THE AFRICAN JOURNAL OF INFORMATION AND COMMUNICATION (AJIC)

ISSUE 24, 2019

RESEARCH ARTICLES

Assessing the Social Media Maturity of a Community Radio Station: The Case of Rhodes Music Radio in South Africa
Mudiwa A. Gavaza and Noel J. Pearse

Teachers' ICT Adoption in South African Rural Schools: A Study of Technology Readiness and Implications for the South Africa Connect Broadband Policy
Samwel Dick Mwapwele, Mario Marais, Sifiso Dlamini and Judy van Biljon

Realities of Microenterprises' ICT Use for Business Activities and for Acquiring Online Government Support: A Study in Western Cape Province, South Africa
Muhammad Ameer Osman, Donald Flywell Malanga and Wallace Chigona

Digital Transformation in South Africa's Short-Term Insurance Sector: Traditional Insurers' Responses to the Internet of Things (IoT) and Insurtech
Andrew J. Moodley

Intelligent Malware Detection Using a Neural Network Ensemble Based on a Hybrid Search Mechanism
Stephen M. Akandwanaho and Muni Kooblal

Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC)
Morné Pretorius and Hombakazi Ngejane

Published by the LINK Centre
University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

The African Journal of Information and Communication (AJIC)

Issue 24, 2019

Published by the LINK Centre, School of Literature, Language and Media (SLLM)
Faculty of Humanities, University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre/ajic

Published since 2000, *The African Journal of Information and Communication (AJIC)* is a peer-reviewed, interdisciplinary, open access academic journal focused on information and communication ecosystems in Africa, elsewhere in the developing world, and at global level. Accredited by the South African Department of Higher Education and Training (DHET), *AJIC* pursues its open access objective by publishing online, free to the user, under a Creative Commons licence, and by not imposing article processing charges on its contributors.

Editorial Advisory Board

Editors

Managing Editor: Tawana Kupe, Vice-Chancellor, University of Pretoria, South Africa, tawana.kupe@up.ac.za

Corresponding Editor: Lucienne Abrahams, Director, LINK Centre, Faculty of Humanities, University of the Witwatersrand, PO Box 601, Wits 2050, Johannesburg, South Africa, ajic.submissions@gmail.com

Publishing Editor: Chris Armstrong, Research Associate, LINK Centre, University of the Witwatersrand, Johannesburg, South Africa, chris.armstrong@wits.ac.za

Peer-Reviewing

AJIC acknowledges with gratitude the following peer reviewers of articles submitted for publication in this issue: Najma Aghardien, Ufuoma Akpojivi, Olufunmilayo Arewa, Andrew Barendse, Mark Burke, Barrry Dwolatzky, Caroline Ncube, Patrick Ndayizigamiye, Sanjay Ranjeeth, Prabhakar Rontala, Kate Skinner, Roopesh Kevin Sungkur, and Ewan Sutherland.

Guest Editors

AJIC acknowledges with gratitude the editorial guidance provided by Prof. Manoj Maharaj (University of KwaZulu-Natal (UKZN), Durban) to the authors of this issue's article drawing on a THREAT 2019 conference paper, and by Prof. Hossana Twinomurinzi (University of South Africa (UNISA), Pretoria) to the authors of the two articles drawing on Digital Skills 2019 conference papers.

Production

Sub-editing: LINK Centre
Proofreading: Linda Van de Vijver
Desktop-publishing: LINK Centre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

AJIC is published by the LINK Centre, School of Literature, Language and Media (SLLM), Faculty of Humanities, University of the Witwatersrand (Wits), PO Box 601, Wits 2050, Johannesburg, South Africa. The LINK Centre is located at the Wits Tshimologong Digital Innovation Precinct, 41 Juta St., Braamfontein, Johannesburg, https://www.tshimologong.joburg

Past issues of *AJIC*, and its precursor *The Southern African Journal of Information and Communication (SAJIC)*, are available at https://www.wits.ac.za/linkcentre/ajic and https://www.wits.ac.za/linkcentre/sajic

CONTENTS

RESEARCH ARTICLES

Assessing the Social Media Maturity of a Community Radio Station: The Case of Rhodes Music Radio in South Africa
Mudiwa A. Gavaza and Noel J. Pearse

Teachers' ICT Adoption in South African Rural Schools: A Study of Technology Readiness and Implications for the South Africa Connect Broadband Policy
Samwel Dick Mwapwele, Mario Marais, Sifiso Dlamini and Judy van Biljon

Realities of Microenterprises' ICT Use for Business Activities and for Acquiring Online Government Support: A Study in Western Cape Province, South Africa
Muhammad Ameer Osman, Donald Flywell Malanga and Wallace Chigona

Digital Transformation in South Africa's Short-Term Insurance Sector: Traditional Insurers' Responses to the Internet of Things (IoT) and Insurtech
Andrew J. Moodley

Intelligent Malware Detection Using a Neural Network Ensemble Based on a Hybrid Search Mechanism
Stephen M. Akandwanaho and Muni Kooblal

Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC)
Morné Pretorius and Hombakazi Ngejane

RESEARCH ARTICLES

Assessing the Social Media Maturity of a Community Radio Station: The Case of Rhodes Music Radio in South Africa

Mudiwa A. Gavaza
Freelance Business Writer and Radio Presenter; Graduate, Rhodes Business School, Rhodes University, Makhanda (Grahamstown), South Africa
https://orcid.org/0000-0002-6104-3886

Noel J. Pearse
Professor, Rhodes Business School, Rhodes University, Makhanda (Grahamstown), South Africa
https://orcid.org/0000-0001-7583-9845

Abstract

Social media has become a major factor within the operations and functions of radio stations. This study used a social media maturity model (SMMM), developed from available literature, to assess the social media maturity of a South Africa community radio station, Rhodes Music Radio (RMR). The study found that RMR had a level 3 rating on a 5-level maturity scale, indicating that it was quite, but not yet fully, mature in its social media use. In addition to outlining the research and its findings, this article makes recommendations for how the station could increase the maturity of its social media use.

Keywords

social media, community radio, social media maturity model (SMMM), Rhodes Music Radio (RMR), Makhanda (Grahamstown), South Africa

Acknowledgements

This article draws on research conducted by the lead author Gavaza for his MBA dissertation, which was completed under the supervision of the second author, Pearse. This article also draws on the contents of a paper presented by the authors at the World Media Economics and Management Conference, 6-9 May 2018, Cape Town.

DOI: https://doi.org/10.23962/10539/28661

Recommended citation

Gavaza, M. A., & Pearse, N. J. (2019). Assessing the social media maturity of a community radio station: The case of Rhodes Music Radio in South Africa. *The African Journal of Information and Communication (AJIC),* 24, 1-21.
https://doi.org/10.23962/10539/28661

1. Introduction

The aim of the research on which this article is based was to develop and implement a social media maturity model (SMMM) to assess a community radio station's use of social media. Rhodes Music Radio (RMR) is a non-profit community radio station based on the campus of Rhodes University in Makhanda (Grahamstown), South Africa (RMR, 2007). The station services the general Makhanda area, which, according to the World Population Review (2019), has a population in excess of 90,000. The station operates within a 50 km radius of its location in the town (RMR, 2015). RMR uses social media in a number of different ways. Social media are sources of news content for shows, a channel of communication for the station's listeners, a mode of internal communication for RMR staff, and a tool for marketing the brand of the station. Almost all operational departments at the station use social media in some way.

Community radio and social media

Jankowski (2003, p. 7) places community radio under a broader category of community media, which includes "a diverse range of mediated forms of communication: electronic media such as radio and television, print media such as newspapers and magazines, and electronic network initiatives which embrace characteristics of both traditional print and electronic media". The uniqueness and contribution of community radio broadcasters is partly reflected in the values that they promote. Through a meta-analysis of the literature, Order (2015) identified these distinguishing values as access, diversity, alternative, independence, representation and participation. In addition, the content of community radio has unique features, which are valued by its listeners. Lewis (2000) has noted that, despite the growing preference for visual media, radio remains important in the personal lives of listeners. This may be explained by the unique offerings of radio in comparison to other media, such as: the appeal of radio music (MacFarland, 2016), the affinity of radio soap opera with storytelling traditions (Makoye, 2006), the growing popularity of radio talk shows (Owen, 2018), and the opportunity that radio provides to the audience to be the co-producers of radio (Hendy, 2013), or to be citizen journalists (Atton, 2003).

Community radio typically has communitarianism (Brevini, 2015), the facilitation of social inclusion (Correia, Vieira & Aparicio, 2019), or the development and maintenance of a local community identity (Scifo, 2015) as its primary purpose. Therefore, central to its raison d'être is the building of a relationship between the station and the local community, particularly if community radio is viewed as a communication system rather than as a distribution system, allowing listeners not only to hear, but also to speak (Hendy, 2013). Community radio can also serve a number of other purposes, including community development (Wabwire, 2013), the promotion of democracy and citizen participation (Barlow, 1988; Mhagama, 2016) and the promotion of socio-cultural cohesion (Correia, Vieira & Aparicio, 2019; Rodríguez, 2005), but relationship-building remains a central characteristic.

Looking specifically at the South African context, the 1993 Independent Broadcasting Authority Act (IBA Act) made provision for three types of radio broadcasters, namely public, commercial and community services (RSA, 1993). Within a few years of the Act being promulgated, around 100 community radio stations had received operating licences (Sparks, 2009; Tacchi, 2003), and by 2007, 152 of South Africa's 191 licensed radio stations were classified as community services, reaching an estimated 6.5 million listeners (Da Costa, 2012). These radio stations were either serving a localised geographic community, or a community that had a common interest (Tacchi, 2003). (The IBA Act was repealed, and its provisions on community broadcasting replaced, by the Electronic Communications Act (ECA) of 2005 (RSA, 2005).)

Subsequently, community radio in South Africa has been found to serve as an effective way to:

- raise awareness about health-related issues (Hlongwana, Zitha, Mabuza & Maharaj, 2011; Mawokomayi & Osunkunle, 2019; Medeossi, Stadler & Delany-Moretlwe, 2014).
- inform and empower women (Fombad & Jiyane, 2019; Oduaran & Nelson, 2019).
- build communities (Mawokomayi & Osunkunle, 2019; Tacchi, 2002).
- provide a vehicle for participatory communication amongst previously disenfranchised communities (Megwa, 2007; Olorunnisola, 2002).
- facilitate access for community members to information and communication technology (Megwa, 2007).

However, Sparks (2009) observes that there is some concern that the essence of community radio in South Africa has been eroded by financial pressures and the adoption by many stations of a more commercialised operating model. Observing international trends in emerging community radio, Da Costa (2012) cautions that there is a tendency for the original purpose of community radio to be eroded when funding sources and models change.

As social media has emerged, it has been increasingly integrated into the activities of radio, with journalists adopting social media as a tool of their trade (Jordaan, 2013). For example, Rooke and Odame (2013) found that community radio hosts in Canada were using blogs primarily to generate a larger audience base and to interact and connect with listeners. In community radio in South Africa, there has been an increasing but uneven use of social network sites, and even a negative correlation between the number of listeners and the number of followers on social media (Bosch, 2014). This anomaly is partly explained by the economic inequalities of South African society, with some of the larger radio stations targeting poorer communities that are unable to afford internet connectivity (Bosch, 2014). Nevertheless, social media provides an added dimension to the relationship that a radio station has with its local community, as it represents an additional tool with which to build these relationships through the two-way communication that it enables.

Furthermore, Bosch (2014) found that audiences already on social media tended to have greater access to, and participation in, community radio, with, for example, their messages being read on air. She also notes that the virtual and distributed nature of these networks is redefining the notion of a community, beyond geographic confines. In addition to building a relationship with their listener base, broadcasters cannot ignore the potential of social media to complement fundraising efforts (Rooke & Odame, 2013) and to generate an additional advertising revenue stream (Albarran & Moellinger, 2013; Lietsala & Sirkkunen, 2008). However, this places greater demands on broadcasters, who must continue to pay attention to the quality of their radio broadcasting as well as effectively integrate their use of social media.

Quality in radio

Radio stations derive their assessment of quality from three main dimensions (Ngcezula, 2008), namely: (1) content produced by the station, such as programming, jingles and music played; (2) the style and overall effectiveness of radio hosts and presenters; and (3) listenership, which determines, in part, the advertising revenue potential of the station.

In South Africa, the Independent Communications Authority of South Africa (ICASA) is mandated by legislation to regulate "the telecommunications, broadcasting and postal industries in the public interest and ensure affordable services of a high quality for all South Africans" (ICASA, n.d.). ICASA fulfils several functions, including receiving and resolving complaints (ICASA, n.d.). Largely due to these regulatory requirements, the quality of radio programming receives a great deal of attention. A typical approach to monitoring the quality of programmes is for executive producers or management to conduct "snoop sessions", which involve listening to the station's content (Radio Talent, 2013). In addition, focus group discussions amongst shows' listeners are held to assess the quality of the on-air content from a listener's point of view (Freitas et al., 1998).

Media organisations are still trying to devise ways to integrate, fully and effectively, the use of social media into their operations (Alejandro, 2010). This is one reason why journalists and media organisations follow, or monitor, each other's activities online. They hope to identify best practices, or new ways of using these platforms (Harper, 2010). Despite some interest in the management of quality in radio, relatively little research has been done on quality management in media organisations. It is not surprising, then, that only a limited number of research studies have been conducted to investigate quality aspects of the use of social media, or online activity in radio. To date, research has focused on issues such as: accessing radio programming using online platforms (Evans & Smethers, 2001); using social media to grow radio listenership (Greer & Phipps, 2003); making radio more personal through social media (Lüders , 2008); investigating youth attitudes towards traditional media in the age of social media (Tapscott, 2009); exploring the place of traditional radio stations in the age of social media and online streaming services (e.g., Pandora, Apple Music and Spotify) (Winans, 2012); and determining how radio stations should be conducting themselves on social media (Resler, 2016).

2. Models for assessing organisational maturity and social media maturity

Operational excellence and organisational maturity

As one aspect of the quality process of an organisation, operational excellence can be described as the consistent and reliable execution of the business strategy (Wilson Perumal & Company, 2013). Organisational maturity is referred to when measuring the level of quality, and is defined by Torres (2014, p. 1) as "a measure of an organization's readiness and capability expressed through its people, processes, data and technologies and the consistent measurement practices that are in place". Models of organisational maturity have been developed, with their origins in the software industry (Wendler, 2012). These models are presented in the form of a matrix that is made up of five or six discrete and cumulative levels (or stages) of maturity, against which varies categories of performance are measured (Wendler, 2012).

While the publication of maturity models is still dominated by the software industry, there has been a rapid growth in the number of areas where maturity models are applied (Tarhan, Turetken & Reijers, 2016; Wendler, 2012) and the development of more generic models such as the business process orientation (BPO) maturity model (Tarhan et al., 2016). The BPO maturity model identifies five levels of maturity or quality, naming them as follows: ad hoc; defined; linked; integrated; and extended (Lockamy & McCormack, 2004). A second generic model, the capability maturity model (CMM) has been adapted from the BPO maturity model (Lockamy & McCormack, 2004, p. 276) and is a five-level generic maturity model used to assess an organisation's ability or capacity to deal with any type of proposed change (Perkins, 2012). According to Perkins (2012, p. 4), "CMM describes the behaviours, practices and processes of an organisation that enables them to reliably and sustainably produce required outcomes." The model adopts a multi-dimensional approach to assess an organisation's ability to adapt to a proposed change (Perkins, 2012). The basic premise of a third model—the organisational IT maturity (OITM) model—is that it specifically examines an organisation's ability to invest in, or implement, information technology solutions (Ragowsky, Licker & Gefen, 2012). This model has six levels, rather than the typical five, making use of a "level 0". These levels go from "ignorant" at level 0 to "aware" to "willing" to "trusting" to "accepting" and ultimately to "responsible" at level 5 (Ragowsky et al., 2012).

Organisational maturity models incorporating social media

The social organisation model (Campbell & Gray, 2014), developed by PMWorks in Australia, is used to assess the likelihood of success when incorporating social media into the operations of an organisation. The basic premise of the model is that the business must first understand the model of social organisation which prevails, before implementing social media, as a failure to do so may "hamper or possibly kill the successful uptake of social media within the organisation" (Campbell & Gray, 2014, p. 9). The five stages, or levels of the social organisation model are: (1) traditional: traditional hierarchical communication structure; (2) decentralised: no centre of power and influence; (3) hub and spoke: communication occurs with a common purpose; (4) dandelion: multiple hub and spoke networks working towards a common purpose or goal; and (5) honeycomb: fully integrated communication without hierarchical structure but with a common purpose (Campbell & Gray, 2014). The least favourable of the five levels is the first one—traditional—which hinders the adoption of social media and is focused on hierarchical communication, while in the fifth level—honeycomb—an organisation is fully adapted to social media (Campbell & Gray, 2014).

Social media maturity model (SMMM)

Organisations are increasingly using social media, in recognition of its strategic importance for marketing, communication and other purposes, and yet there is a paucity of research on social media management in organisations (Chung, Andreev, Benyoucef, Duane & O'Reilly, 2017; Duane & O'Reilly, 2016). PMWorks has put forward a social media maturity model that is focused specifically on the employees of an organisation and how much they are involved with social media in their lives, both personally and professionally (Campbell & Gray, 2014). Given its focus on employee use, the relevance of the work of Campbell and Gray (2014) to this study was recognised. The five levels are labelled and defined as follows (Campbell & Gray, 2014):

- Level 1: Ad hoc or absent: Some individuals are literate in social media and use it for their own personal purposes, mostly, or even exclusively, outside of work.

- Level 2: Isolated users connected: Some individuals use social media to connect with other workers within the organisation for work and/or social purposes. While nothing is officially organised, experimentation and use are tolerated within the organisation.
- Level 3: Emergent community: An application for social media is identified and implemented within a group or in a specific project. This may emerge from organic growth, or an executive sponsor (e.g., marketing), or to support communication efforts associated with a specific project.
- Level 4: Community: Organisation-wide models and tools are broadly deployed for managing social media content and platforms, and some metrics are implemented. Social media is used to support the management of cultural change at the corporate level.
- Level 5: Fully networked: All employees are connected to the organisational social network and have a recognised role. Social media values and practices are an embedded part of the culture, and individuals operate in multiple relationships across the organisation. The inclusion of metrics and determining the return on investment are an accepted part of the model. Social media is an accepted part of the change management tool set and/or marketing mix.

3. Development and application of an SMMM for community radio

It was decided that the organisational maturity of Rhodes Music Radio's use of social media should be rated using an adapted version of the Campbell and Gray (2014) SMMM, with the adaptations drawing on other models from the literature outlined above (Lockamy & McCormack, 2004; Perkins, 2012; Ragowsky et al., 2012).

Five-level scale

The adapted SMMM has a five-level scale, with 1 being the lowest level of maturity and 5 being the highest (Lockamy & McCormack, 2004; Ragowsky et al., 2012). Each level is matched with a general description of characteristics, as adapted from the Lockamy and McCormack (2004) BPO maturity model and the Campbell and Gray (2014) SMMM. The levels of these models differ somewhat. Lockamy and McCormack (2004) include an experimental level between Campbell and Gray's (2014) levels of ad hoc and defined. This level was included to provide a more granular distinction of levels at the lower end of maturity. Furthermore, Lockamy and McCormack's (2004) extended level, which describes multi-firm networks, was not included, given the interest in the maturity of social media use in a single entity, namely RMR. The levels, as outlined in Table 1 in ascending order of maturity from 1 to 5, are therefore: ad hoc; experimental; defined; linked; and integrated.

Table 1: SMMM rating scale for a community radio station

Level	Characteristics
Level 1: Ad hoc	The organisation makes little to no use of social media. Usage is confined to a few individuals who occasionally use social media during shows.
Level 2: Experimental	Some individuals or departments begin to use social media for personal branding purposes or to connect with other similar parties. Usage is spurred by external stakeholders who expose the organisation to social media influence. No systems exist as yet.
Level 3: Defined	Social media used formally in certain departments to engage with stakeholders. Organisation has a formal presence on social media across multiple platforms. Brand is beginning to grow online. Staff members begin to have training on rules and guidelines for social media conduct.
Level 4: Linked	Organisation-wide models and tools are broadly deployed for managing social media content and platforms, some metrics are implemented and monitored, culture is moving towards social media being used in all departments. At the organisational level, social media is now recognised as having strategic value. The organisational structure is adjusted to cater for this. Training and engagement are the norm.
Level 5; Integrated	All staff members and departments are aware of and fully plugged into the social media of the organisation. Policy framework is fully in place and guides issues around social media specifically. Social media used across all departments, with each having its own agenda and uses for online platforms. Online activity is fully integrated with social media having full skills and technical support, as well as providing a revenue stream for the organisation. The brand of the organisation is well articulated on social media with full buy-in from staff members.

Source: Adapted from Campbell and Gray (2014)

This SMMM uses model descriptions at each level to describe the general level of maturity (Campbell & Gray, 2014; Ragowsky et al., 2012). With these descriptions as a base, the SMMM uses more specific descriptions at each level of maturity for the specific factor to be investigated.

Organisational spheres

The organisational spheres chosen for application of the model were:

- organisation-wide spheres: (1) policy and (2) monitoring.
- all the RMR departmental operational spheres, namely: human resources, programming and production, technical, marketing and branding, music, sales and advertising, communication, news, and on-air programming.

Data collection

The model was applied to RMR using two sources of data, namely the RMR's "Operational Policy" document and 14 interviews with RMR staff, including: the station manager, all nine functional managers, and four presenters. All the interviews were conducted within a month and face-to-face, and—with the permission of the interviewees—were audio recorded. The sources of information for developing the SMMM were therefore RMR staff members, who were asked questions during the semi-structured interviews that were customised to their area of functioning. For the most part, the sources had an intimate knowledge of how their department was making use of social media, or of how their department's efforts were contributing to the overall organisation-wide social media use of the station.

Deductive thematic analysis (Boyatzis, 1998; Braun & Clarke, 2006) was used to analyse the data. In accordance with the model, the assessment was focused on finding out which systems the station has in place to make effective use of social media—both generally and within individual departments, and at what level of maturity. For two organisation-wide spheres, as well as for each department, the data collected was summarised and compared to the SMMM rating scale descriptors as set out in Table 1, to reach a judgement on the level of maturity. In addition, based on the summaries, short descriptions of level characteristics were formulated. Table 2 summarises the SMMM's organisational spheres and maturity level characteristics.

Table 2: Organisational spheres and level characteristics

Organisational spheres		Maturity level characteristics				
Organisation-wide spheres	**Departmental-level operational spheres**	**1 Ad hoc**	**2 Experimental**	**3 Defined**	**4 Linked**	**5 Integrated**
Policy social media strategy		*None*	*Social media dealt with using other existing policy or policies*	*Social media policy in development*	*Preliminary enforcement of policy*	*Full policy in place which directs all station social media efforts*
Monitoring social media listening and monitoring		*No systems in place*	*Monitor basic activity and simple metrics online*	*Tracking trends on various social media*	*Use analytic tools like Google and Twitter analytics*	*Full monitoring of all platforms with regular reporting*

	Human resources	*No training, norms or code of conduct for online activity*	*Social media training – occasional and unplanned*	*Establishing a set of norms for conduct and training on social media for staff*	*Enforcement of norms and training*	*Social media becomes integrated into staff training and development*
	Programming and production	*Limited consideration in content production*	*Use social media as a secondary resource/ channel for content*	*Developing norms in how to use social media in content production*	*Social media plan for certain shows, not all*	*Social media plan for all shows*
	Technical	*No specific technical support given to social media*	*Social media used within existing technical support structures*	*Developing technical support norms for social media use*	*Support systems in place for most platforms*	*Full technical support*
	Marketing and branding	*Little to no presence online*	*Brand exists on social media with no set identity or structure*	*Developing brand identity through social media properties*	*Communicate brand identity to the station and staff*	*All internet and social media properties aligned with one brand vision*
	Music	*Little to no social media acknowledgement of music and artists*	*Acknowledgement of artists and music on social media occasional and unstructured*	*Introduce social media formally into on air music playing*	*Social media acknowledgement where information is available*	*All songs played accompanied by social media acknowledgement of artists*
	Sales and advertising	*No part in sales promotion*	*Occasional use of social media in advertising agreements and projects*	*Introduce social media formally into advertising agreements*	*Creating different sales packages with varying levels of social media engagement*	*Advertising agreements include full social media exposure as standard*
	Communication	*No use of social media in internal staff communication*	*Occasional use of social media for less important or casual announcements*	*Social media used to dispense both formal and informal communication*	*Social media used formally as an alternative communication channel*	*All internal communication explicitly conveyed using both email and social media*
	News	*No expectation of social media use to broadcast news stories or headlines*	*RMR News uses social media for certain events*	*Social media only used to give updates on specific types of events e.g., crises and live events*	*Social media used formally as an alternative broadcast channel for news*	*Full integration of social media to accompany all news broadcasts and live events*
	On-air programming	*No expectation to use social media in radio work*	*Staff members use social media if they wish to*	*Staff members expected to have social media accounts*	*Staff use social media during shows and for content production*	*Staff use their personal social media to promote the social media of the station*

Table 3 lists the departments that constitute the operations of RMR and describes the elements with relevance to the SMMM that were investigated in each departmental sphere. After first assessing the social media maturity of each department, an aggregate maturity level for the whole organisation was then determined.

