation. The following conventions of the AU[9] and EU[10] may both be referenced.

6.2.3 ICT Legislative Framework

The legal framework regulating cyber security in South Africa is a hybrid of legislation and the common law. There is a need to review the local statutes and harmonise them with their regional and international legal standards.

The most impactful starting point for the RSA government, would be to, once all due processes have been completed, enact, and promulgate the *CAC Bill, 2017*. Apart from defining 'cybercrime' and related terms, this bill will assist the understanding and combating of cybercrime in numerous ways including the regulating the conclusion of mutual assistance agreements, founding jurisdiction and international cooperation in respect of cross-border investigation of cybercrime, providing for the creation of various structures to deal with cyber security including establishment of an all-hours national cybercrime centre, the declaration, regulating the identification and protection of national critical information infrastructure and repeal or amend certain applicable laws currently in effect. [11]

---

[6] GCA available at *http://bit.ly/2CZZPRT* accessed on 04 January 2018.
[7] UN International Code of Conduct for Information Security Available at *http://bit.ly/1hFMUph* accessed on 04 January 2018.
[8] Council of Europe Inter-Agency and International Cooperation for Search, Seizure and Confiscation of Online Crime Proceeds available at *http://bit.ly/2EtO7uJ* accessed on 05 January 2017.
[9] African Union Convention on cybersecurity and personal data collection, Article 28(2).
[10] Council of Europe Convention on Mutual assistance in criminal matters.
[11] 'Discussion of the cybercrime and cybersecurity' *Department of Justice*, 2016, available at *http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.*pdf, accessed on 01 August 2017.

The protection of the nation critical information, sensitive and mission critical company data and personal information can be improved by putting into effect the entire *Protection of Personal Information Act*, 2013 and not just some parts of it[12] (like the UK's 1998 *Data Protection Act* and the EU General Data Protection Regulation). Once the entire Act is fully in effect then it is recommended that sector authorities issue cybersecurity standards and guidelines for cybersecurity and cyber-risk management.

It is recommended that the Johannesburg Stock Exchange (JSE) listing requirements[13] and the relevant instruments of the Financial Service Board[14] be amended to give effect to s22: "Notifications of security compromises", of the POPI Act. This recommendation is made to strengthen the (minority) shareholder's when holding to account, directors who default on their duty of care to manage company cyber risks. This recommendation is in line with the technology and information disclosure requirements of principle 12 of the King IV Code and s165(2) of the Companies Act, where company information is essential to bring a suitable demand before the court. Furthermore, this recommendation has the potential to benefit the derivative litigants in a manner similar to public enforcement. Section 17 of the USA Securities Exchange Act[15] and the New York State Department of Financial Services[16] have all effected changes similar to those recommended,

6.2.4 Dedicated Arrangements to Manage Cybercrime

Once the ICT legislative framework has been strengthened to outlaw and prosecute cybercrimes, the need for mechanisms, actors, supporting structures and arrangements is then created. These agencies and arrangements are recommended as

---

[12] 'Commencement of sections of the Protection of Personal Information Act' Government Gazette 37544 *SAICA* available at *http://bit.ly/2mehwS9* accessed on 8 January 2018.
[13] JSE Limited Listing Requirements (2017) Available at, *https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/JSE%20Listings%20Requirements.pdf* accessed on 13 February 2017.
[14] Financial Services Board Available at, *https://www.fsb.co.za/Departments/insurance/Pages/legislation.aspx*, accessed on 13 February 2017.
[15] US Securities Exchange Act of 1934.
[16] New York Department of Financial Services 'Cybersecurity Regulations' (2017) Available at,*http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf* accessed on 16 November 2017.

they are essential for the preventative, corrective and restorative aspects dealing with cybercrime in South Africa.

It is recommended that the National Cybersecurity Policy framework for South Africa be fully implemented as it will assist in combating cybercrime by, *inter alia* providing additional definitions for cyber terminology, securing government commitment, establishing dedicated bodies for national cybersecurity decision making, coordination for all role players involved, and capacity development for cyber-criminal threat intelligence, investigations, and prosecution.[17]

It is further recommended that the following, as promised in the National Cyber Security Framework, be implemented:

i. Draft Cyber Security Policy, which seeks to propose a cyber security policy approach for SA;
ii. Draft National Critical Information Infrastructure Policy, which outlines an approach to the identification, protection and security of national information infrastructure that is categorised as critical for the provisioning of essential services to South Africans;
iii. Draft Cyber Crime Policy and Strategy, which seeks to develop a national policy and strategy approach to combating cybercrime;
iv. A Draft Cyber Defence Strategy;
v. Cyber defence for South Africa and is led by the Department of Defence;
vi. Draft Cyber Security Awareness Strategy, which proposes measures to deal with relevant aspects of cyber security awareness within SA.

It is recommended that a Cyber Appellate Tribunal fashioned around the one in India[18] be considered. A new dispensation of virtual and electronic trials can then be ushered in and provide a platform for specialist cybercrime legal practitioners to develop much needed precedents for the courts.

---

[17] National Cybersecurity Policy Framework for South Africa (2015) 7.
[18] India Cyber Appellate Division available at *http://cyatindia.gov.in/Constitution.aspx* accessed on 09 January 2017.

Investigation and prosecuting of cybercrimes requires specialised techniques and procedures that are not readily available in the domestic law enforcement agencies and the criminal justice system. It is thus recommended that the law enforcement officials, legal practitioners[19] , and presiding officers be regularly provided with training on effectively investigating and prosecuting cybercrimes.

6.2.5 On-going Cybercrime awareness

Governments are tasked with raising cyber security awareness within their countries. Combating cybercrime does not only require technical and regulatory intervention, it also relies on people. Public awareness tools may be used to stimulate, motivate, and remind the audience what is expected of them. This is an important aspect of cyber security because it enhances the security knowledge of users, changes attitude towards cyber security, and changes behaviour patterns. These factors improve the resilience of users against cyber-attacks.[20]

a) South Africa should increase its cyber security awareness programmes by collaborating on cyber security awareness at government, business, and societal levels, as guided by an African Cyber Security Awareness Framework.[21]
b) It is recommended that the South African government partner with universities[22] and institutions of higher learning to develop national education programmes and academic curricula that will be for cybersecurity research, and the development of standards and certifications. Professional cyber security training courses can then be offered by these universities. In so doing

---

[19] M Mamabolo 'Ghana to train ECOWAS neighbours in cybercrime and e-evidence' (2017) *ITWEB* available at *http://bit.ly/2CXWgLR* accessed on 23 December 2017.
[20]Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW), 2011 IZ Dlamini et al, 'Framework for an African Policy towards creating cyber security awareness', para 4.
[21] Ibid.
[22] UK National Cyber Security Centre, Academic Centres of Excellence in Cyber Security research available at *http://bit.ly/2D1QAk0* accessed on 09 January 2018.

the cyber workforce can be sustainably increased, home-grown, and periodically assessed[23] post qualification within their workplaces.

c) Regular and effective National Cybersecurity Awareness[24] programmes and initiatives are recommended.

d) Regular and effective national and sector simulated cyber-attack exercises/ war games[25] are recommended.

e) It is recommended that national cyber security assessments be performed annually and the ITU's global cybersecurity index be completed regularly to holistically assess the country's cybersecurity posture and the commitment of member states towards cybersecurity.

---

[23] US Federal Cybersecurity Workforce Assessment Act 2016 available at *http://bit.ly/2D1gvHy*., accessed on 10 February 2015.

[24] National Cybersecurity Awareness Month, Prof. Hlengiwe Mkhize 2016 Available at, *https://www.dtps.gov.za/index.php?option=com_content&view=article&id=682:national-cybersecurity-awareness-month&catid=10&Itemid=137 a*ccessed on 06 December 2017.

[25] An Introduction to Cyber War Games, Deloitte, 2014, Available at, *http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/* accessed on 06 December 2017.

BIBLIOGRAPHY

Primary Sources

Constitution

Constitution of the Republic of South Africa, 1996

Statutes

India

Information Technology Act of 2000
Information Technology Amendment Act of 2008

Kenya

Computer and Cybercrimes Bill 2016.
Information Communication and Technology Amendment Act of 2013.
Information and Communications Act 2013.