Table 3: Elements investigated in each departmental-level operational sphere

Departmental-level operational spheres	**Elements**
Human resources	The Human Resources Department has programmes in place that help staff members to work with social media in the day-to-day presenting and production of shows.
Programming and production	The role of social media in the production of content for shows (e.g., using social media as a source for content, news, features and trends; systems to ensure that content sourced online is true and accurate).
Technical	The role of the Technical Department in the use of social media (e.g., ensuring that staff have access to working computers, RMR's internal computer network and the internet).
Marketing and branding	Online branding of the radio station and ensuring consistency over the various platforms that the station uses to promote or present itself, including social media.
Music	The role of social media in the sourcing, programming and distribution of music, and in interactions with the music industry.
Sales and advertising	The role of social media in bringing revenue to the station, including the nature of advertising agreements and services, and the utilisation and integration of all media for advertising (e.g., during on-air programming and on online platforms).

Communication	The role of social media in communication, particularly with staff members, RMR student society members, and the public at large.
News	How social media is used as a source of news content and to inform the news stories that are covered.
On-air program-ming	How presenters and producers are using social media to gather content for their shows and to communicate with the public about their shows.

4. Findings

Organisation-wide spheres: policy and monitoring

It was found that RMR did not have a formal social media policy in place, but had other working documents that it used as guidelines. The main document used for the day-to-day running of the station was an Operational Policy document that was formulated in 2014. Regarding the use of social media at the station, the Operational Policy was used as a guideline for how staff should conduct themselves online, both professionally and personally. The policy indicated that staff members should not act in ways that bring the name of the station into disrepute or use language on air that is derogatory, for example. This policy originally applied to the general conduct of staff members at RMR, but had since applied to the conduct of staff members in their use of social media. A Social Media Policy was being developed at the time of the field research and still had to be finalised and implemented.

As a station, RMR was using Facebook, Twitter and Instagram. In terms of administration of the different social media accounts, the following portfolios had administrative access on behalf of the station: the Station Manager, the Deputy Station Manager, Communications, Marketing and Brands, and Social Media. When live events were posted, the content for the various accounts was verified by the Social Media Manager.

RMR was monitoring its performance on social media using the analytical tools made available by the different networks, and through feedback received by the station in the form of word-of-mouth and written comments. However, the station had no benchmarks in place to gauge the performance of social media posts, and no formal or systematic way of monitoring the social media activities of staff members to ascertain the quality and integration of social media use.

Departmental-level operational spheres

Human resources

Internally, staff members were expected to participate as much as possible on social media, in ways that helped to promote the station and its programming. However, staff had not received any formal training from RMR on social media use. No training was offered and no guidelines on responsible behaviour were available. Instead, staff had learnt through their own research and experience. Presenters followed national and local media organisations that always seemed to be up to date with what was happening nationally, and that updated their social media platforms frequently. Individuals with national profiles in radio were followed, as well as some with a local profile.

Programming and production

RMR considered social media to be a major source of content for its programming. The production team tended to rely on credible or established news outlets and media organisations to verify the content of stories sourced from social media, and the Production Manager controlled the type of content that was aired, by approving show content plans before shows went on air.

Presenters recognised that social media helped them to stay abreast of trends and the general state of society. One interviewee was of the view that the public's expectation was that presenters "should be informed about what is going on in the society, since they are the people who are a voice for the people." Another interviewee noted that listeners expected presenters to interact with them online when presenting their shows on radio. However, interviewees were of the view that listeners expected presenters to stay neutral on radio and in social media, since they were viewed as journalists. As one interviewee stated: "One needs to be unbiased and I find that my interactions on social media remain consistent whether I'm dealing on a personal or professional level."

Technical

The technical team was responsible for setting up equipment, including ensuring that computers are in working condition and that they can access the internet. While the technical team members were trained as sound technicians, with the expanding scope of their work, they had to develop expertise in the areas of IT, networking and engineering as well.

Marketing and branding

RMR used Twitter, Instagram and Facebook to communicate and market its brand. The station also derived some benefit for its brand through the personal social media accounts and networks of RMR staff. However, it was difficult to monitor how staff members carried the RMR brand online. The Marketing Manager said: "There are no systems in place to help maintain the values, mission and brand image of RMR. There is room for improvement when it comes to RMR's efforts to grow its brand using social media."

Music

RMR's Music Department engaged with the music industry using social media as a channel of communication. Formal communication with public relations companies promoting songs took place through email. Music submissions were mainly done using digital submissions or email, with the sending of physical CDs to the station "becoming less by the week". It was not possible for songs to be added to RMR's library from social media interaction, but when songs were play listed or added to the music library, this was acknowledged on Twitter.

Recording companies and artists tended to interact with RMR on their various social media platforms when their music was played on RMR. Twitter seems to be the music industry's preferred platform, because of its immediacy and the capability to gauge trends on this platform.

Sales and advertising
While potential advertisers were made aware of RMR's presence and engagement on social media through statistics and website links, the main channel for advertising was on-air advertising, and RMR did not charge for advertising on its social media, but offered it as an added benefit to advertisers. Therefore, the radio station did not generate any revenue directly from its social media platforms. Furthermore, competitions were used as a vehicle to get people to view RMR's social media platforms and thereby to view the advertising content placed there.

Communication
The Communications Manager highlighted that the official channel for internal communication for staff members was email, but recently this had been extended to the use of social media: a special Facebook group was established for staff. Email was still used for communication with the RMR Club. For external communications, RMR had established a social media presence and now had to work on increasing the level of interaction with its online platforms.

News
RMR used social media as a source of news and content. RMR recognised that social media can be a biased news source, but there were no formal systems in place at RMR to check the credibility of sources. However, the news team tried to fact check stories before reporting on them. RMR News operated as a broadcast news team with on-air bulletins being the only way in which RMR conveyed news to people. RMR did not publish news anywhere else.

Overall assessment
Table 4 provides a summary of the assessment of RMR's social media maturity. According to the model, the station was assessed as being at level 3 maturity overall in its social media use, with room for improvement. In Table 1, a level 3 maturity was described as "defined", meaning that social media was used formally in some departments. As set out in Table 4, three departments were found to be at level 3, and five at level 4, with only the Technical Department rated at level 2 (as skills related to social media support were still being developed in that department). Furthermore, the organisation had a formal presence across multiple social media platforms, and there was evidence to suggest that the station's brand was beginning to grow online. RMR had also begun tracking the trends in its social media presence. Furthermore, consistent with the level 3 descriptor, staff members were being trained in social media use, and there were rules and guidelines related to social media conduct, even though a formal policy on social media was still to be finalised.

Table 4: Assessment of RMR's social media maturity

Organisational spheres		**Findings on level characteristics**				
Organisation-wide spheres	Departmetal-level operational spheres	Ad Hoc	Experimental	Defined	Linked	Integrated
Policy social media strategy		*None*	*Social media dealt with using other existing policy or policies*	*Social media policy in development*	*Preliminary enforcement of policy*	*Full policy in place, which directs all station social media efforts*
Monitoring social media listening and monitoring		*No systems in place*	*Monitor basic activity and simple metrics online*	*Tracking trends on various social media*	*Use analytic tools like Google and Twitter analytics*	*Full monitoring of all platforms with regular reporting*
	Human resources	*No training, norms or code of conduct for online activity*	*Social media training – occasional and unplanned*	*Establishing a set of norms for conduct and training on social media for staff*	*Enforcement of norms and training*	*Social media becomes integrated into staff training and development*
	Programming and production	*Limited consideration in content production*	*Use social media as a secondary resource/ channel for content*	*Developing norms in how to use social media in content production*	*Social media plan for certain shows, not all*	*Social media plan for all shows*
	Technical	*No specific technical support given to social media*	*Social media used within existing technical support structures*	*Developing technical support norms for social media use*	*Support systems in place for most platforms*	*Full technical support*

	Marketing and branding	*Little to no presence online*	*Brand exists on social media with no set identity or structure*	*Developing brand identity through social media properties*	*Communicate brand identity to the station and staff*	*All internet and social media properties aligned with one brand vision*
	Music	*Little to no social media acknowledgement of music and artists*	*Acknowledgement of artists and music on social media occasional and unstructured*	*Introduce social media formally into on air music playing*	*Social media acknowledgement where information is available*	*All songs played accompanied by social media acknowledgement of artists*
	Sales and advertising	*No part in sales promotion*	*Occasional use of social media in advertising agreements and projects*	*Introduce social media formally into advertising agreements*	*Creating different sales packages with varying levels of social media engagement*	*Advertising agreements include full social media exposure as standard*
	Communication	*No use of social media in internal staff communication*	*Occasional use of social media for less important or casual announcements*	*Social media used to dispense both formal and informal communication*	*Social media used formally as an alternative communication channel*	*All internal communication explicitly conveyed using both email and social media*
	RMR News	*No expectation of social media use to broadcast news stories or headlines*	*RMR News uses social media for certain events*	*Social media only used to give updates on specific types of events e.g., crises and live events*	*Social media used formally as an alternative broadcast channel for news*	*Full integration of social media to accompany all news broadcasts and live events*
	On-air programming	*No expectation to use social media in radio work*	*Staff members use social media if they wish to*	*Staff members expected to have social media accounts*	*Staff use social media during shows and for content production*	*Staff use their personal social media to promote the social media of the station*

5. Recommendations and future research

We now provide our recommendations for how RMR can increase its social maturity level, followed by recommendations for further research.

Technical skills

The department that required the most urgent attention was the Technical Department, to develop its members' capacity so that they could provide the required support for social media. This required creating a position responsible for computer-related technical support, and the recruitment of someone with the relevant skills to fill the post.

Internal capacity development

To develop capacity internally, the station needed to urgently finalise and endorse its Social Media Policy. Thereafter, RMR staff had to be trained on the policy and how to apply it properly in their work. Finally, once staff were informed of the Social Media Policy and formally trained in the use of social media, they had to be encouraged to become more involved in the social media of the station, by following the various RMR accounts and engaging with listeners and other staff members on these platforms.

Integration of social media into activities

Once internal social media capacity had been developed, the station needed to find ways to better integrate social media into its activities. First, it had to find ways to connect more frequently with the Rhodes University and Makhanda communities, as these two audiences formed the main listener base for the station's estimated 3,000 listeners. RMR also needed to find ways to convert its social media following into listeners of its broadcast programming. Marketing through live broadcast events that are also promoted through social media could be an effective means to achieve this. Furthermore, RMR could try using new social media platforms such as Snapchat and Google Plus, to complement its traditional Facebook, Twitter and Instagram platforms. These recommendations highlight the need for RMR to adopt a more strategic and integrated approach in its use of a combination of radio and social media, to provide a more holistic set of media to its audience.

Future research

The SMMM developed in this study seemed to be appropriate for assessing the social media maturity level of RMR and appeared to be practically useful in identifying areas for the station's potential improvement. However, the research was of limited scope given that it involved only one community radio station. It is therefore recommended that further research be undertaken with the same model at other community radio stations, to test the utility of the model in other contexts.

References

Albarran, A. B., & Moellinger, T. (2013). Traditional media companies in the US and social media: What's the strategy? In M. Friedrichsen (Ed.), *Handbook of social media management* (pp. 9–24). Berlin: Springer. https://doi.org/10.1007/978-3-642-28897-5_2

Alejandro, J. (2010). *Journalism in the age of social media*. Reuters Institute Fellowship Paper. Reuters Institute for the Study of Journalism, University of Oxford.

Atton, C. (2003). What is alternative journalism? *Journalism*, *4*(3), 267–272. https://doi.org/10.1177/14648849030043001

Barlow, W. (1988). Community radio in the US: The struggle for a democratic medium. *Media, Culture & Society*, *10*(1), 81–105. https://doi.org/10.1177/016344388010001006

Bosch, T. (2014). Social media and community radio journalism in South Africa. *Digital Journalism*, *2*(1), 29–43. https://doi.org/10.1080/21670811.2013.850199

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: Sage.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brevini, B. (2015). Public service and community media. In *The international encyclopedia of digital communication and society* (1st ed.), (pp. 1–9). Hoboken, NJ: John Wiley and Sons. https://doi.org/10.1002/9781118767771.wbiedcs045

Campbell, C., & Gray, P. (2014). *Social media for change management*. St. Leonards, Australia: PMWorks.

Chung, A. Q., Andreev, P., Benyoucef, M., Duane, A., & O'Reilly, P. (2017). Managing an organisation's social media presence: An empirical stages of growth model. *International Journal of Information Management, 37*(1), 1405–1417. https://doi.org/10.1016/j.ijinfomgt.2016.10.003

Correia, R., Vieira, J., & Aparicio, M. (2019). Community radio stations sustainability model: An open-source solution. *Radio Journal: International Studies in Broadcast & Audio Media*, *17*(1), 29–45. https://doi.org/10.1386/rjao.17.1.29_1

Da Costa, P. (2012). The growing pains of community radio in Africa: Emerging lessons towards sustainability. *Nordicom Review*, *33*(Special Issue), 135–148. https://doi.org/10.2478/nor-2013-0031

Duane, A., & O'Reilly, P. (2016). A stage model of social media adoption. *Journal of Advances in Management Sciences & Information Systems, 2*(2016), 77–93. https://doi.org/10.6000/2371-1647.2016.02.07

Evans, C. L., & Smethers, J. S. (2001). Streaming into the future: A Delphi study of broadcasters' attitudes toward cyber radio stations. *Journal of Radio Studies*, *8*(1), 5–28. https://doi.org/10.1207/s15506843jrs0801_4

Fombad, M. C., & Jiyane, G. V. (2019). The role of community radios in information dissemination to rural women in South Africa. *Journal of Librarianship and Information Science*, *51*(1), 47–58. https://doi.org/10.1177/0961000616668960

Freitas, H., Oliveira, M., Jenkins, M., & Popjoy, O. (1998). *The focus group, a qualitative research method*. ISRC Working Paper 010298. Information Systems Research Group, Merrick School of Business, University of Baltimore.

Gavaza, M. A. (2017). *Assessing the organisational maturity level of Rhodes Music Radio with the introduction of social media*. Master's Thesis, Rhodes University, Makhanda (Grahamstown), South Africa.

Greer, C., & Phipps, T. (2003). Noncommercial religious radio stations and the web. *Journal of Radio Studies*, *10*(1), 17–32. https://doi.org/10.1207/s15506843jrs1001_4

Harper, R. A. (2010). The social media revolution: Exploring the impact on journalism and news media organizations. *Inquiries Journal: Social Sciences, Arts and Humanities*, *2*(3), 1–4.

Hendy, D. (2013). *Radio in the global age*. Oxford: Blackwell.

Hlongwana, K. W., Zitha, A., Mabuza, A. M., & Maharaj, R. (2011). Knowledge and practices towards malaria amongst residents of Bushbuckridge, Mpumalanga, South Africa. *African Journal of Primary Health Care & Family Medicine*, *3*(1), 1–9. https://doi.org/10.4102/phcfm.v3i1.257

Independent Communication Authority of South Africa (ICASA). (n.d.). Our mandate [Web page]. Retrieved from https://www.icasa.org.za/pages/our-mandate

Jankowski, N. (2003). Community media research: A quest for theoretically-grounded models. *Javnost – The Public*, *10*(1), 5–14. https://doi.org/10.1080/13183222.2003.11008818

Jordaan, M. (2013). Poke me, I'm a journalist: The impact of Facebook and Twitter on newsroom routines and cultures at two South African weeklies. *Ecquid Novi: African Journalism Studies*, *34*(1), 21–35. https://doi.org/10.1080/02560054.2013.767421

Lietsala, K., & Sirkkunen, E. (2008). *Social media. Introduction to the tools and processes of participatory economy*. Tampere, Finland: Tampere University Press.

Lewis, P. M. (2000). Private passion, public neglect: The cultural status of radio. *International Journal of Cultural Studies*, *3*(2), 160–167. https://doi.org/10.1177/136787790000300203

Lewis, P. M., & Booth, J. (1989). *The invisible medium: Public, commercial, and community radio*. New York: Macmillan Education.

Lüders, M. (2008). Conceptualising personal media. *New Media & Society*, *10*(5), 683–702. https://doi.org/10.1177/1461444808094352

Lockamy, A., & McCormack, A. L. K. (2004). The development of a supply chain management process maturity model using the concepts of business process orientation. *Supply Chain Management: An International Journal*, *9*(4), 272–278. https://doi.org/10.1108/13598540410550019

MacFarland, D. T. (2016). *Contemporary radio programming strategies*. New York: Routledge. https://doi.org/10.4324/9781315443522

Mawokomayi, B., & Osunkunle, O. O. (2019). Listeners' perceptions of Forte FM's role in facilitating community development in Alice, South Africa, *Critical Arts*, *33*(1), 88–100. https://doi.org/10.1080/02560046.2019.1631364

Mhlanga, B. (2016). The return of the local: Community radio as dialogic and participatory. In A. Salawu & M. B. Chibita (Eds.), *Indigenous language media, language politics and democracy in Africa* (pp. 87–112). London: Palgrave Macmillan. https://doi.org/10.1057/9781137547309_5

Makoye, H. F. (2006). Tale-telling tradition and popularity of radio soap opera in Tanzania: The case of Twende na Wakati. *Utafiti Journal*, 7(1), 91–99.

Medeossi, B. J., Stadler, J., & Delany-Moretlwe, S. (2014). 'I heard about this study on the radio': Using community radio to strengthen good participatory practice in HIV prevention trials. *BMC Public Health*, *14*(1), 876–883. https://doi.org/10.1186/1471-2458-14-876

Megwa, E. R. (2007). Community radio stations as community technology centers: An evaluation of the development impact of technological hybridization on stakeholder communities in South Africa. *Journal of Radio Studies*, *14*(1), 49–66. https://doi.org/10.1080/10955040701301847

Mhagama, P. (2016). The importance of participation in development through community radio: A case study of Nkhotakota community radio station in Malawi. *Critical Arts*, *30*(1), 45–61. https://doi.org/10.1080/02560046.2016.1164384

Ngcezula, A. T. (2008). *Developing a business model for a community radio station in Port Elizabeth: A case study*. Master's thesis, Nelson Mandela University, Port Elizabeth, South Africa.

Oduaran, C. & Nelson, O. (2019). Community radio, women and family development issues in South Africa: An experiential study. *Journal of International Women's Studies*, *20*(7), 102–112.

Olorunnisola, A. A. (2002) Community radio: Participatory communication in post-apartheid South Africa. *Journal of Radio Studies*, *9*(1), 126–145. https://doi.org/10.1207/s15506843jrs0901_11

Order, S. (2015). Towards a contingency-based approach to value for community radio. *Radio Journal: International Studies in Broadcast & Audio Media*, *13*(1–2), 121–138. https://doi.org/10.1386/rjao.13.1-2.121_1

Owen, D. (2018). Who's talking? Who's listening? The new politics of radio talk shows. In S. C. Craig (Ed.), *Broken contract? Changing relationships between Americans and their government* (pp. 127–146). New York: Routledge. https://doi.org/10.4324/9780429502002-9

Perkins, C. (2012). *Organisational change management maturity*. Unpublished report for the CMI White Paper. Sydney: Change Management Institute.

Radio Talent (2013). *Walking on air: How to be a radio presenter: Volume 1 (media success)*. Los Gatos, CA: Smashwords.

Ragowsky, A., Licker, P. S., & Gefen, D. (2012). Organizational IT maturity (OITM): A measure of organizational readiness and effectiveness to obtain value from its information technology. *Information Systems Management*. *29*(2), 148–160. https://doi.org/10.1080/10580530.2012.662104

Republic of South Africa (RSA). (1993). Independent Broadcasting Authority Act (IBA Act), No. 153 of 1993. Retrieved from https://www.wipo.int/edocs/lexdocs/laws/en/za/za064en.pdf

RSA. (2005). Electronic Communications Act (ECA), No. 6 of 2005. Retrieved from https://www.wipo.int/edocs/lexdocs/laws/en/za/za082en.pdf

Resler, S. (2016, June 10). Here's what your radio station should be sharing on social media. Jacobs Media Strategies [Blog post]. Retrieved from http://jacobsmedia.com/heres-what-your-radio-station-should-be-sharing-on-social-media

Rhodes Music Radio (RMR). (2007). Constitution. Unpublished internal policy document. Makhanda (Grahamstown), South Africa: Rhodes Music Radio.

RMR. (2015). Rhodes Music Radio business model. Unpublished management strategy document. Makhanda (Grahamstown), South Africa: Rhodes Music Radio.

RMR. (2015). About us [Web page]. Retrieved from http://www.rhodesmusicradio.co.za/about-us/

Rodríguez, J. M. R. (2005). Indigenous radio stations in Mexico: A catalyst for social cohesion and cultural strength. *Radio Journal: International Studies in Broadcast & Audio Media*, *3*(3), 155–169. https://doi.org/10.1386/rajo.3.3.155_1

Rooke, B., & Odame, H. H. (2013). 'I have to blog a blog too?' Radio jocks and online blogging. *Journal of Radio & Audio Media*, *20*(1), 35–52. https://doi.org/10.1080/19376529.2013.777342

Scifo, S. (2015). Technology, empowerment and community radio. *Revista Mídia e Cotidiano*, *7*(7), 84–111. https://doi.org/10.22409/ppgmc.v7i7.9754

Sparks, C. (2009). South African media in transition. *Journal of African Media Studies*, *1*(2), 195–220. https://doi.org/10.1386/jams.1.2.195/1

Tacchi, J. (2002). Transforming the mediascape in South Africa: The continuing struggle to develop community radio. *Media International Australia, Incorporating Culture and Policy*, *103*(1), 68–77. https://doi.org/10.1177/1329878X0210300110

Tacchi, J. (2003). Promise of citizens' media: Lessons from community radio in Australia and South Africa. *Economic and Political Weekly*, *38*(22), 2183–2187.

Tapscott, D. (2009). *Grown up digital: How the net generation is changing your world*. New York: McGraw–Hill.

Tarhan, A., Turetken, O., & Reijers, H. A. (2016). Business process maturity models: A systematic literature review. *Information and Software Technology*, *75*(2016), 122–134. https://doi.org/10.1016/j.infsof.2016.01.010

Torres, C. (2014, October 31). Understanding organizational maturity [Blog post]. Retrieved from http://blogs.vmware.com/management/author/torresc

Wabwire, J. (2013). The role of community radio in development of the rural poor. *New Media and Mass Communication*, *10*, 40–47.

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. https://doi.org/10.1016/j.infsof.2012.07.007

Wilson Perumal & Company (2013, May 10). A better definition of operational excellence [Blog post]. Retrieved from http://www.wilsonperumal.com/blog/a-better-definition-of-operational-excellence

Winans, S. (2012, April 11). Radio and social media [Blog post]. *Social Media Sun*. Retrieved from http://socialmediasun.com/radio-and-social-media

World Population Review (2019). Population of cities in South Africa [Web page]. Retrieved from http://worldpopulationreview.com/countries/south-africa-population/cities

Teachers' ICT Adoption in South African Rural Schools: A Study of Technology Readiness and Implications for the South Africa Connect Broadband Policy

Samwel Dick Mwapwele
Postdoctoral Fellow, College of Science, Engineering and Technology (CSET), Science Campus, University of South Africa (UNISA), Florida, Johannesburg
https://orcid.org/0000-0003-2316-262X

Mario Marais
Principal Researcher, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0003-3302-1230

Sifiso Dlamini
Researcher, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0002-3756-4980

Judy van Biljon
SARChI Chair in ICT4D, College of Science, Engineering and Technology (CSET), Science Campus, University of South Africa (UNISA), Florida, Johannesburg
https://orcid.org/0000-0002-4646-1641

Abstract

The South Africa Connect national broadband policy of 2013 aims to ensure that the country achieves universal internet access by 2030, thereby fostering digital skills development. This study investigates one dimension of the South Africa Connect policy objectives, by considering rural teachers' adoption of information and communication technologies (ICTs) for teaching and learning at 24 schools. This research used baseline data from the Information and Communication Technology for Education (ICT4E) project undertaken in rural schools in seven South African provinces. The technology readiness index (TRI) was used as the theoretical lens. We found that the vast majority of the teachers surveyed were optimistic about the use of ICTs for teaching and learning, which suggests teachers' readiness to use ICTs despite the existing financial, technical and digital skills challenges at their schools. We also found that the majority of the schools had policies prohibiting student use of personal digital devices, apart from calculators, on school premises. In our analysis, these policies potentially conflict with the objectives of South Africa Connect. This study contributes to theory and practice by offering empirical evidence of the usefulness of the TRI for presenting teachers' readiness to adopt ICTs in situations of conflicting forces. The study also has the potential to contribute to policy deliberations by highlighting the possible disconnect between the schools' bans on student personal digital devices and the objectives and targets set by the South Africa Connect policy.