South Africa

ECT Act
ECTA, Amendment Bill,2012
Companies Act 71 of 2008.
Criminal Procedure Act 51 of 1977
Critical Infrastructure Bill
Cybercrimes and Cybersecurity Bill of 2017
The Banks Act 4 of 1990.
The Banks Regulations (published in Government Gazette no. 21726 of 8 November 2000.

The United Kingdom

Computer Misuse Act 1990

The United States of America

The Uniting, and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.
Cyber Act of War Bill of 2016.
US Penal Code
The Homeland Security Act of 2002
Racketeering
Computer Fraud and Abuse Act of 1986

Cases

Cape Empowerment Trust Limited v Druker and others [2016] JOL 36987 (WCC).

Kukama v Lobelo and Others (38587/2011) [2012] ZAGPJHC 60.

Loureiro v iMvula Quality Protection (PTY) Ltd 2014 3 SA 394 (CC).

Msimang NO and another v Katuliiba and others [2013] JOL 30522 (GSJ).

Mouritzen v Greystone Enterprises (Pty) Ltd & Another (10442/2011) [2012] ZAKZDHC.

Applicable Unreported cases (2017): State v Mduduzi Mkhize; State v N Idediora and another; State v Matatu and 4 others

Secondary Sources

Books

Kshetri N *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan, London, 2013)

Kramer F et al '*Cyberpower and National* Security' 6ed (Washington, D.C: Center for Technology and National Security Policy2009 439, 2009)

Ohlin JD et al '*Cyberwar. Law and Ethics for Virtual Conflicts'* (Oxford University Press, New York, 2015)

Papadopoulous, S & Snail, S '*Cyber@lawSA'* 3ed (Van Schaik, Pretoria, 2012)

Ryle G '*The Concept of the Mind'* 6ed (University of Chicago Press, Chicago, 2002)

Siebel, T & House, P '*Cyber Rules: Strategies for excelling at e-business'* (Currency DoubleDay, United States of America, 1999)

Journals

Bouwman N 'An Appraisal of the Modification of the Director's Duty of Care and Skill' 4 *SA Mercantile Law Journal* 21 (2009) 510-511.

Cassim, F 'Formulating specialised legislation to address the growing spectre of cybercrimes: A Comparative Study' (2009) *Potchefstroom Electronic Law Journal* Volume 12

Cassim, F 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012) *Potchefstroom Electronic Law Journal* Volume 15

Clough JA world of difference: The Budapest convention on cybercrime and the challenges of harmonisation' (2014) 40 *Monash University Law Review* Volume 3.

Gordon S& Ford R ‘On the definition and classification of cybercrime’ (2006) *Journal of Computer Virology and Hacking Techniques* Volume 2.

Healey J and Wilson A.J. ‘Cyber Conflict and the War Powers Resolution’ *Georgetown Journal of International Affairs* 2012.

Hughes D & Colarik A ‘The Hierarchy of Cyber War Definitions’ *Massey University,* 2017

Madarie R ‘Hackers’ Motivations: Testing Schwartz’s Theory of Motivational Types of Values in a Sample of Hackers’ (2017) *International Journal of Cyber Criminology,* Vol 11

Mangena D ‘Will legislation protect your virtual space? Discussing the draft Cybercrime and Cyber Security Bill’ (2016) *De Rebus.*

Nattrass N ‘The new growth path: Game changing vision or cop-out?’107 *South African Journal of Science* (2011) .

Ncube, Caroline B ‘You’re fired! The removal of directors under the Companies Act 71 of 2008’ 2011 *SALJ Volume 1*.

Njontini MN ‘Protecting Critical Databases – Towards a risk based assessment of critical information infrastructures in South Africa’ 2013 *Potchefstroom Electronic Law Journal* Volume 16.

O’Riley K ‘South African law coming to grips with cybercrime’ 2013 *De Rebus*

Price A ‘The contract/delict interface in the Constitutional Court’ 2014 *Stellenbosch Law Review* Volume 25.

Sabillon R et al ‘Cybercriminals, cyberattacks and cybercrime. Privacy, security and control’ (2016) *Institute of Electrical and Electronics Engineers.*

Shackelford SJ ‘Towards Cyber-peace: Managing Cyberattacks through Polycentric Governance’ (2013) *American University Law Review* Volume 62

Stevens R ‘The legal nature of the duty of care and skill’ : Contract or Delict’, 2016, *Potchefstroom Electronic Law Journal* Volume 19.

Stoop H ‘The business judgment rule: how the Companies Act of 2008 is impacting on directors’ duties’2012 *SALJ Volume* 129.

Theses

B Mupangavanhu 2016 'Directors' Standards of Care, Skill, Diligence, And The Business Judgment Rule In View of South Africa's Companies Act 71 of 2008: Future Implications For Corporate Governance' 192

MF Cassim 'The statutory derivative action under the Companies Act of 2008: Guidelines for the exercise of the judicial discretion' (2014) available at *https://open.uct.ac.za/bitstream/item/13147/thesis_hum_2014_cassim_mf.pdf?sequence=1* , accessed on 12 February 2018.

Internet References

'32nd session of the Human Rights Council' 8th July 2016 *United Nations Human rights council* available at at,*http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session32/Pages/32RegularSession.asp*x accessed on 30 November 2017.

An Introduction to Cyber War Games, Deloitte, 2014, Available at, *http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/* accessed on 06 December 2017.

Atkinson S '*Psychology and the hacker – Psychological Incident Handling'*, 2015 available at *https://www.sans.org/reading-room/whitepapers/incident/psychology-hacker-psychological-incident-handling-36077* para 2 accessed on 10 November 2017.

Arora R 'Introduction to Cyber-crimes, cyber security, and legal aspects', available at, *http://bit.ly/2FZPB0S,* 2013, accessed on 07 April 2017.

Anderson R et al 'Measuring the cost of cybercrime' 2012, available at, *http://www.econinfosec.org/archive/weis2012/presentation/Moore_presentation_WEIS2012.pdf*, accessed on 04 December 2017.

Accenture 'Cost of Cyber Crime Framework',2017 available at *https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf* accessed on 12 December 2017 p24

Bergin T 'Costs of bank cyber thefts hit SWIFT profit last year' 2017, available at,*https://uk.reuters.com/article/us-banks-swift-cybercrime/costs-of-bank-cyber-thefts-hit-swift-profit-last-year-idUKKBN1910FX* accessed on 04 December 2017.

Biener C et al 'Insurability of Cyber Risks: An empirical analysis' (2015) *Institute of Insurance Economics* available at *http://bit.ly/2FeD6if* accessed on 28 December 2017 4.

Burns E 'Periodic table of cybercrime attacks: curing cybersecurity's tunnel vision'2017, available at, *https://www.cbronline.com/cybersecurity/business/periodic-table-cybercrime-attacks-curing-cybersecuritys-tunnel-vision/* ,accessed on 03 December 2017.

'CF Disclosure Guidance: Topic No. 2', *U.S. Security and Exchange Commission* 2011,available at, *https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm* accessed on 16 November 2017.

'Cybersecurity, Financial Industry Regulatory Authority'2015, available at, *http://www.finra.org/industry/cybersecurity* , accessed on 20 November 2017.

'Commencement of sections of the Protection of Personal Information Act' Government Gazette 37544 *SAICA* available at *http://bit.ly/2mehwS9* accessed on 8 January 2018.

Council of Europe Inter-Agency and International Cooperation for Search, Seizure and Confiscation of Online Crime Proceeds available at *http://bit.ly/2EtO7uJ* accessed on 05 January 2017.

'Cyber Risks: Board responsibilities' *Vorys* 2014, available at, *https://www.vorys.com/publications-1316.html* accessed on 15 November 2017.

'Cyber liability risks' 2017 *Insurance information Institute,* available at, *https://www.iii.org/article/cyber-liability-risks* accessed on 15 November 2017.

'Cybercrime in South Africa: What's the Plan?' *Hooybeg Attorneys* 2016, available at *https://hooyberglaw.wordpress.com/2016/02/29/cybercrime-in-south-africa-whats-the-plan/ accessed* on 06 December 2017.