Keywords
information and communication technologies (ICTs), schools, rural areas, teachers, adoption, teaching and learning, technology readiness index (TRI), South Africa, national broadband policy, South Africa Connect

Acknowledgements
This article draws on a conference paper presented at Digital Skills 2019: Digital Innovation and Transformation Conference, 29 August 2019, Boksburg, South Africa. We acknowledge the support for this research from the South African Department of Rural Development and Land Reform (DRDLR) ICT for Education (ICT4E) project. The ICT4E project was funded by the DRDLR and supported by the University of the Free State (UFS) through its training of teachers and National Rural Youth Service Corps (NARYSEC) youth at 24 schools in seven South African provinces. We also acknowledge the support of the ICT4E project research and implementation team at the Meraka Institute of the Council for Scientific and Industrial Research (CSIR). The research upon which this article is based was also supported by the South African Research Chairs Initiative (SARChI) of the Department of Science and Technology and National Research Foundation (Grant No. 98564).

DOI: https://doi.org/10.23962/10539/28658

Recommended citation
Mwapwele, S. D., Marais, M., Dlamini, S., & Van Biljon, J. (2019). Teachers' ICT adoption in South African rural schools: A study of technology readiness and implications for the South Africa Connect broadband policy. *The African Journal of Information and Communication (AJIC)*, 24, 1-21. https://doi.org/10.23962/10539/28658

1. Introduction

The fourth industrial revolution (4IR) is centred on the application of digital technologies so that distinctions between the physical, digital and biological spaces are reduced. Among the central manifestations of the 4IR are job automation and an always-connected, converged world (Eberhard et al., 2017). For a country to achieve the benefits of the 4IR, emphasis needs to be placed on building citizens' optimism through providing access to, and the skills to operate, digital technologies, i.e., emphasis needs to be placed on building citizens' skills competencies in the use of information and communication technologies (ICTs).

A country's ICT policies guide the adoption and use of technology by explicitly setting out what needs to be done to achieve national goals (Gibson, Broadley, Downie & Wallet, 2018). Educational technology policy development and implementation aim to facilitate the sustainable adoption and application of technology so that it assists the country's education system, through implementation by students, teachers, parents, principals and administrators. ICTs, which include internet, PCs and mobile devices (e.g., mobile phones, tablets and laptops), are used in schools with the expected national goals (outcomes) being improved access to and dissemination of teaching and learning materials (Hennessy, Harrison & Wamakote, 2010). National goals in education need to align with the United Nations Sustainable Development Goal (SDG) No. 4, which is to ensure that quality education is offered at all educational levels (Department of Basic Education, 2017; Gibson et al., 2018).

In developing countries, ICTs are proposed as tools to assist in reducing the digital divide, especially in education (Rena, 2008) where they can, among other things, provide access to secondary learning materials (Porter et al., 2016) with hard-copy textbooks still being the recommended primary sources (Eberhard et al., 2017). Notwithstanding the concerns raised by Hargittai (2010, p. 93) that researchers should be mindful of the "assumptions about widespread digital skills among [citizens]", African researchers have provided empirical evidence of the efficacy of building digital skills in education and of the spread of digitally enabled education. Kaliisa and Picard (2017), via a systematic review of literature from nine African countries on the use of mobile devices in higher education, find that smartphones are the predominant mobile devices used for learning, followed by tablets.

Rambe and Ng'ambi (2014) have found that students in South Africa can expand their digital skills through the use of Facebook. As a result of the positive empirical evidence witnessed in Ghana, Malawi and South Africa, Porter et al. (2016) conclude by urging relevant authorities in Sub-Saharan Africa to address the challenges faced by youth concerning the use of mobile devices for education. However, there is still very little empirical evidence from Africa on ICT adoption for teaching and learning in schools (Liebenberg, Benade and Ellis (2018) is among the notable exceptions), particularly from the perspective of teachers, and this gap necessitates research of the kind described in this article.

Like other developing countries, South Africa has policies aimed at boosting the adoption and use of ICTs, specifically in education. South Africa Connect, the country's national broadband policy of 2013, mandates the introduction of a broadband connection (with a download speed of at least 100 Mbps) to every primary school and secondary school as part of an initiative to ensure the countrywide availability of broadband internet access by the year 2030 (DoC, 2013). The policy positions the enhancement of teachers' and principals' internet connectivity as necessary to support access to, and the use of, learning materials that can enhance learning in classrooms and foster the development of students' digital skills.

Schools in South African rural areas suffer from shortages of teachers and of teaching and learning materials (Waller & Maxwell, 2017). Projects in South Africa, as in other countries around the world, are providing teachers with ICTs in order to assist them with teaching and to increase their ICT knowledge and skills (Botha, Herselman, Rametse & Maremi, 2017; Frohberg, Göth & Schwabe, 2009; Roberts & Vänskä, 2011). One element of focus has been on ensuring that the digital tools diffused in schools are sensitive to the schools' resource challenges and are sustainable. Central to this sustainability dimension are teachers' skills and attitudes with respect to the use of technology.

Many ICT interventions meet with failure when the recipients of the intervention struggle to sustain the tools introduced and used during the project. Among the reasons for such failures, it has been argued, are lack of fit between the ICTs and user need (Alsabawy, Cater-Steel & Soar, 2011; Avgerou, 2008). To limit the challenges of sustainability of interventions after completion of ICT interventions in school settings, teachers' ICT competencies and attitudes must be assessed, based on the ICTs they have personally adopted and used, prior to the introduction of new ICT tools.

In our study, we collected empirical data from 24 rural schools (primary and secondary) across seven South African provinces in order to seek answers to the following questions:

- what are rural South African teachers' experiences and attitudes in respect of the use of ICTs in support of teaching and learning?
- which technology readiness factors are impacting teachers' ICT adoption in support of teaching and learning?

The overall intention of the research was to interrogate an element of the objectives of the South Africa Connect national broadband policy (rural teacher ICT adoption), and in the process to extend our understanding of the factors that impact teachers' ICT use. The research applied the technology readiness index (TRI) as the theoretical framework to guide the investigation of teachers' ICT readiness and adoption.

2. Literature review

ICTs for teaching and learning in African schools

ICTs have received widespread optimism, adoption, and use in African countries, including use in educational provision (Barakabitze et al., 2019; Kafyulilo, 2014). For teachers, the spread of digital skills offers, among other things, opportunities for formalised recognition of their new competencies—as documented by Botha, Herselman, Rametse and Maremi (2017) in their research into the training of teachers in ICT use in rural schools in South Africa. Botha et al. (2017) looked at a training programme, as part of teacher professional development, whereby teachers received "badges" for skills acquired. Osakwe, Dlodlo and Jere (2017), in their research into Namibian secondary school teachers' and learners' perceptions of mobile learning, found that teachers and learners who owned mobile devices were accessing the internet, accessing social media, and searching for information, which shows that they had mastered digital skills and were participating in digitally-enabled informal educational pursuits outside the school setting.

Meanwhile, Yidana and Maazurre (2012) paint a less optimistic picture. They reveal the discomfort faced by Ghanaian teachers in integrating ICTs into their work due to, inter alia, insufficient digital skills caused by lack of integration of ICT adoption into teaching and learning. Omoniyi and Quadri (2013) have found evidence of insufficient ICT competency among a group of surveyed secondary school teachers in Ogun State, Nigeria.

South Africa Connect policy and its application in education

The South Africa Connect policy, published in 2013 by the Department of Communications (DoC) and currently driven by the newly created (in mid-2019) Department of Communications and Digital Technologies (DCDT), advocates for a digital society characterised by widespread ICT knowledge and use for individuals, communities, organisations, and the society as a whole (DoC, 2013; Hankel et al., 2017).[1] Digital education modalities, through innovations such as the internet, tablets, digital academic content (embedded in applications) on tablets, and mobile services, are positioned as offering hope to the nation towards attaining improved economic and social development (DoC, 2013) through digital education. Operationalising the policy must include the assessment of both innovations that are currently in use and those that are intended for diffusion and adoption.

South Africa Connect seeks to operationalise elements of South Africa's National Development Plan (NDP) of 2012 (NPC, 2012). The NDP provides a vision for the eradication of poverty in South Africa by the year 2030. Sustainable poverty eradication and education are inseparable (Avgerou, 2008; Fardon & Furniss, 1994; Ngwenyama, Andoh-Baidoo, Bollou & Olga, 2006). Education is required to help develop knowledge and skills that assist an individual to either join the job market or create job opportunities for others through innovative discoveries (Rena, 2006). Among other things, the NDP states that "children of today must be guaranteed access to high-quality education and professional training throughout their education and working life" (NPC, 2012, p. 366).

The South Africa Connect policy has, since its adoption in 2013, been augmented by two other policies: the National Integrated ICT Policy White Paper (DTPS, 2016) and the Policy on High Demand Spectrum and Policy Direction on the Licensing of a Wireless Open-Access Network (DTPS, 2019). The Policy on High-Demand

[1] The DCDT was formed in June 2019 through the merger of the Department of Communications (DoC) and the Department of Telecommunications and Postal Services (DTPS).

Spectrum, an extension of the White Paper, has little focus on schools. Meanwhile, the White Paper itself, in naming nine key challenges facing South Africa that ICTs need to assist in addressing, states that one of the challenges is that "[t]he quality of school education is poor" (DTPS, 2016, p. 8). The White Paper points to evidence in other countries that "connecting a school is often the first step to connecting a community …" (DTPS, 2016, p. 36). The policy insists on the need, as also stated in South Africa Connect, for schools and clinics to be key points of ICT access.

South African rural schools and demand for technology

Rural areas are defined as "farms and traditional areas characterized by low population density, low level of economic activity and low level of infrastructure" (Department of Basic Education, 2017, p. 20). Schools in South Africa's rural areas are faced with numerous challenges, including unstable electricity, high dropout rates, poor classroom infrastructure, security problems (Adukaite, Van Zyl, Er & Cantoni, 2017), and, with particular relevance for this study, shortages of qualified teachers and shortages of teaching and learning materials (Mestry & Ndhlovu, 2014). The Department of Basic Education (DBE) Rural Education Draft Policy of 2017 states that "it is difficult to recruit, retain and develop qualified teachers in a rural setting due to the distances of schools from towns, poor infrastructure and limited service delivery" (Department of Basic Education, 2017, p. 18). To assist in reducing this and other problems, the policy recommends increased diffusion of ICTs to rural schools.

ICTs are seen as empowering teachers by allowing them to, inter alia, access teaching content on the internet; develop a better understanding of content they are teaching; improve communication with colleagues when seeking support; participate in online training; and become more knowledgeable about ongoing political, social, economic and financial developments in the world (Hennessy et al., 2010; Kopcha, 2012).

Technology readiness index (TRI)

The technology readiness index (TRI) is a framework, initially developed by Parasuraman, to assess the ability of individuals to adopt and use technology (see Lai, 2008; Parasuraman & Colby, 2015; Summak, Baglibel & Samancioglu, 2010). The framework investigates individuals' intentions to adopt and use technology, primarily based on their *state of mind* rather than their *skills* (with, however, the recognition that digital skills may influence the state of mind). The TRI uses four concepts to understand an individual's (in this study, the individuals were teachers) state of mind, namely:

- optimism;
- innovativeness;
- discomfort; and
- insecurity (Parasuraman & Colby, 2015, p. 60).

In the TRI, *optimism* is characterised by the presence of a positive mindset, i.e., the belief that one can attain intended goals by using technology (Hennessy et al., 2010; Kopcha, 2012; Summak et al., 2010). For our study, we sought to identify instances where teachers believed that the use of technology could enhance classroom interactions and were thus optimistic that increased levels of learner engagement could be the outcome, together with improved learner results and improved digital skills (Partin & Lauderdale, 2013).

Innovativeness, in the TRI, refers to actions such as being the first in a cohort to acquire technology, displaying a willingness to use technology, and being a constant information-seeker in respect of new technologies (Falloon, 2013; Ifenthaler & Schweinbenz, 2013). An innovative individual will, thus, be someone who actively engages with sources of information in order to acquire information on upcoming technologies and the impact they will have on society. Once the technology is widely introduced in a society, the innovator becomes a source of support for colleagues. In the context of our study, we sought evidence of innovativeness in the form of teachers offering technical support to colleagues during the diffusion and adoption of technologies.

Discomfort is conceptualised, in the TRI, as being in evidence when people struggle, for example, to comprehend how technology is used (Frohberg et al., 2009; Ifenthaler & Schweinbenz, 2013). In our study, we looked for teachers expressing discomfort about potential lack of control regarding the use of technology, and expressing the views that suggested they found technology overwhelming. Further, we looked for teachers showing discomfort through expressing that they had limited knowledge and skills in respect of technology (Yidana & Maazurre, 2012).

In the TRI, *insecurity* is seen as resulting from distrust based on, for example, concerns about security and privacy (Ampofo et al., 2014; Summak et al., 2010). Discomfort and insecurity can affect teachers' perceptions of technology and limit the potential value of technology diffusion.

In line with the TRI, teacher optimism and innovativeness were, in our study, positioned as technology enablers, since they would assist teachers in their quest to adopt ICTs. Teacher discomfort and insecurity, meanwhile, were treated, in line with the TRI, as inhibitors of ICT adoption that might not only affect teachers' ICT adoption but might also affect how they viewed ICT use for teaching and learning, and how they viewed other teachers who readily adopt ICTs.

3. Research methodology

The study was conducted under the direction of the Next Generation Enterprises and Institutions cluster at the Council for Scientific and Industrial Research (CSIR). The research was funded by a South African Department of Rural Development and Land Reform (DRDLR) project entitled "Information and Communication Technology for Education" (ICT4E). The 24 rural schools from which we recruited teachers for data collection were primary and secondary schools identified by the DRDLR. The schools were from seven of the nine South African provinces, and 197 teachers served as respondents for data collection.

In South Africa, schools are classified according to the quintile system, starting at quintile 1 for the most disadvantaged schools and ending at quintile 5 for the most affluent schools (Mestry & Ndhlovu, 2014; Roberts & Vänskä, 2011). The 24 rural schools from which data was collected were all in either quintiles 1 or 2. The per-province breakdown of the 24 schools was as follows:

- Eastern Cape (2 schools);
- Free State (3);
- Gauteng (3);
- KwaZulu-Natal (3);
- Northern Cape (7);
- North West (3); and
- Limpopo (3).

A previous project, called ICT for Rural Education Development (ICT4RED) and conducted in the Eastern Cape Province, developed a curriculum that was used, during the diffusion of tablets in schools, to train teachers on their use. The intention of that project was not only to equip teachers with tablets but also to teach them teaching strategies while using the tablets. The results from the ICT4RED study (see Botha et al., 2017; Herselman & Botha, 2014; Marais & Van Biljon, 2017) were used to guide our ICT4E project's approach to understanding ICT adoption by schools. Before commencement of ICT4E, we collected baseline data in order to assess ICTs that teachers had already adopted and were using (1) in their personal lives, and (2) for teaching and learning. The intention of the baseline study was also to identify challenges that teachers faced in using ICTs for teaching and learning so that the ICT4E project could incorporate solutions to the challenges into the curriculum it used. The data on which this article is based, and as reported in the findings section, is a sub-set of the data we collected during that baseline study.

The data collection tool we used was a questionnaire composed of initial demographic questions followed by closed- and open-ended questions. In this article, we focus on the demographic information and the responses from some of the closed-ended questions. The findings from the open-ended questions are discussed in a different publication (see Mwapwele, Marais, Dlamini & Van Biljon, 2019).

The questionnaire was self-administered by teachers in the school settings from June to August 2016. Ethical clearance was received from the CSIR Research Ethics Committee (REC) and the principals of the schools where data was collected. The teachers were informed of the objectives of the research, and of ethical guidelines for consent, confidentiality, data collecting and data reporting. Teachers gave consent for data collection before they completed the self-administered questionnaires. We present our findings using a combination of frequency distributions and percentages from the data. In places where teachers did not respond to a particular question, we use "no response" to denote such an instance.

4. Findings

Teacher demographics and ICT access and ownership

Age

Among the 197 teachers surveyed, the youngest was 22 years old, and the oldest was 64. The majority of the teachers were aged between 46 and 50 years old.

Gender

Among the 197 respondents, there were 129 (65%) female teachers and 68 (35%) male teachers.

Teaching experience

Among the 197 teachers, 128 (65%) had at least 10 years of teaching experience, 43 (22%) had four to nine years of experience, and 25 (13%) had three or fewer years of experience, as represented in Table 1. One teacher did not indicate years of experience.

Table 1: Teachers' teaching experience and positions

Teaching experience		
	Frequency	**Percentage**
3 years or fewer	25	13%
4-9 years	43	22%
10-19 years	51	26%
20-29 years	67	34%
30-39 years	10	5%
No response	1	<1%
Position held at the school		
	Frequency	**Percentage**
Head of Department	30	15%
Deputy Principal	3	2%
Principal	9	5%
No additional position	146	74%
No response	9	5%

Administrative positions

Table 1 also shows the instances where the surveyed teachers held additional positions in their schools, i.e., in addition to their teaching positions. Thirty (15%) were heads of departments (based on the subjects in which they had specialised), three (2%) were deputy principals, and nine (5%) were principals.

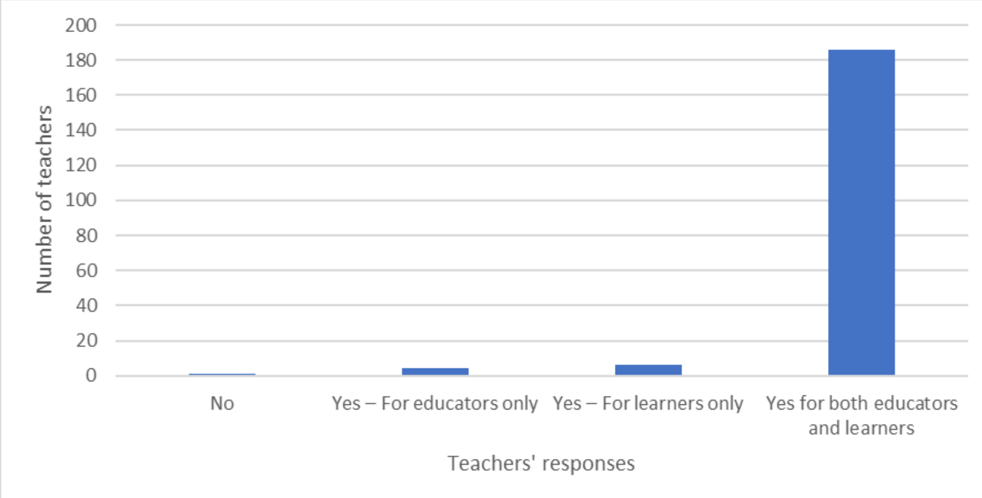
Teachers' access to computers (laptop or PC) at school

It was found that 51 (26%) of the teachers had access to computers for administrative duties at their schools (this included using school secretaries' computers to record academic results and print examinations), 19 (10%) had access to a computer in their school's computer laboratory, and 29 (15%) had access to a computer in their office (where they could use the computer to prepare content for teaching and learning). A total of 97 (49%) of teachers did not have access to computers at their schools. One teacher did not respond to the question.

Teachers' access to tablets at school

Figure 1 presents information on teachers' access at tablets at the surveyed schools, with 186 (94%) of teachers indicating that their school had tablets for both teachers (educators) and learners. Six (3.05%) of the teachers stated that tablets were available for learners only, four (2%) of teachers said that tablets were available for teachers only, and one teacher said there were no tablets at the school. The one teacher who stated that there were no tablets at the school was at a school where the rest of the teachers from the same school stated that there were indeed tablets available and that they were used by teachers and learners alike. This indicated a lack of awareness on the part of the teacher in terms of available resources, and possibly some indifference towards the use of ICTs.

Figure 1: Teachers' access to tablets at their schools



Teachers' ICT ownership and use at home

In respect of personal ownership and use of technology at home, as displayed in Table 2, 133 (67%) of the 197 surveyed teachers said they owned one or more of a smartphone, feature phone (non-smart cellphone) and/or tablet; 121 (61.5%) confirmed that they owned a computer or laptop; 67 (34%) printers in their homes, and 55 (28%) had access to the internet from home.

Table 2: Teachers' ICT ownership and use at home

ICT tool	No. of teachers who owned and used the tool at home	Percentage
Smartphone, feature phone, and/or tablet	133	68%
Computer (PC or laptop)	121	61%
Printer	67	34%
Internet	55	28%

School bans on use of personal digital devices

Of the 197 teachers surveyed, 163 (83%) indicated that their schools had banned learner use of personal digital devices, with the exception of calculators, on school premises. Meanwhile, 17 (9%) of the teachers stated that their schools allowed learners to use personal digital devices on school premises. The remaining 17 (9%) teachers did not respond to the question.

Teacher technology readiness

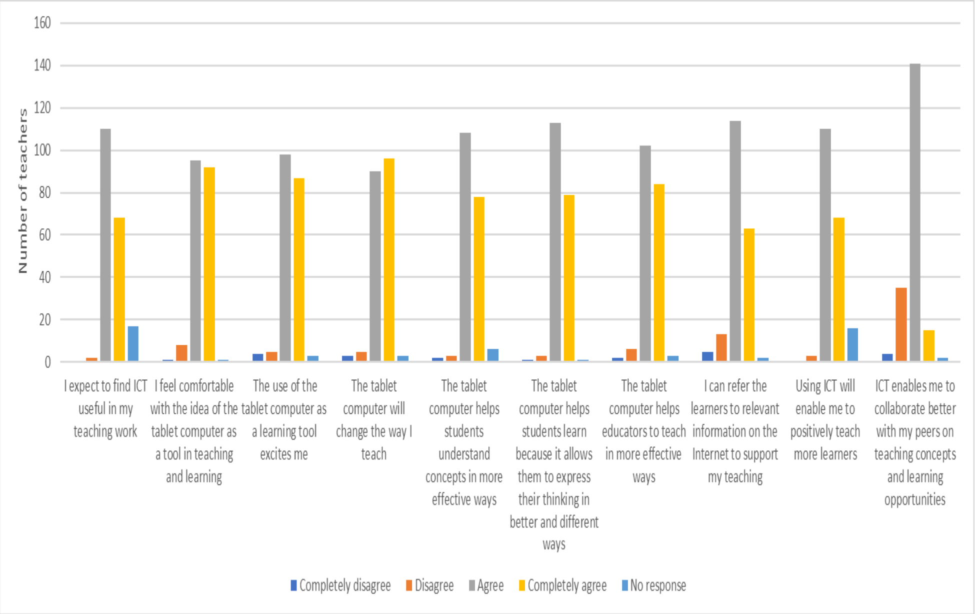
The findings in this sub-section are organised according to the four aforementioned technology readiness index (TRI) dimensions:

- optimism;
- innovativeness;
- discomfort; and
- insecurity.

Teachers' optimism about the use of ICTs

Figure 2 illustrates the findings from the survey questions probing teachers' degree of optimism about using ICTs.

Figure 2: Teachers' optimism about the use of ICTs



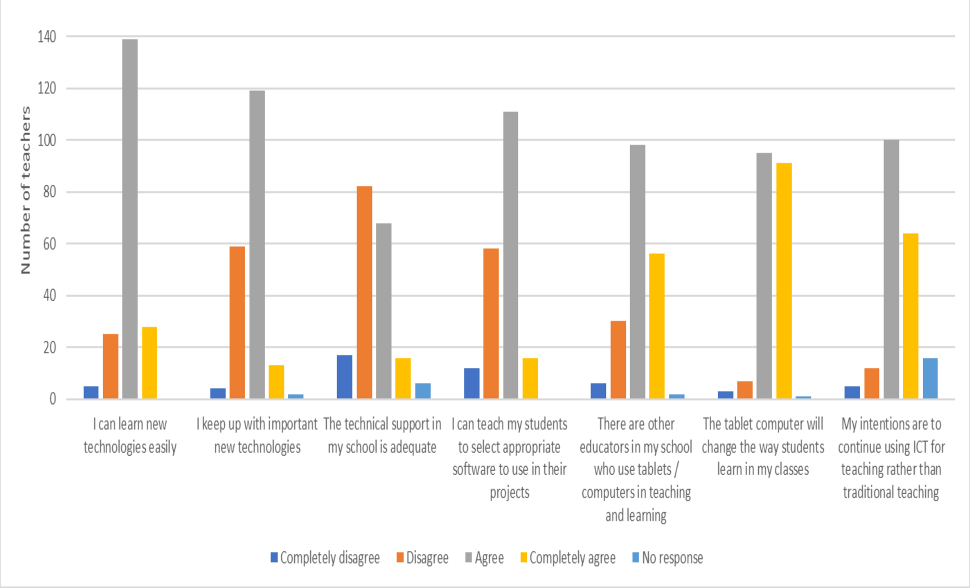
Ninety per cent of the surveyed teachers agreed (via an "agree" or "completely agree" response) with the statement that they expected to find ICTs useful in teaching their subjects, as presented in Figure 3. Ninety-five per cent of the teachers agreed that they were comfortable with the idea of a tablet as a tool for teaching and learning, and 94% agreed that the use of tablets was exciting. With reference to their perception of using tablets for teaching, 94% agreed that tablets would change the way they teach. The same percentage agreed that tablets would assist learners in understanding concepts effectively. Furthermore, 97% of teachers agreed that the use of tablets would allow learners the freedom to express their views, 90% agreed or strongly agreed that ICTs would encourage positive learning experiences for learners, and 90% agreed or strongly agreed that they could refer learners to relevant content on the internet to support content covered in the classroom.

In reflecting on their own abilities, 94% of the teachers agreed that tablets could assist them in approaching teaching effectively, and 79% agreed that their colleagues could assist them in collaborating on teaching and learning opportunities.

Teachers' innovativeness in the use of ICTs

Figure 3 illustrates the findings from the survey questions probing teachers' degree of innovativeness in using ICTs.

Figure 3: Teachers' innovativeness in the use of ICTs

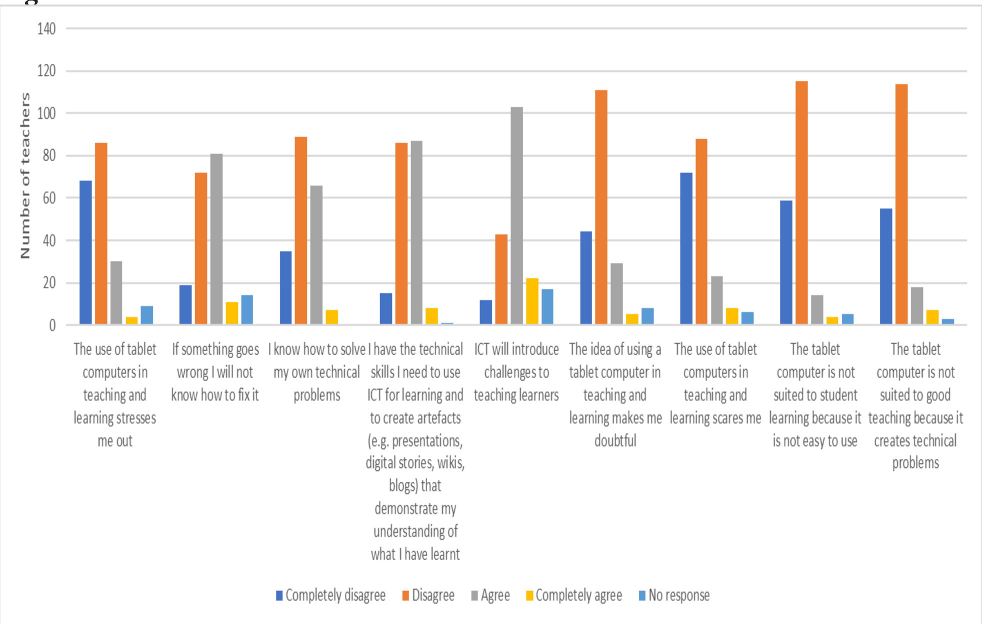


Eighty-five per cent of the teachers agreed (via an "agree" or "strongly agree" response) with the statement that they had the ability to easily learn new technologies, and 67% agreed that they were keeping up with new technologies. Forty-three per cent of the teachers agreed that technical support at their school was adequate, 64% agreed that they could teach learners to select appropriate software to use for their projects, and 78% agreed that teaching colleagues at their school used tablets or computers in the classroom for teaching. When teachers were probed about the impact of tablet computers in the classroom, 94% of the teachers agreed that it "will change the way students learn in my classes", and 83% of the teachers agreed that they intended "to continue using ICT for teaching rather than traditional teaching".

Teachers' discomfort with the use of ICTs

Figure 4 represents the findings from the survey questions probing teachers' levels of discomfort with using ICTs. Because discomfort is an inhibitor, the description of findings is focused on *disagreement* with the potential discomforts posed to them, i.e., the percentages we report are the number of teachers who responded with "disagree" or "completely disagree" to each statement they were asked to respond to.

Figure 4: Teachers' discomfort with the use of ICTs



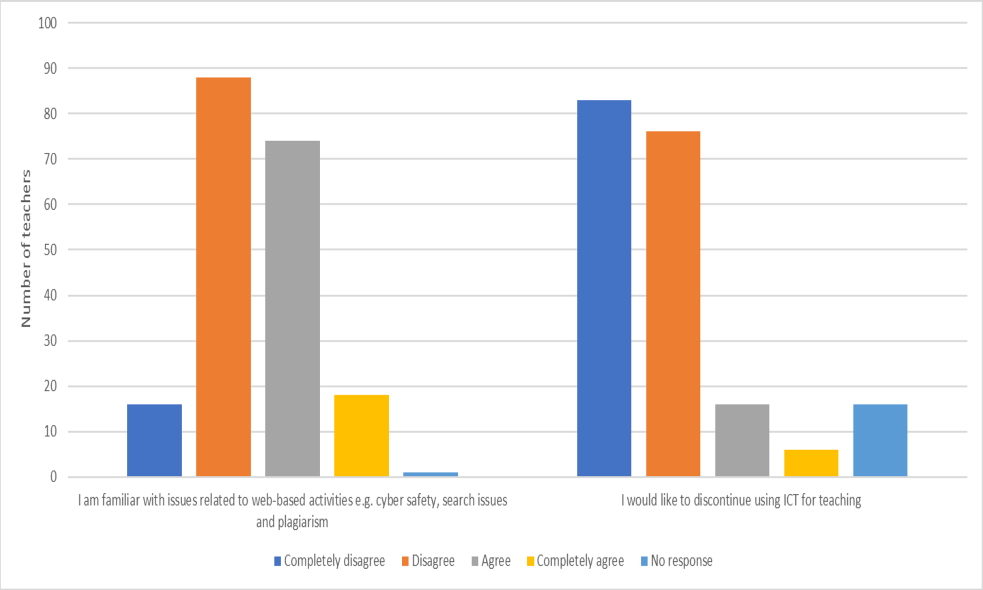
In some areas, the teacher responses suggested very little discomfort. Eighty-eight per cent of the teachers disagreed (via a "disagree" or "completely disagree" response) with the statement that "[t]he tablet computer is not suited to student learning because it is not easy to use", 86% disagreed with the statement that "[t]he tablet computer is not suited to good teaching because it creates technical problems", 81% disagreed with the statement that "use of tablet computers in teaching and learning scares me", 79% disagreed with the statement that "[t]he idea of using a tablet computer in teaching and learning makes me doubtful", and 78% of the teachers disagreed with the statement that using tablets for teaching and learning "stresses me out". All these responses suggest high levels of comfort with ICT.

There were, however, indications of some substantial feelings of discomfort in other areas. Only 28% of teacher disagreed that "ICTs will introduce challenges to teaching learners", and fewer than half (46%) of the teachers disagreed with the statement that "[i]f something goes wrong, I will not know how to fix it".

There were clear indications of discomfort in terms of some of the teachers' personal technical skills. A large number (63%) of the teachers disagreed with the statement that "I know how to solve my own technical problems", and more than half (51%) disagreed with the statement that "I have the necessary technical skills to use ICTs for learning and create artefacts (e.g., presentations, digital stories, wikis, blogs) that demonstrate my understanding of what I have learnt".

Teachers' feelings of insecurity regarding the use of ICTs
Figure 5 represents the findings from the survey questions probing teachers' feelings of insecurity regarding the use of ICTs. Insecurity is an inhibitor and thus the results are, as with "discomfort" above, discussed in terms of a combination of "disagree" and "completely disagree" responses.

Figure 5: Teachers' feelings of insecurity regarding the use of ICTs



Fifty-three per cent of the teachers disagreed (via a "disagree" or "completely disagree" response) that they were "familiar with issues related to web-based activities, e.g., cyber safety, search issues and plagiarism". However, at the same time, only 11% of the teachers disagreed with the statement that "I would like to discontinue using ICT for teaching".

6. Analysis and conclusions

Teachers' technology readiness

Optimism
Most of the teachers were clearly optimistic about the use of ICT as tools for teaching and learning. There was a clear belief that tablets would change the approach to classroom interactions and awaken inactive learners. Teachers had a sense of control of the ICTs, which led them to believe that they could assist learners. Furthermore, the teachers had the perception that ICTs offered an efficient approach to teaching and learning, and they were optimistic about receiving the necessary technical support from their colleagues and the wider community. These findings resonate with those of Haßler, Major and Hennessy (2016) and Mouza and Barrett-Greenly (2015), who

argue that teachers' optimism is produced by both the benefits associated with using ICTs for teaching and the digital skills they gain in the process.

Innovativeness

It was found that the majority of the teachers had confidence in their ability to be innovative in their adoption of ICTs. They believed in the technical support offered, believed they could guide learners in using software for projects, and had colleagues who were innovative and with whom they could collaborate in the quest to transform classroom interactions for learners. Kopcha (2012) provides similar findings, explaining how technical and administrative support coupled with colleagues' assistance influences teachers' innovative approaches to using ICTs for teaching and learning. Rogers (1983, 2003) refers to teachers who are the first to use technologies in society as innovators, and they not only form the support structure for early adopters but are also quick to test any technology.

Discomfort

The results were mixed on the matter of discomfort. There were low levels of teacher discomfort regarding the suitability of tablets for teaching and learning, and ease of use for students, and low levels of general fear, doubt and stress among the teachers about using ICTs for teaching and learning. But, at the same time, there were high levels of discomfort expressed regarding the "challenges to teaching learners", fixing technical problems, and having the necessary personal ICT skills.

Insecurity

Slightly more than 50% of the teachers surveyed indicated concern over their lack of familiarity with matters of cyber safety, search issues, and plagiarism, but only for a very small number of teachers did this concern translate into a desire to stop using ICTs for teaching.

Overall, it would appear that the teachers' strong feelings of optimism and innovativeness in respect of ICT adoption were the technology readiness factors allowing them to overcome most of their feelings of discomfort and insecurity.

Implications for South Africa Connect

The generally positive teacher technology readiness findings discussed above would seem to augur well for the objectives of the South Africa Connect national broadband policy. But there are clearly some teacher training and empowerment requirements that must be addressed if the teaching and learning objectives of South Africa Connect policy are to be met in South African rural schools. More than half (and in several cases substantially more than three-quarters) of the teachers surveyed indicated that they felt discomfort in respect of:

- the challenges inherent in the teaching of learners via ICTs;
- their ability to fix the technical problems that will inevitably arise; and

- having the necessary personal ICT skills "to use ICTs for learning and create artefacts (e.g., presentations, digital stories, wikis, blogs)".

All three elements need to be addressed via teacher training if South African rural schools are to succeed in ways envisioned by South Africa Connect. The identification of these three elements is a practical contribution that this research offers to understanding how to optimise the adoption of ICTs in South African rural schools.

Also, the prohibitions we found at many schools against student use of personal digital devices (with the exception of calculators) on school premises suggest a potential disconnect between bottom-up sentiment at the level of rural schools and the top-down South Africa Connect drive for increased ICT use. Section 36(4)(b) of the South Africa Schools Act of 1996 gives each School Governing Body (SGB) a mandate to determine restrictions on activities that may be harmful to learners on school premises (RSA, 1996). Thus, the interpretation of what is harmful to learners rests with SGBs—and the SGBs have created the aforementioned policies about student use of personal digital devices. Also of note is our finding, cited above, that the majority (83%) of the teachers surveyed said that their schools prohibited use of personal digital devices on school premises, thereby potentially limiting the learners' ability to acquire digital education. This is while the teachers themselves acknowledge the usefulness of ICTs in teaching. The core concern on the part of the SGBs and the teachers seems to be how to avoid student use of personal digital devices, on school premises, for non-educational purposes.

South Africa Connect's stated critical success factors include "implementation of measures that will enable uptake and usage. Examples include the availability of electronic educational content, the use of tablets and mobile devices in schools […]" (DoC, 2013, p. 40). Schools' bans on learner use of personal digital devices on school premises potentially run counter to this South Africa Connect objective.

We recommend that personal digital device use for instructional and learning purposes be permitted in South African classrooms, in line with the objectives of South Africa Connect. At the same time, we realise that schools do experience practical issues in controlling non-educational use of personal devices by learners inside and outside the classroom. Accordingly, we are of the view that the schools in question should rescind or amend their policies prohibiting student use of personal digital devices at school—or, failing that, that the government should revise the relevant section of the Schools Act in such a way as to take the power to dictate classroom ICT use away from SGBs, thus expediting the operationalisation of South Africa Connect and the broader National Development Plan, while at the same time ensuring that the use of personal digital devices at schools is limited to usage for educational purposes.

References

Adukaite, A., Van Zyl, I., Er, Ş., & Cantoni, L. (2017). Teacher perceptions on the use of digital gamified learning in tourism education: The case of South African secondary schools. *Computers and Education*, *111*(August), 172–190. https://doi.org/10.1016/j.compedu.2017.04.008

Alsabawy, A., Cater-Steel, A., & Soar, J. (2011). Measuring e-learning system success (Research in progress). In *PACIS 2011 Proceedings* (Paper 15). Brisbane.

Ampofo, S. Y., Bizimana, B., Mbuthi, J., Ndayambaje, I., Ogeta, N., & Orodho, J. A. (2014). Information communication technology penetration and its impact on education: Lessons of experience from selected African countries of Ghana, Kenya and Rwanda. *Journal of Information Engineering and Applications*, *4*(11), 84–95.

Avgerou, C. (2008). Information systems in developing countries: A critical research review. *Journal of Information Technology*, *23*(3), 133–146. https://doi.org/10.1057/palgrave.jit.2000136

Barakabitze, A. A., Lazaro, A.W., Ainea, N., Mkwizu, M. H., Maziku, H., Matofali, A. X., Iddi, A., & Sanga, C. (2019). Transforming African education systems in Science, Technology, Engineering, and Mathematics (STEM) using ICTs: Challenges and opportunities. *Education Research International*, *2019*, 1–29. https://doi.org/10.1155/2019/6946809

Botha, A., Herselman, M., Rametse, S., & Maremi, K. (2017). Barriers in rural technology integration: A case study from the trenches. In P. Cunningham, & M. Cunningham (Eds.), *IST-Africa 2017 Conference Proceedings* (pp. 1–10). https://doi.org/10.23919/ISTAFRICA.2017.8102349

Chen, X. (2013). Tablets for informal language learning: Student usage and attitudes. *Language Learning & Technology*, *17*(1), 20–36.

Department of Basic Education. (2017). Rural Education Draft Policy. Retrieved from http://pmg-assets.s3-website-eu-west-1.amazonaws.com/180126draftruraledupolicy.pdf

Department of Communications (DoC). (2013). South Africa Connect: Creating Opportunities, Ensuring Inclusion: South Africa's Broadband Policy. Retrieved from https://www.gov.za/documents/electronic-communications-act-south-africa-connect-creating-opportunity-ensuring-inclusion

Department of Telecommunications and Postal Services (DTPS). (2016). National Integrated ICT Policy White Paper. Retrieved from https://www.gov.za/documents/electronic-communications-act-national-integrated-ict-policy-white-paper-3-oct-2016-0000

DTPS. (2019). Policy on High Demand Spectrum and Policy Direction on the Licensing of a Wireless Open Access Network.

Eberhard, B., Podio, M., Alonso, A. P., Radovica, E., Avotina, L., Peiseniece, L., Sendon, M.C., Lozano, A.G., & Solé-Pla, J. (2017). Smart work: The transformation of the labour market due to the fourth industrial revolution (I4.0). *International Journal of Business and Economic Sciences Applied Research*, *10*(3), 47–66.

Falloon, G. (2013). Young students using iPads: App design and content influences on their learning pathways. *Computers & Education*, *68*(October), 505–521. https://doi.org/10.1016/j.compedu.2013.06.006

Fardon, R., & Furniss, G. (Eds.) (1994). *African languages, development and the state*. London: Routledge.

Frohberg, D., Göth, C., & Schwabe, G. (2009). Mobile learning projects: A critical analysis of the state of the art. *Journal of Computer Assisted Learning*, *25*(4), 307–331. https://doi.org/10.1111/j.1365-2729.2009.00315.x

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363

Gibson, D., Broadley, T., Downie, J., & Wallet, P. (2018). Evolving learning paradigms: Re-setting baselines and collection methods of information and communication technology in education statistics. *Journal of Educational Technology & Society*, *21*(2), 62–73.

Haßler, B., Major, L., & Hennessy, S. (2016). Tablet use in schools: A critical review of the evidence for learning outcomes. *Journal of Computer Assisted Learning*, *32*(2), 139–156. https://doi.org/10.1111/jcal.12123

Hankel, L., Burgess, M., Roux, K., Van Deventer, A., Ford, M., Smith, R., & Govender, S. (2017). Study on the accuracy of school location information in South Africa. *South African Journal of Geomatics*, *6*(2), 142–154. https://doi.org/10.4314/sajg.v6i2.1

Hargittai, E. (2010). Digital na(t)ives? Variation in internet skills and uses among members of the 'net generation'. *Sociological Inquiry*, *80*(1), 92–113. https://doi.org/10.1111/j.1475-682X.2009.00317.x

Hennessy, S., Harrison, D. J., & Wamakote, L. (2010). Teacher factors influencing classroom use of ICT in Sub-Saharan Africa. *Itupale Online Journal of African Studies*, *2*(2010), 39–54.

Herselman, M., & Botha, A. (2014). *Designing and implementing an information communication technology for rural education development (ICT4RED) initiative in a resource constrained environment: Nciba school district, Eastern Cape, South Africa*. Pretoria: CSIR Meraka.

Ifenthaler, D., & Schweinbenz, V. (2013). The acceptance of tablet-PCs in classroom instruction: The teachers' perspectives. *Computers in Human Behavior*, *29*(3), 525–534. https://doi.org/10.1016/j.chb.2012.11.004

Kafyulilo, A. (2014). Access, use and perceptions of teachers and students towards mobile phones as a tool for teaching and learning in Tanzania. *Education and Information Technologies*, *19*(1), 115–127. https://doi.org/10.1007/s10639-012-9207-y

Kaliisa, R., & Picard, M. (2017). A systematic review on mobile learning in higher education: The African perspective. *Turkish Online Journal of Educational Technology*, *16*(1), 1–18.

Kalinga, A. E., Bagile, R. B. B., & Trojer, L. (2006). An interactive e-learning management system (e-LMS): A solution to Tanzanian secondary schools' education. *International Journal of Human and Social Sciences*, *1*(4), 250–253.

Kopcha, T. J. (2012). Teachers' perceptions of the barriers to technology integration and practices with technology under situated professional development. *Computers & Education*, *59*(4), 1109–1121. https://doi.org/10.1016/j.compedu.2012.05.014

Lai, M. (2008). Technology readiness, internet self-efficacy and computing experience of professional accounting students. *Campus-Wide Information Systems*, *25*(1), 18–29. https://doi.org/10.1108/10650740810849061

Lee, A. S. (1989). A scientific methodology for MIS case studies. *MIS Quarterly*, *13*(1), 33–50. https://doi.org/10.2307/248698

Liebenberg, J., Benade, T., & Ellis, S. (2018). Acceptance of ICT: Applicability of the unified theory of acceptance and use of technology (UTAUT) to South African students. *The African Journal of Information Systems*, *10*(3), 160–173.

Marais, M., & Van Biljon, J. (2017). Social mapping for supporting sensemaking and collaboration: The case of development informatics research in South Africa. In P. Cunningham, & M. Cunningham (Eds.), *IST-Africa 2017 Conference Proceedings* (pp. 1–10). https://doi.org/10.23919/ISTAFRICA.2017.8102336

Mestry, R., & Ndhlovu, R. (2014). The implications of the National Norms and Standards for School Funding policy on equity in South African public schools. *South African Journal of Education*, *34*(3), 1–11. https://doi.org/10.15700/201409161042

Mouza, C., & Barrett-Greenly, T. (2015). Bridging the app gap: An examination of a professional development initiative on mobile learning in urban schools. *Computers and Education*, *88*, 1–14. https://doi.org/10.1016/j.compedu.2015.04.009

Mwapwele, S., Marais, M., Dlamini, S., & Van Biljon, J. V. (2019). ICT support environment in developing countries: The multiple cases of school teachers in rural South Africa. In P. Cunningham, & M. Cunningham (Eds.), *IST-Africa 2019 Conference Proceedings* (pp. 1–12). https://doi.org/10.23919/ISTAFRICA.2019.8764859

Ngwenyama, O., Andoh-Baidoo, F. K., Bollou, F., & Morawczynski, O. (2006). Is there a relationship between ICT, health, education and development? An empirical analysis of five West African countries from 1997–2003. *The Electronic Journal of Information Systems in Developing Countries*, *23*(5), 1–11. https://doi.org/10.1002/j.1681-4835.2006.tb00150.x

National Planning Commission (NPC). (2012). National Development Plan 2030: Our Future – Make It Work. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf

Omoniyi, T., & Quadri, A. T. (2013). Perceived competence of Nigerian secondary schools teachers in the use of information and communication technology (ICT). *Journal of Education and Practice*, *4*(10), 157–164.

Osakwe, J., Dlodlo, N., & Jere, N. (2017). Where learners' and teachers' perceptions on mobile learning meet: A case of Namibian secondary schools in the Khomas region. *Technology in Society*, *49*(May), 16–30. https://doi.org/10.1016/j.techsoc.2016.12.004

Parasuraman, A., & Colby, C. L. (2015). An updated and streamlined technology readiness index: TRI 2.0. *Journal of Service Research*, *18*(1), 59–74. https://doi.org/10.1177/1094670514539730

Partin, C. M., & Lauderdale, S. (2013). Bringing it all together: Interdisciplinary perspectives on incorporating mobile technologies in higher education. In L. Wankel & P. Blessinger (Eds.), *Increasing student engagement and retention using mobile applications: Smartphones, Skype and texting technologies* (pp. 83–114). Bingley, UK: Emerald. https://doi.org/10.1108/S2044-9968(2013)000006D006

Porter, G., Hampshire, K., Milner, J., Munthali, A., Robson, E., De Lannoy, A., … Abane, A. (2016). Mobile phones and education in Sub-Saharan Africa: From youth practice to public policy. *Journal of International Development*, *28*(1), 22–39. https://doi.org/10.1002/jid.3116

Rambe, P., & Ng'ambi, D. (2014). Learning with and from Facebook: Uncovering power asymmetries in educational interactions. *Australasian Journal of Educational Technology*, *30*(3), 312–325. https://doi.org/10.14742/ajet.116

Rena, R. (2006). Higher education in Africa – A case of Eritrea. *Journal of Educational Planning and Administration*, *21*(2), 125–140.

Rena, R. (2008). The Internet in tertiary education in Africa: Recent trends. *International Journal of Computing and ICT Research*, *2*(1), 9–16.

Republic of South Africa (RSA). (1996). South African Schools Act, No. 84 of 1996.

Roberts, N., & Vänskä, R. (2011). Challenging assumptions: Mobile Learning for Mathematics Project in South Africa. *Distance Education*, *32*(2), 243–259. https://doi.org/10.1080/01587919.2011.584850

Rogers, E. M. (1983). *Diffusion of innovation* (3rd ed.). London: Collier Macmillan.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

Summak, M. S., Baglibel, M., & Samancioglu, M. (2010). Technology readiness of primary school teachers: A case study in Turkey. *Procedia – Social and Behavioral Sciences*, *2*(2), 2671–2675. https://doi.org/10.1016/j.sbspro.2010.03.393

Waller, P. P., & Maxwell, K. L. H. (2017). Mathematics teachers' perceptions of resources and curriculum availability in post-apartheid schooling. *International Journal of Science and Mathematics Education*, *15*(4), 741–757. https://doi.org/10.1007/s10763-016-9713-2

Yidana, I., & Maazurre, C. (2012). Integrating ICT into teacher education curriculum: Faculty perceptions of their technology professional development needs in two Ghanaian universities. *Journal of Continuing, Open and Distance Education*, *2*(1), 175–199.

Realities of Microenterprises' ICT Use for Business Activities and for Acquiring Online Government Support: A Study in Western Cape Province, South Africa

Muhammad Ameer Osman
MCom Graduate, Information Systems, Faculty of Commerce, University of Cape Town
https://orcid.org/0000-0002-0381-6991

Donald Flywell Malanga
PhD Candidate, Information Systems, Faculty of Commerce, University of Cape Town
https://orcid.org/0000-0001-9681-6503

Wallace Chigona
Professor of Information Systems, Faculty of Commerce, University of Cape Town
https://orcid.org/0000-0002-1059-811X

Abstract

This article provides findings from a study, in South Africa's Western Cape Province, of microenterprises' experiences and perceptions of use of information and communication technologies (ICTs) for general business activities and for acquiring online government business support information. Using the capability approach (CA) theoretical framework, the study analysed data from interviews with microenterprise owners and digital government experts. The study found that the microenterprises were adept in their use of ICTs in their businesses, but that they encountered problems in using online government business support information services. These problems were found to be the result of deficiencies in the online services' content, structure, design, navigation, mobile-friendliness, language usage and bureaucratic requirements.