'Cyber Crime – Legal Guidance' *The Crown Prosecutors* 2017, available at *https://www.cps.gov.uk/legal-guidance/cybercrime-legal-guidance,* accessed on 17 December 2017.

'Cybercrime' *European Commission*, 2017, available at, *https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en,* accessed on 19 April 2017.

Davids N 'SA is the leading target in Africa for cyber crime, warns legal firm' 2017, available at,*https://www.businesslive.co.za/bd/world/africa/2017-02-13-sa-is-the-leading-target-in-africa-for-cyber-crime-warns-legal-firm/* accessed on 01 August 2017.

Developing case involving mobile money platform and all banks in India, October 2017 , available at *https://economictimes.indiatimes.com/small-*

biz/startups/mobikwik-glitch-cops-track-those-who-transferred-funds/articleshow/60898149.cms accessed on 5 December 2017.

'Discussion of the cybercrime and cybersecurity' *Department of Justice*, 2016, available at *http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.*pdf accessed on 01 August 2017.

DIRCO 'Xiamen Declaration' 2017 *BRICS* available at *http://bit.ly/2CWOiSs* accessed on 22 December 2017.

'Directors liability Booklet' *Werksmans Attorneys* 2013, available at, *https://www.werksmans.com/wp-content/uploads/2013/04/Werksmans-Directors-Liability-Booklet.pdf* , accessed on 12 February 2018.

'Enhanced Cyber Risk Management Standards' *Financial services Sector Coordinating Council* 2017 Available at, *https://www.federalreserve.gov/SECRS/2017/February/20170221/R-1550/R-1550_021717_131709_429070260162_1.pdf* accessed on 13 December 2017.

Ellipsis 'Policy direction on effective competition in broadband markets', 2016 available at http://bit.ly/2BiUouT, accessed on 21 August 2017.

Frierson R, 'Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security' 2017, available at, *https://www.federalreserve.gov/SECRS/2017/May/20170518/R-1550/R-1550_021717_131709_429070260162_1.pdf* accessed on 16 November 2017.

'Financial Institutions Examination Council' 2017, Available at, *https://www.ffiec.gov/* accessed on 16 November 2017.

Flockhart R 'Cyber risk and directors' liabilities: an international perspective' 2016, Norton Rose Fulbright available at, *http://www.nortonrosefulbright.com/knowledge/publications/145122/cyber-risk-and-directors-liabilities-an-international-perspective* accessed on 16 November 2017.

Financial Services Board Available at , *https://www.fsb.co.za/Departments/insurance/Pages/legislation.aspx* , accessed on 13 February 2017.

Farisani DM 'Corporate Criminal Liability for Deaths, Injuries and Illnesses: Is South Africa's Mining Sector Ready for Change?' 2015 available at *https://www.moneyweb.co.za/wp-content/uploads/2015/11/Corporate-Criminal-*

GCA available at *http://bit.ly/2CZZPRT* accessed on 04 January 2018.

Gercke M 'Understanding Cybercrime: Phenomena, challenges, and legal responses.' 2012, available at, *http://www.itu.int/ITU-*

D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, accessed on 5 April 2017.

Geach W 'Statutory, Common Law And Other Duties Of Directors' Available at *https://www.chartsec.co.za/documents/speakerPres/WalterGeach/GeachStatutoryCommonLawAndOtherDutiesOfDirectors.pdf*, 2009, accessed on 11 February 2018.

Gemalto '2017 First Half Breach Level Index'2017, available at *http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf* accessed on 13 November 2017.

Gervais B 'Cyber Risk Management Guidance for Corporate Directors', 2017 available at, *https://www.lexology.com/library/detail.aspx?g=800d6480-500a-424d-839f-68879eb98637* accessed on 16 November 2017.

Gordon B 'Internet Criminal Law' Available at, *http://www.legalnet.co.za/cyberlaw/cybertext/chapter15.htm, accessed on 08 November 2017 para 426.*

Glance D 'What is the Dark Web?*'* 2017, available *at*

http://theconversation.com/explainer-what-is-the-dark-web-46070> accessed on 12

December 2017.

Hummel R 'Securing against the most common vectors of cyber attacks '2017 *SANS Institute* available at, *https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995* ,accessed on 04 December 2017.