Keywords

microenterprises, digital government, e-government, government business support information, government websites, information and communication technologies (ICTs), capability approach (CA), Western Cape, South Africa

Acknowledgements

This article draws on the lead author Osman's research conducted during completion of the degree of Master of Commerce in Information Systems at the University of Cape Town, and on a conference paper presented at Digital Skills 2019: Digital Innovation and Transformation Conference, 29 August 2019, Boksburg, South Africa.

DOI: https://doi.org/10.23962/10539/28659

Recommended citation
Osman, M. A., Malanga, D. F., & Chigona, W. (2019). Realities of microenterprises' ICT use for business activities and for acquiring online government support: A study in Western Cape Province, South Africa. *The African Journal of Information and Communication (AJIC)*, 24, 1-23. https://doi.org/10.23962/10539/28659

1. Introduction

Microenterprises play a significant role in the socio-economic development of numerous developing countries, including South Africa (Makoza & Chigona, 2014). They provide income generation, sources of employment, and improved social conditions for disadvantaged or "underserved" communities (Chacko & Harris, 2006; Duncombe & Heeks, 2005). In this study, microenterprises are defined as businesses with fewer than 10 employees that support the livelihood of households in developing nations for economic development (Makoza & Chigona, 2012). The majority of microenterprises fail to survive or to grow due to myriad challenges, including lack of access to information, difficulty securing capital, limited business skills, difficulty identifying markets, and difficulty understanding the regulatory requirements for a business (DTI, n.d.). As a result, most microenterprises do not survive beyond their first two years (Makoza & Chigona, 2014).

Prior studies have shown that the use of information and communication technologies (ICTs), such as mobile phones, social media platforms and government websites, can offer solutions to some of the challenges facing microenterprises. ICTs can provide improved access to information, reduced administrative costs, improved productivity and profitability, operational efficacies, and improved market share (Kamal & Qureshi, 2009). The use of digital government (also often referred to as "electronic government" or "e-government") websites providing government-to-business (G2B) services can reduce the time and costs that businesses expend in accessing the information needed for setting up a new business (i.e., through reduced bureaucratic barriers), can improve conformity to government rules and regulations for operating a business (e.g., licensing and tax filing), and can facilitate microenterprises' provision of paid services to government through e-procurement, e-business and e-commerce portals (Makoza, 2011).

Studies suggest that, in developing countries, microenterprises struggle to access online digital government support services because, inter alia, they lack sufficient access to ICTs (Kamal & Qureshi, 2009; Makoza, 2011). This can be exacerbated by a lack of ICT skills and/or low literacy levels of microenterprise entrepreneurs, insufficient resources to procure and maintain ICTs, and the poor quality of some government websites, including poorly organised information (PMG, 2012; Venter & Lotriet, 2005). Other developing-country research has probed factors influencing the adoption and implementation of digital government (Bwalya, Du Plessis & Rensleigh, 2013; Bwalya & Healy, 2010; Grönlund, 2011). However, microenterprises' use of online government support information has not been widely explored.

Likewise, in South Africa, microenterprises' use of ICTs for business activities and for online government business support information has received marginal attention. Studies on the impact of ICT use in South Africa have largely focused on small and medium enterprises (SMEs), with a focus on areas such as productivity and formalisation (Makoza, 2011). The G2B category has also not received attention in the South African literature on digital government. The predominant focus has been on citizens, i.e., government-to-citizen (G2C) modalities (Zaidi & Qteishat, 2012). Therefore, the main objectives of the study described in this article were to explore microenterprises' experiences and perceptions of:

- using ICTs for general business activities; and
- using online government business support information.

The study consisted of interviews with 17 Western Cape microenterprise owners and interviews with two digital government experts. We analysed the data in terms of the capability approach (CA) theoretical framework as developed by Sen and Nussbaum (Nussbaum, 2009; Robeyns, 2003; Sen, 1993).

The hope is that generating greater understanding of how microenterprises experience and perceive ICTs and online government support information services can help government departments to provide tailored digital government services that will benefit microenterprises in South Africa. Eventually, this could have a positive impact on the growth of the country's microenterprise sector, and of the sustainability of individual enterprises. The study was underpinned by the capability approach (CA) theoretical framework (Nussbaum, 2009; Sen, 1993), as recently operationalised in an African context by Nyemba-Mudenda (2014).

2. Study context

South Africa's Western Cape Province is home to more than 6.2 million people (Stats SA, n.d.). About half of the province's inhabitants reside in the metropolitan area of Cape Town, which is the provincial capital (City of Cape Town, n.d.). The predominant language spoken in the province is Afrikaans, with English and isiXhosa being the other two leading languages (Western Cape Government, n.d.).

Research in the Delft South and Thabong townships of the Western Cape found that 15% of all identified microenterprises were operated by individuals who are under the age of 30 years (Charman, 2016). According to the national Department of Small Business Development (2019), South African microenterprises can be found engaged in, inter alia, agriculture, mining, manufacturing, construction, retail, automotive repair, catering, accommodation, transport, storage, communications, business services and community services. The Western Cape Government offers support information and services to encourage the development of microenterprises (Makoza, 2011). These services seek to, inter alia, improve the formation of small businesses in underprivileged communities, to build entrepreneurial skills, to decrease unemployment, and to encourage the evolution of microenterprises into SMEs (Makoza, 2011).

In the relevant developing-world research, it has been found that, despite myriad forms of online government business support information services, the use of such business support information has not been optimal, especially by microenterprises (Shambour, 2012). The low use of online government support information services has, in some cases, been attributed to microenterprises not being sufficiently aware of the support being offered and implemented by government departments and development agencies (Mitrovic & Bytheway, 2009). Another challenge that has been identified is that government support information for small business is not available and/or accessible in rural areas (Makoza, 2011). Evidence has also been found of skepticism among potential information recipients because of the apparent absence of cohesion among the government stakeholders involved in providing support information for small business (Mitrovic & Bytheway, 2009). Low literacy levels (e.g., personal computer (PC) literacy) have also been found to play a role in limiting microenterprises' use of the support information (Mawela, Ochara & Twinomurinzi, 2016).

Another element that could limit the use of online government support information by developing-world microenterprises is their informality. Most developing-world microenterprises do not maintain business records and are typically unregistered (Esselaar, Stork, Ndawalana & Deen-Swarray, 2007). Meanwhile, government support will often be contingent on the microenterprises being registered. Rogerson (2008) explains that for microenterprises operating in the informal sector, formalisation in certain instances can limit the business activities that these enterprises can engage in.

Another possible reason for low microenterprise use of online government support information is that the information tends to be siloed and segmented across various levels of government (e.g., in the South African context, the national, provincial and local levels) and across various government departments (Western Cape Government, n.d.).

The Western Cape Province has, in South African terms, a high internet connectivity rate. A 2018 estimate stated that 95.6% of individuals in the province accessed the internet using a mobile phone, compared to the national average of 70.8% (RIA & UCT, 2018). The Western Cape Government also offers ICT access initiatives, such as telecentres, which have been established to provide people in underserved areas with access to ICTs and ICT-related services (Kaisara & Pather, 2011).

3. Literature review

Microenterprises in developing countries

Microenterprises provide, inter alia, sources of income, opportunities for employment, opportunities for skills development, and opportunities for self-empowerment (Makoza, 2011). In South Africa, micro, small and medium-sized enterprises (MSMEs) employ an estimated 50-60% of the country's workforce and contribute around 34% of gross domestic product (GDP) (IFC & World Bank, 2018). In South Africa and other developing countries, microenterprises are usually characterised as being survivalists, because they generate only small revenues, due to the small scale of their business operations (Abor & Quartey, 2010). Furthermore, as stated above, developing-world microenterprises usually do not maintain business records and are often unregistered (Esselaar et al., 2007), as they mostly operate in the informal sector.

Microenterprises and ICTs

Duncombe and Heeks (2005) describe ICTs as technologies for capturing, processing, storing and disseminating information. Microenterprises typically use ICTs such as PCs, laptops, mobile phones and printers (Duncombe & Heeks, 2005). Microenterprises can benefit from using ICTs in the form of improved access to information, reduced administrative costs, improved productivity and profitability, operational efficacies, and improved market share (Kamal & Qureshi, 2009). For example, by using social networking and a website, updated via a mobile smartphone, microenterprises can reach large numbers of customers at a very low cost, effectively growing and harnessing their social capital (Good & Qureshi, 2009). Previous research has found that the majority of Cape Town's microenterprises use mobile telephony for the key informational elements of their engagements in trade and commerce (Noruwana, Chigona & Malanga, 2018).

Microenterprises and online government support information services

Digital government is the use of ICTs to improve access to, and delivery of, government information services to citizens (G2C), businesses (G2B) and other government agencies (G2G) (Agangiba & Kabanda, 2016). Examples of digital government information services include information on business licensing, tax filing, grant submissions, and tendering for government contracts (Good & Qureshi, 2009; Mutula, 2013).

Microenterprises can access business support information services through government websites (Agangiba & Kabanda, 2016), which can potentially provide quick and flexible access to necessary information and service delivery options

(Noruwana et al., 2018; Malik, Shuqin, Mastoi, Gul & Gul, 2016). However, for digital government websites to be fully accessible and useful, their web-based applications should be easy to interact with, irrespective of the device being used (e.g., mobile device, laptop, PC) (Rubaii-Barrett & Wise, 2008).

4. Theoretical framework: The capability approach (CA)

This study adopted the capability approach (CA) framework developed by Sen and Nussbaum (Nussbaum, 2009; Robeyns, 2003; Sen, 1993), and as recently operationalised in an African context by Nyemba-Mudenda (2014). CA emphasises not amounts or levels of income, but rather capabilities such as "access to healthcare, education, information, participating in economic life and the autonomy in decision making" (Zheng & Walsham, 2008, p. 224). CA has achieved recognition as a multi-disciplinary analytical instrument and has been used in numerous ICT for development (ICT4D) studies (see, for example, Alexander & Phahlamohlaka, 2006; Grunfeld, Hak & Pin, 2011).

The core concepts in CA are commodity, capabilities/potential functionings, conversion factors, functionings, freedom, agency and well-being. Table 1, from Nyemba-Mudenda (2014, p. 56), summarises the core CA concepts.

Table 1: Capability approach (CA) core concepts

Concept	Description	Examples
Commodity	Resources—their characteristics, access, and use to generate capabilities for a person	Services, products, goods
Capabilities/ Potential functionings	The alternative combinations of actions/activities that are feasible for a person to achieve—things that a person is effectively able to do and to live a life they value	To be health[y]
Conversion factors	Individual capacities or personal characteristics and social structures that affect the transformation of capabilities into achieved outcomes	Intellect, socio-cultural factors
Functionings	What a person chooses to be or to do from their capability set to live a life they value (achieved outcomes)	Being literate
Freedom	Choice in terms of people's preferences and perceived value of goods (the freedom to lead different types of life is reflected in the person's capability set)	Choice, preferences
Agency	A person's ability to pursue and realise goals that he/she values and has a reason to value	
Well-being	The state of being health, happy or prosperous; welfare	

Source: Nyemba-Mudenda (2014, p. 56)

Commodities

In CA, *commodities* are goods and services that are of specific importance to individuals and =they do not have to be income- or money-related (Robeyns, 2006). The use of commodities contributes to social situations and to personal characteristics, which successively feed back to conversion factors and decision-making instruments (Robeyns, 2006). The commodities in this study were:

- ICTs for general business activities; and
- online government business support information.

CA analysis goes beyond commodity access. It seeks to understand individual differences, capabilities and decisions, so as to determine why people use commodities, and how they use and value these commodities (Alampay, 2006).

Capabilities and functionings

In CA, a *functioning* is an achievement, while a *capability* is an ability to achieve. Therefore, there is a relationship between functionings and capabilities (Zheng & Walsham, 2008). Capabilities can be understood as actions and activities in which an individual would like to participate, and which represent elements that the individual aspires to (Robeyns, 2005).

Certain capabilities need, for their development, financial resources and economic production, whereas other capabilities are more reliant on institutional settings, political arrangements, social or cultural practices, and social structures and norms (Zheng & Walsham, 2008).

Examples of functionings are being literate, being part of a community, being confident, and working with others (Robeyns, 2006). In the context of this study, microenterprises' access to, and understanding of how to use, ICTs and online government support information services were treated as capabilities. Instances of microenterprises harnessing these capabilities to search for, and acquire, relevant business support information on the internet using digital government websites were treated as functionings.

Conversion factors

In CA, the relationship between a commodity and functionings is affected by *conversion factors*, which include environmental factors, social factors and personal characteristics (Robeyns, 2005). Environmental factors entail elements such as geographical position, infrastructure, and resources; social factors include power relations, cultural beliefs and practices, and social norms; and personal characteristics include gender, literacy, and physical condition (Nyemba-Mudenda & Chigona, 2017).

Freedom

In CA, *freedom* denotes decisions and actions taken by individuals with regard to their personal lives in particular circumstances (Robeyns, 2003). Full freedom is when individuals have the freedoms or valued opportunities to live the type of life they would like to live, to do what they would like to do, and to be the individuals they would like to be (Nyemba-Mudenda, 2014).

Agency and well-being

In CA, *agency* is the freedom to plan and follow an individual's own objectives and interests, with the pursuit of *well-being*, e.g., via a better standard of living, constituting a potential objective or interest (Zheng & Walsham, 2008).

Justification for use of the CA approach

Although CA has been criticised for being methodologically vague, it was chosen for this study because it allowed for an exploratory approach and interpretive methods, whereby microenterprise owners could define and select relevant capabilities in their contexts (Nyemba-Mudenda & Chigona, 2017). Grounded in the CA approach, the study looked at two sets of commodities—(1) ICTs for general business activities; and (2) online government business support information—and at the capabilities, conversion factors, and functionings linked to these commodities, in the experiences and perceptions of the interviewed Western Cape microenterprise owners.

5. Study methodology

Data was collected via document analysis and semi-structured interviews. The primary documents analysed were government policies and reports, annual reports, and published statistics necessary to establish the context of the Western Cape microenterprises that were targeted. Semi-structured interviews were conducted with 17 microenterprise owners and two digital government experts (from the City of Cape Town and the Cape Winelands District Municipality).

The target population for the interviews consisted of microenterprises in the Western Cape, South Africa, that were using ICTs. The province's two largest municipalities, Cape Town and the Cape Winelands, were targeted because of their active involvement in the province's digital government and ICT programmes. Table 2 provides information on the 17 microenterprises whose owners were interviewed for the study.

Table 2: The 17 microenterprise owners interviewed

Respondent number	Nature of microenterprise	Enterprise's years since establishment	Respondent gender
Respondent 1	Metal manufacturing and welding	3	Male
Respondent 2	Mobile phone accessories	13	Male
Respondent 3	Clothing manufacturing	6	Male
Respondent 4	e-Commerce website	3	Male
Respondent 5	Business support	12	Male
Respondent 6	Clothing retailer	12	Female
Respondent 7	Car accessories	6	Male
Respondent 8	e-Commerce website	6	Male
Respondent 9	Mechanic	31	Male
Respondent 10	Locksmith	4	Male
Respondent 11	Beautician	3	Female
Respondent 12	Bookkeeper	20	Male
Respondent 13	Caterer	25	Female
Respondent 14	Real estate agent (rentals)	24	Female
Respondent 15	Real estate agent (rentals)	4	Female
Respondent 16	Baby care accessories	3	Female
Respondent 17	Plumber	5	Male

The interviews were conducted in March and April 2017. Each interview was audio-recorded, transcribed into a Microsoft Word document, and subjected to thematic analysis.

Permission to conduct the study was obtained from the Western Cape Government's Department of Economic Development and Tourism. Research Ethical Clearance approval was obtained from the University of Cape Town, since the research was conducted in partial fulfilment of the lead author's Master of Commerce in Information Systems degree.

6. Findings

Commodity 1: ICTs for general business activities

In respect of ICTs for general business activities as a commodity, it was found that most of the 17 microenterprises used only generic and affordable ICTs for general business activities, with some notable exceptions. The exceptions were as follows: the microenterprise providing mobile phone accessories owned a point-of-sale system in addition to a laptop and mobile device; the mechanic used specialised software on his laptop to diagnose car repair issues for newer vehicle models; and the locksmith used expensive software to cut specific keys for clients.

Table 3 summarises the ICTs owned and used for general business activities by the 17 microenterprises whose owners were interviewed in this study.

Table 3: ICTs owned and used by the 17 microenterprises

ICT owned and used	Uses	No. of microenterprises
Mobile phone	• communicating with friends • communicating with suppliers • searching for information • electronic fund transfers • online marketing • mobility	17
Laptop	• communicating with clients • invoicing • searching for information • drafting legal documents • diagnosing car issues • online marketing • web design	14
PC	• communicating with clients • communicating with suppliers • invoicing • searching for information • web design	4
Printer	• printing legal documents • printing pamphlets	2
Point-of-sale devices	• selling airtime vouchers	1

Capabilities

The potential capabilities cited by the 17 interviewees included access to information, communication, marketing exposure, cost-savings, efficiency and productivity. In respect of communication, respondent 15 spoke of the potential capabilities in these terms:

> Now you can just email all the documents, but before that wasn't available. You had to go and sit with them [i.e. clients] and fill it in. So, everything is done via the email now.

On the subject of information access, respondent 2 said:

> It makes accessing information much quicker.

The owner of the mobile phone accessories microenterprise was of the view that a potential opportunity for use of the ICT commodity was that it made access to information much quicker.

The beautician (respondent 11) said that, in terms of marketing exposure, it helped her to improve the brand awareness of her business.

> With social media it's easier to get the word out there.

One of the e-commerce microenterprise owners (respondent 4) cited cost savings as a capability offered by ICTs:

> I think one benefits, that you can save a lot of cost by using technology. So, it drives down overheads [for my business].

Conversion factors

It was found that infrastructure (ICT facilities) and resources (ICT resources) influenced how the microenterprises generated a capability set to use the ICT commodity for general business activities. All 17 microenterprises had access to internal ICT facilities in their businesses, which enabled them to use the ICT commodity. Therefore, they did not experience the challenge of having to use shared ICT facilities, such as telecentres and internet cafés, which could affect their general business activities. Furthermore, the 17 microenterprises also had access to ICT resources such as mobile phones, laptops and PCs, which enabled them to use the ICT commodities.

No barriers were identified in respect of the ICT literacy and skills needed to use the ICT commodity for general business activities. The microenterprise owners had either received computer training from a technical college or were self-taught. All could competently use the ICTs they needed. In the words of the locksmith (respondent 10):

> Any computer training that I got was from learning and educating myself.

Instances were identified where socio-economic factors impacted how a microenterprise generated a capability set to use the ICT commodity. For example, the plumber said he used a mobile phone to communicate with clients, to purchase materials and to search for information, with the mobile phone having to serve as his main ICT tool because he could not afford to buy a laptop.

Functionings

The study determined that the microenterprises found that an ICT, i.e., the internet, enabled them to access information such as product and supplier information more quickly. According to respondent 7:

> It has helped me to find [information] that I'm looking for [on the Internet] quicker.

Furthermore, some microenterprises were found to be using their mobile phones, and mobile applications such as WhatsApp, to improve communication with their clients. The beautician (respondent 11) used ICT, in the form of social media platforms (e.g. Facebook and Instagram) to promote her brand and to improve the marketing of her products.

> It definitely has [allowed me to acquire more clients]. So, I post something on social media, and one girl is gonna share it on her [social media] page, and 10 of her friends are gonna see it, and out of that 10, maybe five [are] gonna share it, and so forth. That is how I've built up my clientele, and my name is quite well known because of that.

The mechanic stated that using ICTs enabled him to operate his businesses efficiently and to improve his productivity.

Commodity 2: Online government business support information

Capabilities

The interviewed microenterprise owners identified a number of capabilities that could potentially be harnessed via access to, and use of, online government business support information, including: improved competitiveness; accelerated business growth; improved business management skills, especially marketing skills; additional products and services; acquisition of more clientele; access to new markets; and increased staff employment.

In the words of the locksmith (respondent 10):

> If we had some form of support in that aspect, then I think that the five-year plan that we have would probably turn into two years. It will accelerate growth big time by far.

The car accessories microenterprise owner (respondent 7) suggested that use of online government business support information commodity could create an opportunity for him to grow his business.

> If I could access it, I could perhaps grow my existing business. I could open [a store] in a good location where I could sell on a bigger scale. At the moment, I'm selling on a small scale from home.

The mechanic (respondent 9) said he believed that using government business support information, particularly funding information, could improve the competitiveness of his business, and allow him to employ additional staff.

> You'll obviously employ more people as well. You'll look at increasing the employment level.

The clothing manufacturer stated that accessing online government business support information could help him to market his products.

Conversion factors

It was found that none of the microenterprises could generate functionings from the government websites because of the challenges they experienced in trying to use the sites' business support information. The clothing manufacturer (respondent 3) had tried to find government support information relating to funding (grants and/or loans), but had been unsuccessful. The plumber (respondent 17) had tried unsuccessfully to find support information on business management skills training for his business.

> I tried to access support information for business training because remember we have to run the business in a professional way, so the one thing that we are lacking is how to operate this business efficiently and effectively.

The microenterprises had experienced several challenges in seeking to use support information on government websites to improve the competitiveness of their businesses. The car accessories owner (respondent 16) said that it was difficult, on the government websites, "to find information that is current and not missing anything". The caterer (respondent 13) complained that the sites tended to list outdated contact details.

Another challenge cited was that the support information was not structured to meet the needs of businesses at different maturity levels. According to expert respondent 1:

> [The Western Cape] Government does not offer that [diverse information] because they don't know what is needed. They just use their own idea. If they knew, then they [would] put that [on their] website.

It was stated that the government websites in question needed to be more mobile-friendly, thus improving the accessibility of the support information. According to expert respondent 1:

> As a businessman, I want a website that can scale nicely for mobile use.

The microenterprises also found that navigation of the online government business support information was difficult, which limited their use of the information:

> It's not easy to navigate. (respondent 3)
>
> You don't know where to start [using the website once you get there]. It's organised chaos. (respondent 1)

Additionally, it was found that lack of content in the isiXhosa language was a challenge that prevented some microenterprises from using the support information.

> The one thing that I found out is that it's very difficult for an isiXhosa-speaking person because they [do] not have that website in isiXhosa translation. It was only in English and Afrikaans. If it's not sort of like trilingual, because English, Afrikaans and isiXhosa are the predominant languages in the Western Cape, then how [do] they expect people [to access the support information]? (respondent 15)

Functionings

The capabilities discussed above were those identified by the microenterprise owners as potentially resulting if they could make use of online government business support information. Therefore, their discussions of functionings were only in respect of *potential*, not *actual,* functionings.

The plumber (respondent 17) mentioned that he could use funding gained via support information to purchase additional vehicles and equipment, thereby increasing the operational capacity of, and growing, his business.

> It [would] help me to buy more vehicles because I want to buy more vehicles. Normally [in] the business of plumbing, the basic thing that you need is a vehicle, and buying equipment.

Another microenterprise owner spoke of potential functionings that could arise from business management skills training, especially marketing training, if he could find such training via online government support information.

> If I received training on marketing, I could market and sell my products better. (respondent 2)

The locksmith (respondent 10) also cited potential functionings that could emerge if online government information could connect him to business skills development opportunities—including, for example, branching out into closed-circuit television accessories:

> It would create [new] services for our business.

The mobile phone accessories microenterprise owner (respondent 2) said that if he could grow his business through using online government support information, he would expand his operations into new markets.

> [Accessing support information] would allow me to open another shop that could also create more opportunities for employment.

The bookkeeper said that if he could make use of online government support information on how to provide internships to unemployed graduates, he could train and mentor graduates, thereby indirectly contributing towards mitigating the high unemployment rate in South Africa.

Freedom, agency and well-being

Elements of potential freedom, agency and well-being cited by the interviewed microenterprise owners as being potentially linked to online government business support information included: women's empowerment, an improved standard of living, increased self-confidence and increased motivation.

The locksmith, car accessories microenterprise owner and clothing retailer all stated that they believed use of online support information on matters of funding and skills development could, by improving the competitiveness of their businesses, enable them to more freely pursue their personal objectives and interests, such as accessing higher education, building a home, and achieving an improved standard of living.

> Personally, it would give me the opportunity to do the things that I love doing … which is to study, to learn more, and to grow [personally]. [respondent 10]
>
> It would speed up my personal goals. For example, I would like to build my own house. [respondent 7]
>
> It [would] improve my standard of living. [respondent 6]

The mobile phone accessories enterprise owner (respondent 2) believed that if he could use online government support information to make his business more stable, it would enable him to achieve his personal objective, which was to devote more energy to his home life.

> It would give me more time to spend with my family.

The caterer believed that if she could access funding, it would give her the freedom to achieve her personal objective, which was to empower female homemakers by training them to cook and cater at small-scale events.

7. Discussion

Microenterprises' use of ICTs for general business activities

The study found that microenterprises mostly used mobile phones (all 17 enterprises) and laptops (14 enterprises) for general business activities. This aligns with the findings of Donner (2006) and Esselaar et al. (2007) that microenterprise owners mostly use mobile phones for their business activities. Among the benefits of mobile phones for microenterprises are immediate access to, and better use of, information, and rapid communication (i.e., rapid information flow) (Julsrud & Rolan, 2014).

The study found that some of the microenterprises favoured the use of mobile phones, as opposed to laptops, for information access, because of the challenge of affordability, i.e., not having the necessary funds to purchase or lease a laptop. For instance, the plumber said he used his mobile phone for most of the functions of his business—including communicating with clients, purchasing materials and searching for information—because he could not afford a laptop.

The microenterprises were also found to be attempting to access support information relating to business skills development, products and services development, and funding. Literature suggests that individuals seek information to satisfy a knowledge gap or a desired goal (Malanga & Jorosi, 2018). This was evident in the information needs that were identified by the enterprises, e.g., information on marketing, products and services, and grant and loan information.

There was an expectation that some microenterprises would access business support information through shared ICT facilities, such as telecentres and internet cafés. This expectation was based on existing research showing that ineffective ICT infrastructure and limited ICT resources are among the many ICT challenges that microenterprises experience in developing countries (Chigona, Lekwane, Westcott & Chigona, 2011), and that shared ICT facilities would therefore be attractive to the enterprises. However, this was found not to be the case with the respondents in this study.

Microenterprises' experiences with online government support information

It was found that the microenterprises surveyed experienced several challenges with using online government support information. Among other things, the microenterprises generally found that the online government support information tended to be outdated, incomplete and unreliable. This finding aligns with statements in Parliament, to the National Council of Provinces (NCOP) Economic and Business Development Committee, to the effect that microenterprises experience challenges in finding and accessing reliable information (PMG, 2012).

It was found that the microenterprises also regarded online government support information as often irrelevant, i.e., because the information was not structured to meet the needs of businesses at different maturity levels, from start-ups to established businesses. The majority of participants in this study were established businesses, and therefore required support information linked to growing their businesses and becoming more competitive. However, the respondents found that most of the online government support information was aimed at start-up businesses. The digital government expert interviewee who consulted to the Western Cape Government said that the government did not offer diverse online support information because it was not sufficiently aware of what businesses at different maturity levels needed (expert respondent 2).

Some enterprise owners said they found certain online business support information too complex and sometimes even incomprehensible. This challenge was found to have prevented the clothing manufacturer from accessing support information relating to grants and loans. This finding corresponds with Makoza's (2011) finding that many microenterprises struggle to evaluate support information and to apply the information in their business activities. It was also found that the microenterprises were critical of the navigation modalities of government websites. This finding aligns with Lotriet's (2005) finding that ineffective website design can lead to inaccessibility of information. Surveyed enterprise owners also stated that government websites were not designed to be mobile-friendly, thus creating an additional usage barrier.

Another complaint voiced by some of the surveyed enterprise owners was that a barrier was created by the absence of government website content in the isiXhosa language, which was the home language of many of the microenterprise owners. This finding corresponds with the findings from a study by Agangiba and Kabanda (2016), who found that aspects of culture, such as language, can be substantial obstacles to the use of digital government services.

Also identified by the microenterprise owners surveyed were the challenges presented by cumbersome bureaucratic procedures linked to government online business support, e.g., applications for funding. One of the e-commerce microenterprise owners (respondent 15) said he had to complete a 20-page questionnaire just to see if he could qualify for funding. This finding aligns with findings from other research showing that some of the biggest hindrances to the growth of entrepreneurs in South Africa are the many regulatory obstacles (Mitrovic & Bytheway, 2009). The challenges that South African small enterprises experience when seeking to comply with regulations have also been voiced in Parliament, in the aforementioned hearing of the NCOP Economic and Business Development Committee (PMG, 2012).

8. Conclusions

The study sought to explore the challenges that microenterprises in South Africa's Western Cape Province experience in using ICTs and in using support information on government websites. Guided by the capability approach framework, we treated ICTs and online government business support information as two separate commodities.

In respect of the first commodity—*ICTs*—it was found that the microenterprise owners had an appreciation for ICTs, and were able to gain several benefits from using them, including improved access to information, improved communication, improved marketing, reduced costs, improved efficiency and improved productivity. It was also found that the microenterprise owners did not experience any particular ICT access or usage challenges.

In respect of the second commodity—*government online business support information*—it was found that the microenterprises experienced challenges when they attempted to access and use the information. The difficulties encountered were found to be a result of deficiencies in content, structure, design, navigation, mobile-friendliness, language provision and bureaucratic requirements. These challenges were found to limit the benefits that the microenterprises could derive from the support information. It is thus evident that for the G2B information services to be of value to Western Cape microenterprises, numerous deficiencies must be addressed.

The support information must be up-to-date, complete and relevant for established businesses. There is also a need for the structure of the support information to be simplified, i.e., the information must be made clearer and easier to comprehend. The information targeting Western Cape businesses should be available in at least three languages: English, Afrikaans and isiXhosa. We also recommend the development of a national, centralised and inclusive G2B portal that links to all South African online government business support information at the national, provincial and municipal levels. This would help the South African Government to more fully pursue digital transformation of its support services to microenterprises, and, in turn, to stimulate enhanced economic growth.

References

Abor, J., & Quartey, P. (2010). Issues in SME development in Ghana and South Africa. *International Research Journal of Finance and Economics*, *39*, 218–228.

Agangiba, M., & Kabanda, S. (2016). E-government accessibility research trends in developing countries. In *Proceedings of the Mediterranean Conference on Information Systems* (pp. 1–18).

Alampay, E. A. (2006). Beyond access to ICTs: Measuring capabilities in the information society. *International Journal of Education and Development using Information and Communication Technology*, *2*(3), 4–22.

Alexander, P. M., & Phahlamohlaka, L. J. (2006). Amartya Sen's Capability Approach applied to Information Systems research. *South African Computer Journal*, *37*, 1–11.

Bwalya, K. J., & Healy, M. (2010). Harnessing e-government adoption in the SADC region: A conceptual underpinning. *Electronic Journal of e-Government, 8*(1), 23–32.

Bwalya, K. J., Du Plessis, T., & Rensleigh, C. (2013). *Multi-dimensional factors impacting on e-government adoption in Botswana, Mozambique, and Malawi*. In S. K. Sharma (Ed.), *Adoption of virtual technologies for business, educational, and governmental advancements*. Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-4666-2053-7.ch005

Chacko, J. G., & Harris, G. (2006). Information and communication technology and small, medium, and micro enterprises in Asia-Pacific – size does matter. *Information Technology for Development, 12*(2), 75–177. https://doi.org/10.1002/itdj.20034

Charman, A. (2016). *The South African township economy and informal micro-enterprises: What are the prospects for youth employment and entrepreneurship?* Washington, DC: Development Policy Research Unit, World Bank.

Chigona, W., Lekwane, O., Westcott, K., & Chigona, A. (2011). Uses, benefits and challenges of public access points in the face of growth of mobile technology. *The Electronic Journal of Information Systems in Developing Countries, 49*(5), 1–14. https://doi.org/10.1002/j.1681-4835.2011.tb00349.x

City of Cape Town. (n.d.). [Website]. Retrieved from https://www.capetown.gov.za/

Department of Small Business Development. (2019). Revised Schedule 1 of the National Definition of Small Enterprise in South Africa. Pretoria: Government of South Africa.

Department of Trade and Industry (DTI). (n.d.). Small medium micro enterprise development. Retrieved from http://www.dti.gov.za/sme_development/sme_development.jsp

Donner, J. (2006). The use of mobile phones by microentrepreneurs in Kigali, Rwanda: Changes to social and business networks. *Information Technologies and International Development, 3*(2), 3–19. https://doi.org/10.1162/itid.2007.3.2.3

Duncombe, R., & Heeks, R. (2005). *Information and communication technologies (ICTs), poverty reduction and micro, small and medium-scale enterprises (MSMEs).* Manchester: Institute for Development Policy and Management (IDPM), University of Manchester.

Esselaar, S., Stork, C., Ndawalana, A., & Deen-Swarray, M. (2007). ICT usage and its impact on profitability of SMEs in 13 African countries. *Information Technologies and International Development, 4*(1), 87–100. https://doi.org/10.1162/itid.2007.4.1.87

Gigler, B.-S. (2004). Including the excluded – Can ICTs empower poor communities? Towards an alternative evaluation framework based on the capability approach. Paper presented at the 4th International Conference on the Capability Approach, 5–7 September, University of Pavia, Italy.

Good, T., & Qureshi, S. (2009). Investigating the effects of micro-enterprise access and use of ICTs through a capability lens: Implications for global development. In *Proceedings of the 2nd Annual SIG GlobDev Workshop,* Phoenix, AZ, December 14.

Grönlund, Å. (2011). Connecting egovernment to real government: The failure of the UN eParticipation Index. In M. Janssen, H. J. Scholl, M. A. Wimmer, & Y.-H. Tan (Eds.), *Electronic Government: 10th IFIP WG 8.5 International Conference, EGOV 2011, Delft, The Netherlands, August 28 – September 2, 2011: Proceedings* (pp. 26–37). Berlin: Springer. https://doi.org/10.1007/978-3-642-22878-0_3

Grunfeld, H., Hak, S., & Pin, T. (2011). Understanding benefits realisation of iREACH from a capability approach perspective. *Ethics and Information Technology*, *13*(2), 151–172. https://doi.org/10.1007/s10676-011-9268-4

International Financial Corporation (IFC), & World Bank (2018). *The unseen sector: A report on the MSME opportunity in South Africa*. Washington, DC.

Jantjies, S. O. (2010). *An evaluation of e-government within the Provincial Government Western Cape (PGWC).* Master's dissertation, University of Stellenbosch, South Africa.

Julsrud, T. E., & Rolan, M. D. G. Z. (2014). Mobile phones and business networks among Malaysian micro and small enterprises: A comparative network approach. *Asia-Pacific Social Science Review, 14*(1), 21–42.

Kaisara, G., & Pather, S. (2011). The e-government evaluation challenge: A South African *Batho Pele*-aligned service quality approach. *Government Information Quarterly, 28*(2), 211–221. https://doi.org/10.1016/j.giq.2010.07.008

Kamal, M., & Qureshi, S. (2009). Sustaining the growth of micro-enterprises that adopt information and communication technologies. In *Proceedings of the Annual Workshop of the AIS Special Interest Group for ICT in Global Development,* Phoenix, AZ.

Lotriet, H. (2005). Accessibility of South African Web sites to visually disabled users. *South African Journal of Information Management*, *7*(2), 1–9. https://doi.org/10.4102/sajim.v7i2.263

Malanga, D. F., & Jorosi, B. N. (2018). Information literacy skills among the undergraduate students at the University of Livingstonia, Malawi. *International Journal of Library and Information Services (IJLIS), 7*(2), 43–56. https://doi.org/10.4018/ijlis.2018070104

Makoza, F. (2011). *The impact of ICT use on livelihoods of microenterprises: Case of South Africa*. Master's dissertation, University of Cape Town.

Makoza, F., & Chigona, W. (2012). The livelihood outcomes of ICT use in microenterprises: The case for South Africa. *The Electronic Journal on Information Systems in Developing Countries, 53*(1), 1–16. https://doi.org/10.1002/j.1681-4835.2012.tb00374.x

Makoza, F., & Chigona, W. (2014). Accessibility of e-government websites: Case of Malawi. In *Proceedings of the 15th Annual Conference on World Wide Web Applications,* Cape Town (pp. 10–13).

Malik, B. H., Shuqin, C., Mastoi, A. G., Gul, N., & Gul, H. (2016). Evaluating citizen e-satisfaction from e-government services: A case of Pakistan. *European Scientific Journal*, *12*(5), 346–370. https://doi.org/10.19044/esj.2016.v12n5p346

Matavire, R., Chigona, W., Roode, D., Sewchurran, E., Davids, Z., Mukudu, A., & Boamah-Abu, C. (2010). Challenges of egovernment project implementation in a South African context. *The Electronic Journal Information Systems Evaluation, 13*(2), 153–164.

Mawela, T., Ochara, N. M., & Twinomurinzi, H. (2016). E-government implementation: Lessons from South African municipalities. In *SAICSIT '16: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, Johannesburg, September 26–28. https://doi.org/10.1145/2987491.2987499

Moyi, E. D. (2003). Networks, information and small enterprises: New technologies and the ambiguity of empowerment. *Information Technology for Development, 10*(4), 221–232. https://doi.org/10.1002/itdj.1590100402

Mitrovic, Z., & Bytheway, A. (2009). Awareness of e-government related small business development services in Cape Town. *The Electronic Journal of Information Systems in Developing Countries*, *39*(4), 1–14. https://doi.org/10.1002/j.1681-4835.2009.tb00278.x

Mutula, S. M. (2013). E-government divide: Implications for sub-Saharan Africa. In D. Ocholla, J. Britz, R. Capurro, & C. Bester (Eds.), *Information ethics for Africa: Cross-cutting themes* (pp. 59–69). Pretoria: African Centre of Excellence for Information Ethics, University of Pretoria.

Noruwana, L., Chigona, W., & Malanga, D. F. (2018). How information and communication technologies empower disadvantaged communities in Cape Town, South Africa. In *SAICSIT '18: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologies*, Port Elizabeth, South Africa (pp. 171–178). https://doi.org/10.1145/3278681.3278702

Nussbaum, M. (2009). Capabilities as fundamental entitlements: Sen and social justice. In K. Schneider, & H.-U. Otto (Eds.), *From employability towards capability* (pp. 15–43). Luxembourg: Inter-Actions.

Nyemba-Mudenda, M. (2014). *A pathway through which mhealth outcomes are produced for maternal healthcare consumers in a developing country context*. PhD thesis, University of Cape Town.

Nyemba-Mudenda, M., & Chigona, W. (2017). mHealth outcomes for pregnant women in Malawi: A capability perspective. *Information Technology for Development*, *24*(2), 245–278. https://doi.org/10.1080/02681102.2017.1397594

Parliamentary Monitoring Group (PMG). (2012). Small medium & micro enterprises [Summary of Committee meeting]. Economic and Business Development Committee, National Council of Provinces (NCOP). Retrieved from https://pmg.org.za/committee-meeting/15288/

Praditya, D., & Janssen, M. (2015). Benefits and challenges in information sharing between the public and private sectors. In *Proceedings of the 15th European Conference on e-Government 2015: ECEG 2015* (pp. 246–253).

Research ICT Africa (RIA), & University of Cape Town (UCT). (2018). *Western Cape digital readiness assessment 2015*. For the Western Cape Department of Economic Development and Tourism. Retrieved from https://www.westerncape.gov.za/assets/departments/economic-development-tourism/digital_readiness_full_report.pdf

Robeyns, I. (2003). The capability approach: An interdisciplinary introduction. Paper presented to Training Course preceding 3rd International Conference on the Capability Approach, Pavia, Italy, 6 September. Retrieved from https://www.semanticscholar.org/paper/The-Capability-Approach%3A-An-Interdisciplinary-Robeyns/49fbe60b5aa9152d3789e43b8991bc6034f24f49

Robeyns, I. (2005). The capability approach: A theoretical survey. *Journal of Human Development, 6*(1), 93–117. https://doi.org/10.1080/146498805200034266

Robeyns, I. (2006). The capability approach in practice. *Journal of Political Philosophy*, *14*(3), 351–376. https://doi.org/10.1111/j.1467-9760.2006.00263.x

Rogerson, C. (2008). Tracking SMME development in South Africa: Issues of finance, training and the regulatory environment. *Urban Forum, 19*(1), 61–81. https://doi.org/10.1007/s12132-008-9025-x

Rubaii-Barrett, N., & Wise, L. R. (2008). Disability access and e-government: An empirical analysis of state practices. *Journal of Disability Policy Studies, 19*(1), 52–64. https://doi.org/10.1177/1044207307311533

Sen, A. (1993). Capability and well-being. In M. Nussbaum, & A. Sen (Eds.). *The quality of life*. Oxford: Blackwell. https://doi.org/10.1093/0198287976.003.0003

Sekaran, U., & Bougie, R. (2011). *Research methods for business: A skill-building approach*. New York: John Wiley & Sons.

Shambour, Q. Y. (2012). *Hybrid recommender systems for personalized government-to-business e-services.* PhD thesis, University of Technology, Sydney.

Statistics South Africa (Stats SA). (n.d.). Tourism: Employment, economy, and foreign income. Retrieved from http://www.statssa.gov.za/?p=6166

Venter, S., & Lotriet, H. (2005). Accessibility of South African Web sites to visually disabled users. *South African Journal of Information Management*, *7*(2), 1–15. https://doi.org/10.4102/sajim.v7i2.263

Walton, P., Kop, T., Spriggs, D., & Fitzgerald, B. (2013). Digital inclusion: Empowering all Australians. *Australian Journal of Telecommunications and the Digital Economy, 1*(1), 1–17. https://doi.org/10.7790/ajtde.v1n1.9

Western Cape Government (2012). *eGovernment strategy, 2012–2019*. Retrieved from https://www.westerncape.gov.za/text/2012/10/wcg-draft-e-government-strategy-for-public-comment-october-2012.pdf

Western Cape Government. (n.d.). *Western Cape Government: Overview*. Retrieved from https://www.westerncape.gov.za/your_gov/70

Woodward, D., Rolfe, R., Ligthelm, A., & Guimaraes, P. (2011). The viability of informal microenterprise in South Africa. *Journal of Developmental Entrepreneurship*, *16*(1), 65–86. https://doi.org/10.1142/S1084946711001719

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly, 24*(3), 646–665. https://doi.org/10.1016/j.giq.2007.01.002

Zaidi, S. F. H., & Qteishat, M. K. (2012). Assessing e-government service delivery (government to citizen). *International Journal of eBusiness and eGovernment Studies*, *4*(1), 45–54.

Zheng, Y., & Walsham, G. (2008). Inequality of what? Social exclusion in the e-society as capability deprivation. *Information Technology and People, 21*(3), 222–243. https://doi.org/10.1108/09593840810896000

Appendix: Interview protocol

Opening

1. What are your business goals, which you aim to achieve?

List of capabilities (potential functionings)

2. What are the potential opportunities of using ICTs for your business?
3. What are the potential opportunities of accessing government online support information for your business?

Conversion factors for generating a capability set

4. How do you access ICTs for your business (i.e. internal or shared ICT facilities)?
5. Which ICT devices do you use for your business?
6. Have you received computer training on to how to use the ICT devices?
7. What type of government websites do you use to search for online government support information?
8. What type of online government support information have you accessed or attempted to access?

Conversion factors affecting outcome

9. How competently can you use the ICT devices for your business?
10. What challenges do you experience in accessing online government support information for your business?

Outcome of ICTs for general business (achieved functionings)

11. How has technology enabled you to achieve your business goals?

Outcome of online government business support information (potential achieved functionings)

12. How would access and use of support information enable you to achieve your business goals?

Personal agency

13. How would access and use of ICTs for business enable you to achieve your goals?
14. How would access and use of support information enable you to achieve your personal goals?

Digital Transformation in South Africa's Short-Term Insurance Sector: Traditional Insurers' Responses to the Internet of Things (IoT) and Insurtech

Andrew J. Moodley
Master's Student, LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://orcid.org/0000-0001-6390-4806

Abstract

This article explores the impact of the internet of things (IoT) and insurtech on South Africa's short-term insurance industry. The research found, based on interviews with high-level players in or connected to the South African industry, that while IoT and insurtech are significant potential drivers, the country's incumbent insurers have to date been slow to adopt these digital transformation elements in their business models. This article outlines the drivers of IoT and insurtech, the factors influencing the slow adoption of these elements by traditional South African insurers, and recommendations for the adoption of these elements by South African insurers.

Keywords

insurance, insurtech, internet of things (IoT), business models, digital transformation, South Africa

Acknowledgement

This article draws on the contents of the author's 2018 research report for the Advanced Professional Practice in Digital Innovation and Leadership course, LINK Centre, University of the Witwatersrand (Wits), Johannesburg.

DOI: https://doi.org/10.23962/10539/28657

Recommended citation

Moodley, A. (2019). Digital transformation in South Africa's short-term insurance sector: Traditional insurers' responses to the internet of things (IoT) and insurtech. *The African Journal of Information and Communication (AJIC)*, 24, 1-16. https://doi.org/10.23962/10539/28657

1. Introduction

South African short-term insurers—providers of short-term coverage products, as distinct from annual policies—operate within a highly regulated financial services industry (Short-term Insurance Act 53, 1998; Maupa, 2018). The South African insurance sector, similar to the global industry, is in a continual state of transition, influenced by, inter alia, changing economic factors, privacy laws, customer rights, and access to information requirements (SAIA, 2019). As the needs of consumers evolve and mature, insurers face a continuing challenge to maintain relevance with policyholders (EY, 2017). However, in a digitally transforming sector, traditional insurers have to contend with insurtech start-ups that are using emerging technologies (including internet of things (IoT) technologies), analytics, and other digital transformation capabilities to disrupt traditional insurers' value propositions (IBM, 2011; Pillay, 2019).

South Africa's incumbent short-term insurance players have demonstrated limited adoption of IoT technologies, which can enable new or improved policyholder insights, enable new or improved insurance product and business model innovations, and drive a transformational shift in the value provided to policyholders (EY, 2016; PwC, 2016). By adopting an IoT-centric business model, an insurer can use real-time information to build or improve its products, service models and portfolio—as opposed to using traditional mechanisms, which rely on historical, periodically updated, macro-level data (EY, 2017).

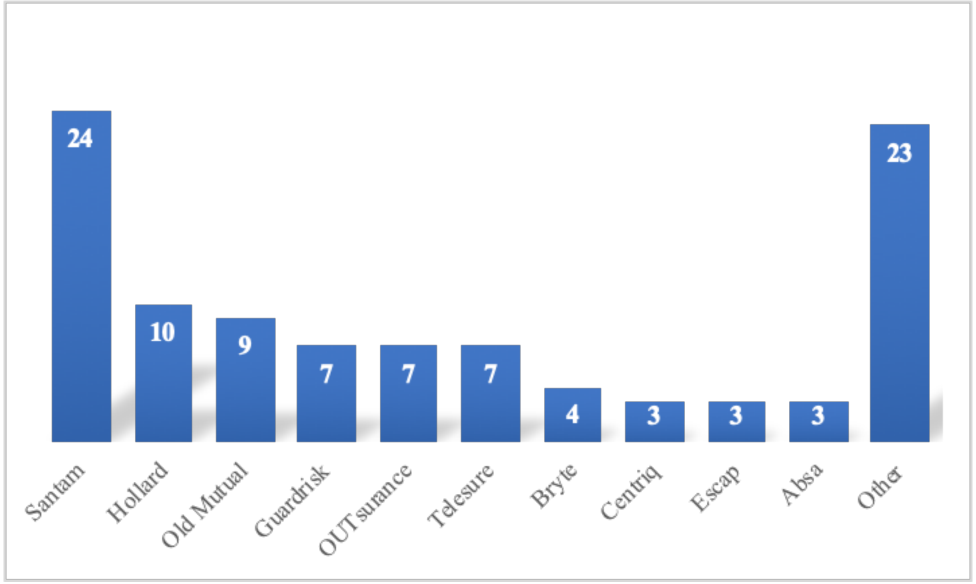
Several South African companies have been providing vehicle-tracking telemetry technology, which is essentially an elementary application of IoT technology, to the insurance sector since the 1990s, but these vehicle-tracking companies, and the insurers, have been slow to leverage the telematics data to provide insurtech benefits in their products (Geotab Africa, 2019; Minnie, 2018).

Due to the still-nascent state of insurtech in South Africa, there is very little published information about insurtech offerings in the country, and the sector information for this study was gathered from news articles, organisational webpages and promotional material. Those insurtech firms that seem to be gaining traction in South Africa have a strong focus on using automation, cloud-based systems, machine learning and mobile apps to modernise the insurance experience or capability, with little use of IoT technology (Littlejohns, 2019). The use of IoT in South Africa is emerging, but with a focus on monitoring and measuring, and its application to the insurance sector is limited (Mpala, 2018).

There are examples of digital start-ups that have developed insurance sector solutions in partnership with a traditional insurer, such as a solution for preventing and reporting geyser (tanked water heater) bursts (Santam Specialist Real Estate, 2019). This geyser solution can also provide the homeowner with an app to manage the geyser and its environment, to leverage machine-learning-delivered insights on the behaviour of the geyser environment, and to benefit from other potential sensors connected to the IoT device (Jonckie, 2019).

In 2016 it was estimated that 65% of vehicles and households in South Africa were not insured, presenting a significant opportunity for insurers (PwC, 2016). Even with that low level of short-term insurance take-up, the sector earned ZAR102 billion in billed premiums in 2018 (KPMG, 2019). Figure 1 shows the leading players, and their revenue sizes, in the short-term insurance industry in South Africa in 2018, based on annualised premiums collected (KPMG, 2019).