Hunt T 'Questions about the Massive South African "Master Deeds" Data Breach Answered'2017, available at *https://www.troyhunt.com/questions-about-the-massive-south-african-master-deeds-data-breach-answered/* accessed on 13 November 2017.

Hutchinson W 'Survival in the e-conomy: 2nd Australian information warfare &

security conference 2001' 2001, available at

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7758&context=ecuworks#page=38

accessed on 8 November 2017

Information Security Forum 'Protecting the Crown Jewels'2016, available at *https://www.securityforum.org/uploads/2016/09/ISF_Protecting-the-Crown-Jewels-Executive-Summary-final.pd*f accessed on 13 November 2017.

Institute of Risk Management 'Cyber risk and risk management' 2018, available at, *https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/* accessed 13 November 2017.

'Improving Critical Infrastructure Cybersecurity Executive Order 13636' 2013, available at, *http://www.cyberriskinsuranceforum.com/sites/default/files/preliminary-cybersecurity-framework.pdf* accessed on 14 November 2017.

Irwin L 'More data was lost or stolen in the first half of 2017 than all of 2016' *IT Governance Institute* 2017, available at *http://bit.ly/2EPoU1L* , accessed on 13 November 2017.

International Telecommunication Union (2017) 'Global Cybersecurity Index 2017 Africa Report' 27, available at http://bit.ly/2C3zrRn, accessed on 29 December 2017.

ISAC Available at *http://bit.ly/2AJZQD6* accessed on 28 December 2017.
India Cyber Appellate Division available at *http://cyatindia.gov.in/Constitution.aspx* accessed on 09 January 2017.

India Ministry of Finance 'Report of The Working Group For Setting Up of Computer Emergency Response Team In The Financial Sector (Cert-Fin)' 2017, available at,*http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf* accessed on 18 November 2017.

Internet Safety Campaign Africa 'Cybercrime Definition' available at *http://cybercrime.org.za/definition* accessed on 29 March 2017.

Institute of Directors in Southern Africa '*King IV Report on Corporate Governance for South Africa*' (2016) 21.

ICO fines Sony £250,000 for failure to prevent hacking on Sony PlayStation Network Platform, by PLC IPIT & Communications', 2013 available at, *https://uk.practicallaw.thomsonreuters.com/5-523-7306?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&comp=pluk* accessed on 16 November 2017.

JSE Limited Listing Requirements (2017) Available at, *https://www.jse.co.za/content/JSERulesPoliciesandRegulationItems/JSE%20Listings%20Requirements.pdf* accessed on 13 February 2017.

Juma V 'CBK tells banks to boost cyber crime protection' 2017, available at, *http://www.businessdailyafrica.com/news/New-cyber-crime-rule-for-commercial-banks/539546-3981762-12c4in7/index.html* , accessed on 21 November 2017.

Kanza E 'How universal internet access could reboot South Africa' (16/062017) *World Economic Forum*, available at http://bit.ly/2z9sgcx, accessed on 15 November 2017.

Kerala High Court, C.M Philip vs The Registrar of Co-Operative, 2013, available at, *https://indiankanoon.org/doc/16257664/* accessed on 5 December 2017.

Kisicek G & Zagar IZ 'What do we know about the world? Rhetorical and argumentative perspectives',2013, available at *http://bit.ly/2C6f2LD,* accessed on 20 April 2017.

*Liability-for-Deaths-Injuries-and-IllnessArticleby-DM-Farisani.pd*f, accessed on 12 February 2018.

LexInformatica – 2013 Cyberlaw Conference, A Nel *'Advancement of cyberlaw and information ethics in Africa and globally'* available at *http://www.justice.gov.za/cfw/confw.htm* accessed on 22 December 2017.

Lipton M, 'Risk Management and the Board of Directors', *Harvard Law School* , 2017 available at , *https://corpgov.law.harvard.edu/2017/02/15/risk-management-and-the-board-of-directors-4*/ accessed on 02 November 2017.

Mamabolo M 'Ghana to train ECOWAS neighbours in cybercrime and e-evidence' (2017) *ITWEB* available at *http://bit.ly/2CXWgLR* accessed on 23 December 2017.