Figure 1: South African short-term insurance market in 2018 (annualised premiums, in ZAR billions)



Source: KPMG (2019)

In 2016, according to Accenture (2016), an estimated 55% of South African policyholders had changed insurers in the preceding three to five years in order to pay reduced premiums. It has also emerged that traditional insurance models are not attractive to South African millennials (people born between 1981 and 1996), who make up 28% of the market (Tayengwa, 2017). Millennials, who are "digital natives", present a clear challenge to any insurer that has low engagement, and low investment, in digital transformation strategies (see Ayuso, Guillen & Nielsen, 2019).

Insurtech companies are demonstrating the value of digital innovations in the provision of insurance products. Among other things, these companies use social media platforms to create shared-risk peer groups, i.e., peer-to-peer (P2P) insurance options (PwC, 2016). The entire peer group benefits, in profit distribution and premium reduction, from risk mitigation and risk reduction mechanisms adopted by the group's members (Sandquist, Gasc & Sollmann, 2015). The insurer can create and adjust incentives based on the behaviours that influence the reduction of insurance risk factors or claim frequency, which the insurer benefits from directly in both claim reduction and perceived value by the policyholder (Maupa, 2018).

Meanwhile, the traditional short-term insurance business models thrive on the economic principle that the premiums of a large number of non-claiming policyholders sufficiently cover the payouts to the comparatively smaller number of policyholders who claim, with the premium levels modelled to the guaranteed financial advantage of the insurer (Tayengwa, 2017).

Many South African vehicle owners have accepted the installation of third-party telemetry devices for data collection to aid in stolen vehicle recovery (EY, 2016). These devices collect, store and transmit information such as speed, GPS location and engine performance to a central collection point, such as a vehicle tracking company (Ayuso et al., 2019). Vehicle telemetry devices, which use telematics for their operation, have been in the mainstream for many years in South Africa, and have evolved to include driver behaviour-reporting and accident-scenario determination (Accenture, 2016; Ayuso et al., 2019).

There is undoubtedly a need for South Africa's incumbent, traditional short-term insurers to leverage the business benefits offered by the current implementation of digital technology in the sector, and to evaluate their investment choices with cognisance of the insurtech sector's digitally enabled risk calculation, mitigation and policyholder engagement technologies (EY, 2017). Increasing the use of IoT-generated data in product innovations has the potential to optimise costs, decrease premiums, and allow many of the uninsured to take up insurance tailored to their social, economic and geographic circumstances (Sandquist et al., 2015).

2. Perspectives from the literature

The internet of things (IoT)

The IoT has enabled globally and functionally disparate networks and devices to interact with one another (Lee, 2019; Marek & Woźniczka, 2017). This interaction is enabled by devices that act as a bridge between geographically or topologically disparate networks and devices. These bridges perform local activities, in response to data from their attached sensors, and communicate this data to an online platform for rapid analysis, optimisation and functional adaption (Kang & Choo, 2018; Lee, 2019). This phenomenon of devices that can dynamically communicate and respond is positively contributing to the way organisations design their services and how customers can consume them (Porter & Heppelmann, 2015).

An intelligent device can be any device or thing, embedded with a combination of sensors, actuators and microprocessors, that is proficient in communicating with other devices, systems or even humans (Kang & Choo, 2018). With the advent of IoT and real-time, bi-directional communication, machines and things, not only humans, will be regarded as the customers of an organisation (Hung, 2017). Things becoming customers, while these things are simultaneously augmenting customers' experiences, will create an environment where some of the traditional intermediaries between producers and their customers are potentially bypassed (Porter & Heppelmann, 2015). IoT enables the consumer to digitally interact with products, including maintaining, monitoring, conserving, adjusting and allocating activities (Groopman, 2015). This interaction enables a new level of active engagement, interaction and feedback between consumers and producers (Hung, 2017).

Consumers will embrace and adopt interactive technology as they increasingly gain positive experiences and outcomes from such engagements (Marek & Woźniczka, 2017). With this increase in interactions, a service provider will organically receive more usage data from its customers. As these data points grow, so does the precision of analytics (Porter & Heppelmann, 2015). Analytics develop the service provider's ability to understand customer expectations, which in turn inform product innovation and development, user experience, preventative maintenance, and service delivery innovations, shifting them into a data-driven business (Groopman, 2015). Consider that the traditional urban spaces that people occupy are being transformed into digitally enabled smart cities, driven by the expectation that 60% of the world's population will be urbanised by 2025 (Petrolo et al., 2015). A smart city operates by using technology that leverages sensor data, from IoT-connected devices within the city, to enable citizen services on a large, co-ordinated scale (Hancke, Silva & Hancke, 2012). The integration of IoT into a city changes risk variables and reduces certain risk factors, while at the same time introducing new risk considerations (Breading, 2017).

IoT's transformation of business models

Fuster and Scherrer (2015) examine how new ideas, solutions and services can be created from the collecting, analysing and processing of IoT data that smart devices provide on products' utilisation, contents and consumption. IoT-data driven capability enables organisations to develop or improve products as well as build useful services and businesses (Lee, 2019). It encourages the organisation to broaden its value proposition and reshape itself to leverage the new opportunities that smart devices provide (Porter & Heppelmann, 2015). Business benefits include operational improvement, in-usage optimisation, and preventative maintenance of products—coupled with digitally supported, proactive, and data-driven engagement and response to the market (Hung, 2017). McAfee and Brynjolfsson (2012) show how organisations that leverage data-driven insights to transform their operations or business models perform better on objective financial and operational metrics when compared to their industry counterparts that do not engage in such transformations.

IoT and South Africa's short-term insurance sector

Four factors that catalyse innovative disruption are: (1) a new entrant's product or service addresses consumers' current challenges faced with existing suppliers; (2) existing suppliers are replaced by a new entrant providing an innovative, technology-enabled offering; (3) there are no significant regulatory barriers to impede the disruptive innovation or innovators; and (4) there is aggressive investment from investors driving the adoption of a new innovation or technology (KPMG, 2019). South Africa's incumbent short-term insurers need to consider these factors when determining how to remain relevant to the evolving digital needs of policyholders, to a consumption economy, and to a sector shifting to insurtech (Svahn, Mathiassen, Lindgren & Kane, 2017). The traditional insurer needs to develop the competencies in digital product innovation necessary to satisfy policyholders looking for insurance personalisation, i.e., customisation to their specific social, economic and risk circumstances (IBM, 2011).

Sandquist et al. (2015) describe how insurers adapting to the changes brought by insurtech are focusing on data-driven customer experiences, channel digitisation, the role of ecosystems and IoT. The introduction of IoT-enabled insurance products allows the insurer to introduce experiential value and rewards for the adoption of risk-reducing behaviours. These activities can positively drive the insurer's relevance in the market (Cortis, Debattista, Debono & Farrell, 2019; EY, 2016). IoT adoption is growing, driven by three distinct technology trends (Porter & Heppelmann, 2015). The first is the volume of data generated and received using a variety of technologies and communication standards. The second is the maturity of cloud-based technologies, which now enable the affordable collection, storage and conversion of data into meaningful information. The third is the growing presence of always-connected mobile, smarter and more socially collaborative networks that make vast amounts of information available for decision-making and real-time response (Marafie, Lin, Zhai & Li, 2018). Insurers who integrate these trends into their business models are reaping the rewards. For example, Tayengwa (2017) found that IoT adoption enabled insurers to reduce their quoting and underwriting processing time by as much as 60%, enabling cost reduction and improving policyholder experiences.

Natural disasters affect everyone in a community, and they may result in the loss of property and lives. An IoT-enabled disaster management system can be unified and integrated using real-time alerts and historical data analysis to determine probable areas needing emergency services, crisis management teams and critical relief when a disaster occurs. Insurers can leverage these types of disaster management systems to equip themselves and manage their response in the event of disaster striking (Koduru, Reddy & Padala, 2018). Another emerging trend is the integration of IoT data with analytics tools to build a holistic picture of a risk environment or to manage claims (EY, 2016). Data collected from connected vehicles, buildings and other insured assets are passed on to analytics systems to influence the insurers' processing and underwriting claims (Chekriy & Mukhin, 2018; Cortis et al., 2019). Analytics enable automated claims payment and assist in fraud detection, thus improving the underwriting process and driving down the cost of transactions (McAfee & Brynjolfsson, 2012).

IoT, insurance industry regulation and privacy

The South African Insurance Association (SAIA) is the representative body of the country's short-term insurance industry, and its Executive Committee comprises the country's prominent short-term insurers (SAIA, 2019). Existing insurance industry regulations do not promote digital technologies (SAIA, 2019). The composition of the SAIA Executive Committee may be a limiting factor for the sector, given the potential for the protection of self-interest in regard to the regulation of insurtech.

Globally, consumer rights and information privacy are significant trends in influencing policy and regulation within the insurance sector (Maupa, 2018). Technology innovations have a direct influence on the rise of data privacy and security challenges for insurers and other users of IoT technologies (Zhou, Jia, Peng, Zhang & Liu, 2019). Policyholders are sometimes not consciously aware of their data passing through networks and the storage devices of the insurers and their service providers (Porter & Heppelmann, 2015). This invisible data collection is driving the emerging challenge of digital trust and privacy for the insurance sector (Fuster & Scherrer, 2015). Data collection allows the insurer to provide services to the policyholder that it could otherwise not provide (Petrolo et al., 2015). It simultaneously places an obligation on the insurers to mitigate the leakage of this data, as such leakage could affect the security or invade the privacy of the policyholder (Fuster & Scherrer, 2015). In an always-connected world, it is often difficult to quantify how the data generated is used to benefit the policyholder directly and what data generation unnecessarily compromises the policyholder (Zhou et al., 2019).

3. Research methodology

This study employed a qualitative data-gathering method, via semi-structured, one-on-one interviews with eight senior executives in, or linked to, the South African insurance sector. These interviews occurred between February and April 2018, at the corporate offices of each of the executives, in Johannesburg. The eight executives interviewed (see Appendix A) were from four entities:

- a short-term insurer;
- an organisation building insurance products for short-term insurers;
- a telecommunications operator involved in providing IoT services to the market; and
- an established leader in IoT technology for the South African short-term insurance sector.

The interviews generally followed an Interview Guide (see Appendix B), and focused on understanding:

- how IoT can enable or improve market insights for insurance providers;
- what new or improved insurance models or products are possible through the adoption of IoT; and
- how IoT adoption can transform the short-term insurance market.

4. Findings

IoT and insurtech in South Africa's short-term insurance sector

There was a consensus amongst all eight respondents that IoT technology is essential to South Africa's short-term insurance sector, with the current use of IoT being the use of sensors for event reporting (fire, water, smoke, security alarms); telemetry for asset tracking (vehicles, animals and cargo); human activity tracking to measure healthy behaviours (motion and body statistic sensors); and GPS data for location-based risk calculation.

Five respondents stated that, among the many advantages offered by data-driven insights, they enable policyholders to be voluntarily involved in constant, bi-directional and positive engagement with the insurer. Customer engagement increases, plus the policyholder becomes an active participant and partner in understanding and mitigating risk factors. Cooperation by policyholders releases the insurer from a permanent supervisory and educational cycle with its policyholders regarding risk prevention. The insurer is also able to adjust or modify its rewards systems based on the learnings it derives from the data collection. Policyholders who elect not to meet the adjusted reward conditions do so knowing that this may negatively affect their premiums, benefits or rewards, according to three respondents.

Telemetry use in South Africa originated in the nature conservation sector, leveraged for animal location and anti-poaching activities. South African insurers did not actively seek vehicle-tracking telemetry technology, but instead were introduced to it by technology entrepreneurs. According to two respondents, IoT use in South Africa began approximately two decades ago, when a local organisation partnered with international counterparts to bring industrial telemetry technology to the market. Insurance companies adopted this technology, which proactively transmitted the vehicle's location and movement to aid in stolen vehicle location and recovery. These respondents noted that, around a decade ago, the sector evolved from employing telemetry data for only vehicle location and recovery to also include driver behavioural monitoring and rewards systems. As the technology matured, the traditional insurers leveraged their vehicle telemetry data to evolve their product offerings. They used data analytics to derive new insights into risk factors affecting motor vehicles and engaged policyholders in risk-lowering activities.

All the respondents observed that conditions in South Africa's short-term insurance sector are ripe for insurtech offerings to emerge. A few years ago, an insurtech-centric organisation would have struggled to find resources, capability and market receptiveness. The success of other risk/reward models in the broader market has created a platform for the establishment of insurtech. Additionally, in South Africa, the socio-political environment is conducive to modalities that can grow insurance take-up by the large numbers of people currently uninsured. Value-based insurtech models are highly relevant to the South African context because of their ability to provide differentiated pricing models based on the effect of environmental or situational conditions on the insured item.

IoT and insurtech's impacts on the insurance sector's business models

Traditionally, short-term insurers have determined their risk calculation models based on data gathered at the time of policyholder signup or during a claims process. Digital technologies are changing the face of risk calculation. Two respondents working with telemetry indicated that when insurers initially adopted vehicle telemetry, the technology and network costs restricted the devices' design and function to only a few data points, with data delivered only every few minutes. By 2018, however, insurers were able to collect over 100 data points per second, due to the increased sophistication of the technology. This significant volume of data presents an unprecedented level of insight into motor vehicle risk factors. All respondents agreed that insurers could employ these data-driven insights to engage their policyholders positively.

Insurtech companies, e.g., P2P insurers, have a digital-technology-led operating model. They engage with the market on digital platforms; engage in real-time policy engagement, claim management and rewards redemption; and engage in risk-sharing models with their policyholder communities. They are employing IoT smart home technology to remodel the way they estimate household risk and to digitally dispatch emergency or security services during an incident. Five respondents mentioned that insurtech companies employ sensors to switch off geysers, water and electricity when a leak is detected, with their platforms automatically dispatching repair technicians based on their GPS location and current work status. The ability to detect a risk event in real-time, act to mitigate it, utilise data to inform the risk model, then update the technology in the field and perform preventative maintenance on other similar-state environments is the automated business model of digital insurers.

Utilising IoT, insurers can cover event types that were previously uninsurable or excluded from a policy. For a variety of reasons, policyholders are not always able to fully comply with their contracted risk agreement with an insurer. Four respondents recommended that, instead of penalising the policyholder during these instances, insurers could instead implement new risk models whereby real-time, non-contractual, incident-based insurance products could be created, used and discarded, as required. A respondent gave the example of covering a non-named driver to use a policyholder's vehicle for an errand. Using IoT and mobile application technology, the time of use, the duration of the trip, the driving behaviour and the route of the errand would all be factors that influence the price for that particular insurance instance. Five respondents stated that when small (traditionally uninsured) events are covered in a tailored way, both the insurer and the policyholder gain from the opportunity of a value-adding, bespoke, incident-based, digitally-enabled insurance offering.

IoT, insurtech, and organisational transformation

All eight respondents were of the view that insurers who leverage IoT data can take new data-driven services and products to market. Two respondents said that, through the use of digital technology, the insurer could move its business model away from only insuring risk to also insuring prevention-of-loss events. All eight respondents were emphatic that IoT is a game-changer for insurers. There was consensus amongst all respondents that South Africa, in general across many sectors, has been sluggish in the adoption of IoT and in harnessing the enterprise and employment possibilities it creates. Adoption through external introduction emerged as a central theme in how technology adoption occurs in the South African insurance sector. According to four respondents, the country's insurers are slow to adopt new technology, especially single-use or single-purpose devices. The lack of practical use cases, outside of the vehicle and wildlife tracking telemetry cases, is also a factor that inhibits the adoption of IoT in the insurance sector.

According to six respondents, the sector has to date failed to leverage the successful business case of telemetry to drive acceptance of and investment in new products enabled by IoT. Policyholders with the incumbent firms, five respondents stated, will embrace usage-based and value-based pricing models for insurance as they become familiar with the lifestyle options and experiences that such models provide to them. Four respondents indicated that partnerships with, or acquisitions of, existing insurtech players could be a key mechanism through which traditional insurers could allow new learning to enter their organisations, i.e., allowing for internalisation of the insights and knowledge of an insurtech, including understanding the skills required for employees to participate in the insurtech future.

Traditional insurers' resistance to change

All respondents indicated that organisational resistance to change is prevalent in most incumbent insurance organisations, attributable to the urge to safeguard existing business models and existing stakeholder interests. There is a delicate balance between the financial rewards offered by technology adoption and the magnitude of change required to adapt existing business models. Five respondents stated that insurers' propensity to adopt an innovative technology increased as they grew more familiar with its application, as their organisational models evolved due to the technology, and as the ability of the technology to scale across their policyholder base grew.

Impact of smart cities and smart homes

The communications infrastructure is in place for IoT-driven smart cities and smart homes to emerge strongly in many parts of South Africa, with all the significant mobile GSM telephony providers providing IoT capability on their networks, and with the presence of dedicated IoT networks provided by local and global players, including Consol and Sigfox. Insurtech can be expected to drive the adoption of smart devices in the household, from utility meters to intelligent lighting and security systems.

Seven respondents indicated that the consumer would adopt such technology if the cost of use is lowered, with tangible rewards for the policyholder, such as cost savings or value-adding services. Most homes with internet connectivity have little else connected to the internet or the network, other than personal entertainment and computing devices. An opportunity exists for traditional insurers to look at using their reach, through the existing short-term insurance policies for homes and their contents, to influence the adoption of smart devices, e.g., IoT security cameras, doorbells, lights and locks for insurtech purposes. The insurer could become an active participant in risk mitigation activities, instead of being only the underwriter of theft or loss and allowing a third-party security company to mitigate potential loss with the policyholder.

Privacy and digital trust

Digital trust is a crucial component of the digital age. Insurers need policyholder data and information to innovate and produce customer-centric solutions and offerings. According to four respondents, some consumers believe that telemetry collects data that can negatively affect their insurance premiums or cover, a sentiment that could prevent those insurers who adopt digital business models from retaining or attracting digital pessimists. Policyholders will yield their personal information if insurers prove that the data collection is done morally and ethically, to benefit the policyholder, and not to discriminate negatively against them. Insurers have to begin the journey of digital transformation to develop digital-centric business models that tangibly benefit policyholders, rather than using the data to preserve existing business models and to penalise policyholders. This journey is challenging for a traditional insurer, declared seven respondents, as it requires the insurer business model to change dramatically.

5. Conclusions

Due to the emergence of IoT and insurtech, traditional South African short-term insurance players have to contend with, among other things:

- potential policyholders' increasing access to competitive product offerings;
- existing policyholders' requirements for higher service levels; and
- shifting business models.

New insurtech entrants move at the speed of digital and do not have the shackles of preserving an existing business model and revenue stream, or of being held back by limitations created by their past. Their lack of history allows insurtech firms to swiftly adopt new ideas, leverage new technology, and appropriate social-commercial models, such as P2P risk-sharing and pay-per-use, to defy and erode the policyholder base of traditional insurers.

In addition to, and in support of, growing their own internal IoT and insurtech capabilities, the traditional South African short-term insurance players should seek opportunities to partner with, and/or acquire, existing start-up insurtech and IoT companies, so as to build competence and capacity in the delivery of IoT-based products and services.

Among other things, lowering barriers for insurance adoption, via IoT and insurtech, can open up insurance options to low-income market segments not previously able to procure insurance—because traditional models made insurance prohibitively expensive and practically unusable. Using technology to create an ecosystem where more consumers can participate in insurance services, through insurtech P2P insurance communities and value-based models, will help drive the transformation of the traditional insurer business model. The cornerstone of traditional insurance is that the premiums of the many pay for the claims of the few. IoT-enabled, community-based insurtech offerings will allow incumbent insurers to leverage their market position to utilise technology to benefit all stakeholders, who can collectively reduce risks, claims and costs.

References

Accenture. (2016). Be digital: A R115,2 billion opportunity for South Africa's short-term insurance industry. Johannesburg. Retrieved from https://www.accenture.com/t20170707T155858Z_w_/za-en/_acnmedia/PDF-25/Accenture-Be-Digital-POV.pdfla=en

Ayuso, M., Guillen, M., & Nielsen, J. P. (2019). Improving automobile insurance ratemaking using telematics: Incorporating mileage and driver behaviour data. *Transportation, 46*(3), 735–752. https://doi.org/10.2139/ssrn.2885214

Breading, M. (2017). Smart cities and insurance: Exploring the implications. Strategy Meets Action (SMA). Retrieved from https://cdn2.hubspot.net/hubfs/732222/SMA-RR-2017-Smart-Cities-and-Insurance-082917-V115-Synerscope.pdf?t=1505751589866

Chekriy, S., & Mukhin, Y. (2018). Blockchain platform for insurance-related products. Edinburgh: The Glass Cube Company. Retrieved from https://icosbull.com/whitepapers/3394/i-chain_whitepaper.pdf

Cortis, D., Debattista, J., Debono, J., & Farrell, M. (2019). InsurTech. In T. Lynn, J. G. Mooney, P. Rosati, & M. Cummins (Eds.), *Disrupting finance: FinTech and strategy in the 21st century* (pp. 71–84). Palgrave Pivot. https://doi.org/10.1007/978-3-030-02330-0_5

Ernst and Young (EY). (2016). *The Internet of Things in insurance: Shaping the right strategy, managing the right risks*. London. Retrieved from https://www.eycom.ch/en/Publications/20161109-The-Internet-of-Things-in-insurance/download

EY. (2017). *The future belongs to the connected: Achieving the vision of digital insurance*. London: Ernst & Young. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-achieving-the-vision-of-digital-insurance/$FILE/ey-achieving-the-vision-of-digital-insurance.pdf

Fuster, G. G., & Scherrer, A. (2015). *Big data and smart devices and their impact on privacy*. Brussels: European Parliament Directorate General for Internal Policies. Retrieved from https://www.researchgate.net/publication/289538954_Big_Data_and_Smart_Devices_and_their_Impact_on_Privacy

Geotab Africa. (2019). Adopting usage-based insurance for SA fleets [Blog post]. Retrieved from https://geotabafrica.com/adopting-usage-based-insurance

Groopman, J. (2015). Customer experience in the Internet of Things: Five ways brands can use sensors to build better customer relationships. San Francisco: Altimeter. Retrieved from http://boletines.prisadigital.com/Customer-Experience-in-the-Internet-of-Things-Altimeter-Group.pdf

Hancke, G., Silva, B., & Hancke, J. G. (2012). The role of advanced sensing in smart cities. *Sensors, 13*(1), 393–425. https://doi.org/10.3390/s130100393

Hung, M. (Ed.). (2017). *Gartner insights on how to lead in a connected world: Leading the IoT.* Gartner. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IBM. (2011). *Digital transformation: Creating new business models where digital meets physical.* New York: IBM Global Business Services. Retrieved from https://www.ibm.com/downloads/cas/B6Y8LY4Z

Jonckie. (2019, September 13). Sensor Networks shakes up insurance sector [Blog post]. Retrieved from https://www.insurancechat.co.za/2019-09/sensor-networks-shakes-up-insurance-sector

Kang, B., & Choo, H. (2018). An experimental study of a reliable IoT gateway. *ICT Express, 4*(3), 130–133. https://doi.org/10.1016/j.icte.2017.04.002

Koduru, S., Reddy, P., & Padala, P. (2018). Integrated disaster management and smart insurance using cloud and internet of things. *International Journal of Engineering & Technology, 7*(2.6), 241–246. https://doi.org/10.14419/ijet.v7i2.6.10777

KPMG. (2019). *The South African insurance industry survey 2019*. Johannesburg. Retrieved from https://home.kpmg/content/dam/kpmg/za/pdf/south-african-insurance-survey-2019.pdf

Littlejohns, P. (2019, June 26). Six South African insurtech start-ups disrupting the country's insurance market [Blog post]. Retrieved from https://www.nsinsurance.com/analysis/south-african-insurtech-start-ups

Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things,* 7. https://doi.org/10.1016/j.iot.2019.100078

Marafie, Z., Lin, K.-J., Zhai, Y., & Li, J. (2018). Proactive fintech: Using intelligent IoT to deliver positive insurtech feedback. In *2018 IEEE 20th Conference on Business Informatics (CBI), Vienna*. https://doi.org/10.1109/CBI.2018.10048

Marek, L., & Woźniczka, J. (2017). The Internet of Things as a customer experience tool. *Jagiellonian Journal of Management, 3*(3), 163–176. https://doi.org/10.4467/2450114XJJM.17.011.9562

Maupa, M. (2018). 5 trends shaping the insurance industry in 2018 [Blog post]. Retrieved from https://www.fanews.co.za/article/intermediaries-brokers/7/general/1227/5-trends-shaping-the-insurance-industry-in-2018/23601

McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. *Harvard Business Review*, October, 3–9. Retrieved from http://tarjomefa.com/wp-content/uploads/2017/04/6539-English-TarjomeFa-1.pdf

Minnie, L. (2018, July 13). Best car tracking devices [Blog post]. Retrieved from https://www.autotrader.co.za/cars/news-and-advice/automotive-news/best-car-tracking-devices/2655

Mpala, D. (2018, March 12). 10 South African start-ups leading innovation in IoT [Blog post]. Retrieved from https://ventureburn.com/2018/03/iot-digital-all-stars

Petrolo, R., Loscrì, V., & Mitton, N. (2015). Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. *Transactions on Emerging Telecommunications Technologies, 28*(1), 1–11. https://doi.org/10.1002/ett.2931

Pillay, T. (2019). The influence of insurtech on the existing insurance business model. MBA dissertation, University of Pretoria. Retrieved from http://hdl.handle.net/2263/68935

Porter, M. E., & Heppelmann, J. E. (2015). How smart, connected products are transforming companies. *Harvard Business Review,* October. Retrieved from https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies

PricewaterhouseCoopers. (PwC). (2016). Insurance through challenging times: Insurance industry. Johannesburg. Retrieved from https://www.pwc.co.za/en/assets/pdf/insurance-industry-analysis-2016pdf.pdf

Republic of South Africa (RSA). (1998) Short-Term Insurance Act, No. 53 of 1998. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/a53-98.pdf

Sandquist, E., Gasc, J.-F., & Sollmann, R. (2015). *Reimaging insurance distribution.* Accenture Research. Retrieved from https://financialservices.accenture.com/rs/368-RMC-681/images/reimagining-insurance-distribution-distribution-and-agency-management-survey.pdf

Santam Specialist Real Estate. (2019, May 27). Say hello to the house of the future [Blog post]. Retrieved from https://www.cover.co.za/say-hello-to-the-house-of-the-future

South African Insurance Association (SAIA). (2019). Board members. Retrieved from https://saia.co.za/board-members.html

Svahn, F., Mathiassen, L., Lindgren, R., & Kane, G. C. (2017). Mastering the digital innovation challenge. *MIT Sloan Management Review, 58*(3), 14–16.