McAfee 'McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies' 2014 available at, *https://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx* accessed 20 November 2017.

Minges M 'Exploring the Relationship Between Broadband and Economic Growth' *World Development Report 2016: Digital Dividends*, 2016, available at *http://bit.ly/2lZTn4p,* accessed on 7 December 2017.

Morgus R et al 'National CSIRTs and Their Role in Computer Security Incident Response' 2015, available at http://bit.ly/2BDskCP accessed on 05 December 2017 5.

National Prosecution Authority 'Annual Report National Director of Public Prosecutions 2016/17' available at *https://www.npa.gov.za/sites/default/files/annual-reports/NDPP-Annual%20Report-2016*-17.pdf, accessed on 13 February 2018

National Cybersecurity Awareness Month, Prof. Hlengiwe Mkhize 2016 Available at, *https://www.dtps.gov.za/index.php?option=com_content&view=article&id=682:national-cybersecurity-awareness-month&catid=10&Itemid=137 a*ccessed on 06 December 2017.

New York Department of Financial Services 'Cybersecurity Regulations' (2017) Available at,*http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf* accessed on 16 November 2017.

Ngafeeson M 'Cybercrime Classification: A Motivational Model', 2009, available at *http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf* accessed on 10 November 2017.

Nyamanga M ‘A Layered Framework Approach to Mitigate Crimeware’ (2010) Annual ADFSL Conference on Digital Forensics, Security and Law. Available at *http://commons.erau.edu/adfsl/2010/thursday/7* accessed on 30 January 2018

‘National Infrastructure Protection Plan’ *Department of Homeland Security* 2017, available at, *https://www.dhs.gov/national-infrastructure-protection-plan* accessed on 14 November 2017.

O’Connor B & Moodley V ‘The Growing Need For Cybercrime Insurance In South Africa’ 2016, available at,*https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2016/dispute/downloads/Dispute-Resolution-Alert-10-August-2016.pdf* accessed on 07 November 2017.

Organisation for Economic Co-operation and Development ‘Protection Of ‘Critical Infrastructure’ And The Role Of Investment Policies Relating To National Security’2008, Available at,*https://www.oecd.org/investment/investment-policy/40700392.pdf* accessed on 18 November 2017.

Pay U ‘SA companies under cyber-attack?’ 2015, available at, *https://www.payu.co.za/press-room/sa-companies-under-cyberattack* accessed on 01 August 2017.

Paganini P ‘G7 Declaration on responsible state behaviour in Cyberspace’, para 6-7 2017, available at *http://securityaffairs.co/wordpress/57932/cyber-warfare-2/g7-declaration-responsible-states-behavior-cyberspace.htm*l accessed on 05 December 2017.

Plenipotentiary Conference of the International Telecommunication Union ‘*International Telecommunications Union resolution ’Connect 2020 Agenda for global telecommunication/information and communication technology development*’ adopted in Busan ,2014, available at *http://bit.ly/2FXvRLa*, accessed on 11 December 2017.

Porche I et al ‘Redefining Information Warfare Boundaries, for an army in a wireless world’, 2013 available at *https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf*, accesses on 10 February 2018 xvi.

Presidential Infrastructure Coordination Commission ‘A summary of the South African infrastructure plan’, 2012, available at *http://bit.ly/2EdBjJy,* accessed on 31 October 2017.

‘Removing a Director Under the Companies Act 71 of 2008’ 2015, available at, *http://www.polity.org.za/article/removing-a-director-under-the-companies-act-71-of-2008-2015-06-30,* accessed on 11 February 2018.

Rees A ‘Cybercrime Laws of the United States’ *US Department of Justice: Computer Crime and Intellectual Property Section* 2006 available at *https://www.oas.org/juridico/spanish/us_cyb_laws.pdf* accessed on 10 February 2018

Rogin J ‘NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history’, 2012 available at,*http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/* access on 04 December 2017.

Sarkar R ‘Four Key Cyber risk Management Questions for Directors and Officers’ 2017, available at, *http://www.rmmagazine.com/2017/09/01/four-key-cyberrisk-management-questions-for-directors-and-officers/* accessed on 15 November 2017.

Schwab K ‘The Fourth Industrial Revolution: what it means, how to respond’ *World Economic Forum* 2016, available at *http://bit.ly/1pBfye4*, accessed on 02 April 2017

Stadler S & Kok R ‘Protecting your rights as a minority shareholder in South Africa: The derivative action’(2015) available at *http://www.puleinc.co.za/publications/protecting-your-rights-as-a-minority-shareholder-in-south-africa-the-derivative-action/,* accessed on 12 February 2018.

Smit W ‘Companies Act 2008 – Directors’ Responsibilities and Liability’ 2011 available at *https://www.exceedinc.co.za/news/companies-act-2008-directors-responsibilities-and-liability/?id=8&entryId=13* , accessed on 12 February 2018.

Symantec ‘2016 Internet Security Threat Report’, 2017, available at *https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf,* 46 accessed on 18 November 2017.

Tamarkin E, ‘The AU’s cybercrime response A positive start, but substantial challenges ahead’2015, available at, *https://issafrica.s3.amazonaws.com/site/uploads/PolBrief73_cybercrime.pdf* accessed on 19 April 2017.

Tamarkin E ‘Cybercrime: A complex problem requiring a multi-faceted response’ *Institute for Security Studies* 2014, Available at, *https://issafrica.s3.amazonaws.com/site/uploads/PolBrief51Feb14.pdf* accessed on 10 April 2017.

Tucker C 'Greater duty of skill by the directors of a bank' 2003, available at *http://www.bowmanslaw.com/insights/greater-duty-of-skill-by-the-directors-of-a-bank/* , accessed on 12 February 2018.

'Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders' *United Nations* 2000, available at *http://bit.ly/2kjJFXN* accessed on 19 December 2017.

ThreatBrief 'Consumers worry more about cybercrime than physical crime' 2017, available at,*http://threatbrief.com/consumers-worry-cybercrime-physical-crime/* accessed on 04 December 2017.

The information sharing network 'What is critical infrastructure?' *Australian National Security* 2018, available at, *https://www.tisn.gov.au/Pages/Critical_infrastructure.aspx* ,accessed on 18 November 2017

United Nations Human Rights Council '32nd session of the Human Rights Council (13 June to 1 July and 8 July 2016', 2016, available at *http://bit.ly/1rK70TS*, accessed on 30 November 2017

'UNODC Global Programme on Cybercrime' available at *http://bit.ly/2AN6DvP* accessed on 04 January 2018.

UN International Code of Conduct for Information Security Available at *http://bit.ly/1hFMUph* accessed on 04 January 2018.

US Federal Cybersecurity Workforce Assessment Act 2016 available at *http://bit.ly/2D1gvHy*., accessed on 10 February 2015.

Van Zyl G '8.8 million South Africans hit by cyber crime - study' 2016, available at,*http://www.fin24.com/Tech/News/88-million-south-africans-hit-by-cyber-crime-study-20160707* accessed on 01 August 2017.

Van Zyl G 'Ripe for a digital revolution: 40% of SA now has internet access – study' ,2017, available at *https://www.biznews.com/tech/2017/07/19/sa-internet-access-study/*, accessed on 17 November 2017

Vez J 'Recommendations for Public-Private Partnerships against Cybercrime' *WEF*, 2016, available at *http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf*, accessed on 19 April 2017.

Vullo MT 'Cybersecurity Requirements For Financial Services Companies' *New York Department of Financial Services* 2017, available at,*http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf* accessed on 16 November 2017.

World Economic Forum 'Global Information Technology Report 2016', 2016, available at *http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index,* accessed on 15 November 2017.

National Cyber Policies, Strategies, and Frameworks

India

National Cyber Security Policy 2013

Kenya

National Cybersecurity Strategy, 2014

South Africa

National Planning Commission 'National Development Plan 2030

National Cybersecurity Policy Framework for South Africa (2015).

The United States of America

US DoD Strategy for Operations in Cyberspace 2015

The United Kingdom

UK National Cyber Security Strategy 2016 – 2021 (2016)

Treaties and Conventions

African Union Convention on Cybercrime and Data Protection

Council of Europe Convention on Cybercrime