Tayengwa, S. (2017). Digital transformation – the new-age insurer. Johannesburg: TransUnion Africa. Retrieved from https://www.cover.co.za/wp-content/uploads/2017/09/Digitisation-In-Insurance-Presentation-SamuelT-1.pdf

Vidanagama, T. N. (2017). Towards realization of an IoT environment: A real-life implementation of an IoT environment and its analytics. In *2017 Global Internet of Things Summit (GIoTS), Geneva.* https://doi.org/10.1109/GIOTS.2017.8016259

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal, 6*(2), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733

Appendix A: Interview respondents

Respondent	Respondent's expertise and experience
Respondent 1: Telemetry Expert	C-level Technology Executive in a telemetry company dealing with all the major insurers. Background in engineering, business and commercial modelling.
Respondent 2: Telemetry Expert	Technology Executive in a telemetry company dealing with all the major insurers. Background in engineering, product development and data modelling.
Respondent 3: Insurance Industry Executive	Senior Business Executive in a large short-term insurer in South Africa with an interest in insurtech. Background in customer services, risk and finance.
Respondent 4: Insurance Industry Executive	Senior Technology Executive in a large short-term insurer in South Africa with an interest in insurtech. Background in technology, procurement and risk.
Respondent 5: IoT Expert	Product Executive in a telecommunications business providing IoT services to business and consumers. Background in marketing and product development.
Respondent 6: IoT Expert	C-level Executive in a telecommunications business providing IoT services to business and consumers. Background in technology, business and strategy.
Respondent 7: Insurance Product Expert	C-level Executive in a specialised company developing products and services for insurers. Background in risk, product development and strategy.
Respondent 8 Insurance Product Expert	Product Executive in a specialised company developing products and services for insurers. Background in risk, product development and business.

Appendix B: Interview guide

IoT as an Enabler of the Insurtech Sector

1. How can IoT enable or improve market insights for insurance providers?

- Where has IoT been deployed in the insurance sector and to what success?
- How has IoT technology evolved since its inception and what does adoption look like now?
- How did the policyholders and customers react to IoT, or not, in terms of value to them?

2. What new or improved insurance models or products are possible through the adoption of IoT?

- How has IoT affected the relevance of insurance providers' products and services?
- What products and service capabilities are possible because of IoT?

3. How can IoT adoption create a transformational shift in the short-term insurance market?

- How is IoT redefining or transforming (or how will it redefine or transform) the business of insurance?
- How will traditional insurance companies contend with digital-first new next generation IoT companies?

Intelligent Malware Detection Using a Neural Network Ensemble Based on a Hybrid Search Mechanism

Stephen M. Akandwanaho
Richfield Graduate Institute of Technology, South Africa
https://orcid.org/0000-0002-1520-1847

Muni Kooblal
Richfield Graduate Institute of Technology, South Africa
https://orcid.org/0000-0001-5145-9071

Abstract

Malware threats have become increasingly dynamic and complex, and, accordingly, artificial intelligence techniques have become the focal point for cybersecurity, as they are viewed as being more suited to tackling modern malware incidents. Specifically, neural networks, with their strong generalisation performance capability, are able to address a wide range of cyber threats. This article outlines the development and testing of a neural network ensemble approach to malware detection, based on a hybrid search mechanism. In this mechanism, the optimising of individual networks is done by an adaptive memetic algorithm with tabu search, which is also used to improve hidden neurons and weights of neural networks. The adaptive memetic algorithm combines global and local search optimisation techniques in order to overcome premature convergence and obtain an optimal search outcome. The results from the testing prove that the proposed method is strongly adaptive and efficient in its detection of a range of malware threats, and that it generates better results than other existing methods.

Keywords

cybersecurity, malware, malware detection, artificial intelligence, neural networks, neural network ensemble, memetic algorithm, optimisation, hybrid search, tabu search

Acknowledgement

This article draws on the contents of a conference paper presented at THREAT 2019: Enhancing Africa's Cybersecurity Posture, 26-27 June 2019, Johannesburg, https://www.threatcon.co.za/2019.html

DOI: https://doi.org/10.23962/10539/28660

Recommended citation
Akandwanaho, S. M. , & Kooblal, M. (2019). Intelligent malware detection using a neural network ensemble based on a hybrid search mechanism. *The African Journal of Information and Communication (AJIC)*, 24, 1-21.
https://doi.org/10.23962/10539/28660

1. Introduction

Malware attacks have increased recently, in Africa and globally, due to advances in technology and the growing number of miscellaneous internet of things (IoT) devices being connected to data networks (Xiao, Lin, Sun & Ma, 2019). The nature of malware attacks has also dramatically changed, as sophisticated attacks have become ubiquitous. The sophistication and complexity of malware have manifested in miscellaneous ways; the common way has been malware camouflage and obfuscation, where the attack comes in the form of a solution to a problem together with a demand for ransom money (Kalaimannan, John, DuBose & Pinto, 2017). This type of attack has continued to evolve and to produce more variants, so that the perpetrators can continue to profit from such pernicious attacks.

According to Symantec, malware has increased sharply since 2014 (Lee & Kwak, 2016) and continues to increase. Symantec also reports that the majority of the new malware programs are variants of the existing destructive malware, which is indicative of the evolution that is taking place in order for the programs to be more complex for the countermeasures and to avoid detection.

In order to mitigate malware, a number of countermeasures have been advanced in the literature (Jerlin & Marimuthu, 2018). However, existing techniques have not fared well due to the obfuscation tactics of malicious software and other advances in evading detection. Malware targets have also expanded to include mobile platforms, thereby posing another challenge to existing mitigation efforts.

Most existing research has reported on the efficiency of machine learning (ML) and artificial intelligence (AI) techniques in malware detection and mitigation (Chen, Su & Qiao, 2018). The techniques are useful in the classification of malware, such as Trojans, worms, among others, and in mapping suitable techniques to the malware type. In addition, the ML techniques, through feature extraction, increase the accuracy of detecting malware by reducing the search space, so as to home in on the specific malware (Khammas, 2018). This alleviates some of the current challenges, including the conventional detection methods being evaded by new variants of malware due to search limitations. This can be attributed to the learning abilities of ML, as well as their capacity to mine data patterns, relationships and procedure analysis.

The modern malware is increasingly adaptive and dynamic in nature, which makes self learning techniques important. Specifically, the self learning techniques, such as neural networks, are able to self-organise and self-evolve, as well as classify and process data in parallel, and are hence able to detect mutated and other instrinsic forms of malware (Barriga & Yoo, 2017).

Agent-based methods have also become promising approaches for malware detection in both web and mobile applications (Kendrick, Criado, Hussain & Randles, 2018). This is due to the interactions between agents and their environments, which create more focused and accurate inputs, so as to generate robust intelligent solutions against malware. (Agents are any entities that can make decisions like a human being through their interactions with one another and the environment.) Moreover, the heterogeneity of agents and of their attributes enriches the capabilities of agent-based applications in combating different types of malware. Through these interactions and the inherent data collection and storage capabilities of agents, patterns can be inferred, which are useful for predictions.

Prediction has been extensively explored in the domain of malware detection, especially using machine learning techniques to predict the behaviour of malware and its hotspots or risk areas (Mahrin et al., 2018). The behavioural analysis of malware also includes classification, which is essential for investigating and prioritising threats. The recent malware attacks have become much more coordinated, for example, botnets which represent a string of devices that are interconnected to communicate and share information with one another, so as to launch large-scale and high-level attacks. Botnets use autonomous programs known as bots, which mimic human behaviour in interactions with users with a view to collecting information and using it to conduct various kinds of malicious attacks (Khoshhalpour & Shahriari, 2018). The level of complexity inherent in these kinds of attacks continues to pose a significant challenge to the traditional malware detection techniques, as well as to the common network environments.

The threat of malware has spread to mobile telephony platforms and proliferated exponentially on account of the openness, and popularity of use, of mobile platforms (Ren, Liu, Cheng, Guo & Chen, 2018). These mobile platforms have become carriers of very sensistive data, ranging from personal financial information to the private details of users' lives. Any data breach on these platforms due to malware attacks can have severe consequences.

The web and desktop platforms nowadays also carry a similar risk, due to a proliferation of desktop applications that enable users to process sensitive information, and also due to mixed storage and processing of business and personal information. One of the biggest attacks in modern times was the WannaCry ransomware attack in 2017, which affected more than 150 countries in less than a week. More than 200,000 devices were attacked in a matter of days, through forcing the encryption of users' data until a ransom was paid (Wang et al., 2018). This is one of the many examples of malware that use advanced algorithms to conduct large-scale malicious attacks. The existential challenge posed by these techniques is their ability to evade detection and literally throw the traditional and less intelligent detection methods into confusion.

In this article, we advance a novel approach, with a view to outflanking the intelligent malware and providing a robust countermeasure to a wide variety of malware. The approach is based on a *neural network ensemble*, wherein an intelligent search optimisation process is conducted by memetic algorithm and by the k-means machine-learning clustering algorithm, in order to generate the optimal solution for complex malware detection. The approach that we advance applies to cyber systems throughout the world. Malware attacks in Africa are similar to attacks elsewhere, and thus we have designed the algorithm with the aim of helping to solve a global problem.

The rest of the article is organised as follows: section 2 provides a review of related work, section 3 provides the problem definition, section 4 provides the methodology, section 5 provides the discussion and presentation of experimental results, and section 6 concludes.

2. Related work

Neural-network-based malware detection

Due to the dynamic behaviour and increasing obfuscation tactics of malware, more intelligent solutions have been sought, and prominent among them are neural networks. Many factors make neural networks attractive for solving problems of this nature, but the overriding factor is that, due to their intrinsic training processes, they achieve accuracy and efficacy in solving very complex problems (Hassan & Hamada, 2017), thus making them suitable for malware detection.

Yan, Qi and Rao (2018) present an *ensemble* method for detecting malware based on a deep neural network. The approach uses a *convolutional* neural network and a memory technique to learn raw data and make inferences regarding the existence or nonexistence of malware. The inferences are based on patterns extrapolated from both the structure and code of the malicious file. (A convolutional recurrent neural network is a blend of the recurrent neural network and the convolutional neural network. Convolutional neural networks can be characterised as those that apply convolutions (a kind of mathematical operation) and that classify data regardless of the positioning.) This approach is similar to the *recurrent neural network ensemble* proposed by Rhode, Burnap and Jones (2018). The ensemble studies behavioural data and makes inferences regarding the maliciousness of an executable file. This is done during the execution by collecting a small sample of behavioural data with a view to detecting and blocking malicious processes before they cause damage. In order to classify this behavioural data, a classifier is presented based on a convolutional recurrent neural network (Alsulami & Mancoridis, 2018), in order to classify families of malware and to extrapolate better patterns for improving detection acurracy. The method extracts features adaptively from MS Windows files to classify them.

In the same vein, Kabanga and Kim (2018) apply the convolutional neural network to the classification of malware *image*. Instead of using text and other forms of data as inputs, image vectors are used to train neural networks. The convolutional neural network is set up with three layers, in order to achieve the classification function.
In order to identify and classify complex patterns in data for malware detection, Le, Boydell, Namee and Scanlon (2018) present a classification method based on deep learning. The approach uses data-driven techniques to identify features for classification. Multiple deep-learning architectures are utilised, and each input is classified into a malware class in terms of various neural network layers, whereby vectors are generated for feature extraction and classification. This classification method contrasts with mechanisms that rely on expert domain knowledge. For example, Zarras, Webster and Eckert (2016) propose a malware classification strategy based on both recurrent and convolutional neural networks. System calls are obtained and sequenced using a sequential model to form a domain for feature extraction and classification. The same principle is applied by Martinelli, Marulli and Mercaldo (2017), wherein a dynamic analysis is conducted on system calls and a convolutional neural network is deployed to distinguish malicious data from benign data in an Android data sample. The recurrent neural networks, unlike convolutional neural networks, recall input samples and reuse them for classification of the current samples.

A dynamic malware detection technique based on deep learning is also presented by Yin, Zhou, Wang, Jin and Xu (2018), wherein malware execution and monitoring functions are separated and analysed independently. A log is produced for the monitoring processes where information is then extracted as the input for the neural network. The training enables the neural network to recognise and classify various types of malware. The approach of Selvaganapathy, Nivaashini and Natarajan (2018) uses a restricted Boltzmann machine (RBM) with a stacking technique to select features in a neural network and detect malicious patterns in uniform resource locators (URLs). A miscellany of classes are used for classification. A similar problem is solved by Le, Pham, Sahoo and Hoi (2017), with convolutional neural networks and the detection technique embedded in the URL so as to train the neural network in all aspects of the URL, including words and characters. An RBM is an artificial neural network that is stochastic (i.e., randomly determined) in nature, and a probability distribution can be generated from its inputs.

In order to detect and classify malware in unseen files, Rad, Nejad and Shahpasand (2018) apply a binary classifier to MS Windows files. The training of the neural network classifier is done with a view to giving it the ability to distinguish malicious files from benign ones.

Many of the aforementioned approaches provide novel solutions, but the malware landscape has dramatically changed in recent years. The changes are mostly epitomised in the shifting optima (Souri & Hosseini, 2018), i.e., shifts in the most favourable solution among a set of constantly changing feasible solutions. The shifting optima makes tracking difficult, and makes it overwhelmingly difficult for static and slow-evolving solution approaches to find optima. Thus, the more efficient malware countermeasures will be those that are highly adaptive and dynamic in their search and optimisation processes for malware detection.

Memetic algorithm solutions

As malware has become more disguised and sophisticated, search heuristics have come to be considered effective optimisation mechanisms, not only for detecting malware threats but also for finding optimal solutions. However, the challenge for single search heuristics is that they get stuck in local optima in the course of the search (Xu et al., 2017), which undercuts the quality of the search outcome. Thus, hybrid mechanisms, such as memetic algorithms, are preferred metaheuristics for conducting the optimisation search process, especially in non-stationary malware environments.

Okobah and Ojugo (2018) present a memetic model for malware intrusion detection. The approach uses classification rules, as well as a fitness function based on the evolutionary process, to generate a feasible solution. Mohammadi and Namadchian (2017) apply a memetic algorithm to optimise detection of irregular traffic. In order to classify malicious traffic, a memetic evolutionary classifier is used. The classifier functions in diverse and dynamic environments. This approach draws parallels with the hybrid mechanism proposed by Xue, Jia, Zhao and Pang (2018), where the feature selection is done by differential evolution, and neighbourhood improvements are conducted by the k-nearest algorithm, with a view to averting premature convergence. Shah, Ehsan, Ishaq, Ali and Farooq (2018) present a hybrid classifier to classify irregular activity. A genetic algorithm and a support vector machine are deployed for, respectively, feature selection and optimising of parameters to enhance accuracy. The training resources required, with respect to time, are significantly reduced through faster covergence, provided a robust and optimal feature selection process exists.

Dash (2017) applies a hybrid of particle swarm optimisation (PSO) and gravitational search to detect intrusions and malicious activity (Dash, 2017). In the same vein, Altaher and Barukab (2017) combine the PSO with the adaptive neural fuzzy inference system in order to distinguish malware-infected Android applications

from malware-free applications. Fuzzy rules are generated to guide the classification process, through intelligent optimisation of parameters, using PSO search based on the evolutionary process that Razak et al. (2018) apply to solve a similar problem.

In the work by Zhirou and Jing (2018), the malicious attack vector is presented as a weighted network, and a memetic algorithm is used to optimise the cost on each node with a view to minimising the cost of attacking a node. An optimal search yields a node combination with the lowest cost.

Although all the approaches outlined above represent state-of-the-art advances in the area, the malware problem landscape continually evolves, at a exponential speed, as a result of the interconnectedness of systems (WEF, 2018) in the fourth industrial revolution (4IR), which demands more intelligent and adaptive solutions provided by advanced algorithms to counter the increasingly complex attacks.

3. Problem definition

The malware detection problem we addressed with this research is a *combinatorial optimisation* problem, where there is a finite set of multiple feasible solutions and the aim is to optimise and generate the best solution (Schweidtmann & Mitsos, 2019). The neural network ensemble we developed represents a blend of various neural networks whose functions are synergised with a view to minimising error and achieving precision (Yan et al., 2018). Neural networks are trained to build a strong capability for solving specific problems. Once they are trained, neural networks generate invidual outcomes which are combined to form an ensemble solution outcome. Ensemble approaches aim to offset the drawbacks associated with individual networks, and they present robust solutions to complex problems.

Accordingly, the problem we seek to address with our proposed model is two-fold: (1) optimisation of a neural network ensemble, and (2) malware detection. The mathematical formulation of the problem is as follows:

Notation	Denotation
C_l	class label
C_m	class of malware
C_b	class of benign
B_i	behaviour
Δ	dataset

$$\Delta = (v_1, v_2, .., v_n) \quad (1)$$

where $v_1, v_2 v_1, v_2$ are feature vectors in the dataset. The behaviour of the data is then represented as $B_{v_n} B_{v_n}$ and the directed graph, which represents the data relationships and dependencies in the form of weights in a neural network (Xiao et al., 2019), is denoted by $G_n G_n$, where nn represents the retrieved number of graphs from the dataset. The behaviour of the sample for a class of malware is defined as follows:

$$B_{S_\Delta} = B_{v_n} C_m \tag{2}$$

$$B_{S_\Delta} = B_{v_n} C_b \tag{3}$$

where $B_{S_\Delta} B_{S_\Delta}$ is the behaviour of the sample, $S,S,$ in the dataset.

Therefore, the behaviour of the dataset is defined as:

$$BS_{G_n} = B_{v_n} C_m + B_{v_n} C_b \tag{4}$$

$$BS_{G_n} = B_{v_n} (C_m + C_b) \tag{5}$$

$B_{v_n} = \{0,1\} \, B_{v_n} = \{0,1\}$ for malware or benign, so that if the sample contains 1 then data is malware and if it contains 0 then data is benign.

This helps to calculate the detection error from the fitness function (Sheng et al., 2017), as follows.

$$F = \beta_1 \, x \, t_e + \beta_2 \, x \, n_c + \beta_3 \, x \, d_t \tag{6}$$

$$t_e = \sum_{j=1}^{P} \sum_{i=1}^{N} (y_i - z_i)^2 \tag{7}$$

$$n_c = \frac{AC}{TC} \tag{8}$$

$$d_t = \frac{1 - B_{V_n} C_m}{B_{V_n}(C_m + C_b)} \tag{9}$$

where $t_e t_e$, $n_c \, n_c$ and $d_t d_t$ denote, respectively, the training error, complexity of the neural network, and detection error. The target output, $y_i y_i$ and current network output, $z_i z_i$ are used to compute the error generated from training the neural network, as shown in Equation (7). The parameters are defined by $\beta_1 \beta_1$, $\beta_1 \beta_1$ and $\beta_1 \beta_1$ while active connections with weights, total connections including those on hidden neurons, training patterns, and neurons, are represented, respectively, by $AC \, AC$, $TC \, TC$, PP and NN. The problem therefore is to minimise the function FF in Equation (6), which ultimately reduces training and detection errors, which in turn increases the detection rate of malware behaviour patterns in the data sample.

The second part of the problem is the optimisation of a neural network ensemble based on connection weights. As mentioned before, the neural network ensemble represents an amalgam of disparate networks (Choi & Lee, 2018), where each individual network generates an output pattern from training input data. The network connections are defined by weights, which indicate the strength of these connections and of the influence of neurons on each other (Ojha, Abraham & Snasel, 2017) through synapses. The influence of neurons is determined by the strength level of the connections between them. The synapses generate an output, as a product of weight and input. Let ww represent weight of the neural network connection, such that $w = w_1, w_2, \dots, w_N w = w_1, w_2, \dots, w_N$ and pp represents inputs. In order to adjust and map outputs and inputs to the neuron, a bias operator, bb is utilised. This is expressed as follows.

$$F = A. \sum_{i=1}^{N} w_i \, p_i + b \tag{10}$$

where all connections, $N,N,$ use the activation function, AA, which activates neurons based on the weight, thus creating a bias to the process with a view to achieving a nonlinear output pattern, as demonstrated by Abiodun et al. (2018). The problem therefore is to optimise the weights in Equation (10) for all connections using a learning optimisation algorithm, so as to create a convergence of high-quality networks to the ensemble.

4. Methodology

Memetic algorithm

Memetic algorithm is one of the methods we used in this study to tackle the optimisation problem defined in the previous section. Memetic algorithm is a blend of global and local search heuristics that combines exploration and exploitation search processes in order to generate high-quality solutions (Nguyen & Sudholt, 2018). The main differentiating factor between memetic algorithm and genetic algorithm is that memetic algorithm mimics the evolution of the cultural environment, rather than mimicking the natural evolution of genes. This capability enables memetic algorithm to lend itself to malware detection, since malware, seeking to avoid detection, is capricious in its attributes and its interactions with the environment (Acarali, Rajarajan, Komninos & Zarpelao, 2019).

The memetic algorithm exploitation function is executed by the local search technique, with a view to forestalling premature convergence of the search process, and thus yielding an optimal result. The local search scours the neighbourhood regions of the solution for a better solution, based on fitness values for mutated solutions. Due to this strength and other benefits, memetic algorithm has been extensively applied to solve various real-world complex problems (Chaimanee & Supithak, 2018) that have become increasingly difficult to deal with through single and non-dynamic optimisation techniques. As indicated by Gu et al. (2019), hybrid algorithms provide a good balance between diversification and intensification of the search, enhancing the quality of the search process as well as the outcome.

In the model we developed and tested, adaptive mutation and recombination operators are applied to the memetic algorithm, in order to create better *offspring* configurations, which are essentially hybrid solutions composed of two existing *parent* configurations. The features from both parent chromosomes (i.e., individual solutions in the sample) are extracted and combined using the recombination operator through individual interactions and cooperation. The mutation operator is then applied to build new features, with a view to forming more robust solutions (Bereta, 2019). The mutation operator helps in calibrating the diversification levels of the population sample, e.g., if there is low diversification, new features are injected by increasing mutation. Figure 1 illustrates this memetic algorithm procedure.

Figure 1: Algorithm 1 (memetic algorithm procedure)

```
begin
P = Intitialise Population
Evaluate fitness of individuals
repeat
      Select parents
      Apply Operators
      Apply Local Search
      Evaluate fitness
         if offpsring is better than the existing individual
           Replace existing solution with offspring
      or else
            keep existing solution
      end if
      Adjust mutation operator
      Update population
until termination criteria reached
return optimal solution
end
```

The population is randomly constructed in Algorithm 1, and one of the essential features of memetic algorithm is application of the local search technique. The local search procedure implemented in this work is the tabu search metaheuristic, and one of the prominent hallmarks of tabu search is its use of the adaptive memory function to store solutions as the search progresses through various iterations. This is important because it makes the information readily available for decision-making at any point in the course of the search (Lucay, Galvez & Cisternas, 2019). The search can then be strategically directed to promising areas where optimal solutions are most likely to be found, based on search information collected by tabu search. Figure 2 illustrates this tabu search procedure.

Figure 2: Algorithm 2 (tabu search procedure)

```
begin
Choose a solution, $ii$ in sample, $PP$
while stop criterion is not reached do
Perform improvement search
Create a subset $s^*s^*$ of solutions in $PP$
Add visited solutions to tabu, t
Evaluate fitness of individuals
Choose best, $jj$ in $s^*s^*$
if $f(j) > f(i)f(j) > f(i)$ then
Replace $ii$ with $jj$ in $PP$
end if
Update tabu list
Output optimal solution
end
```

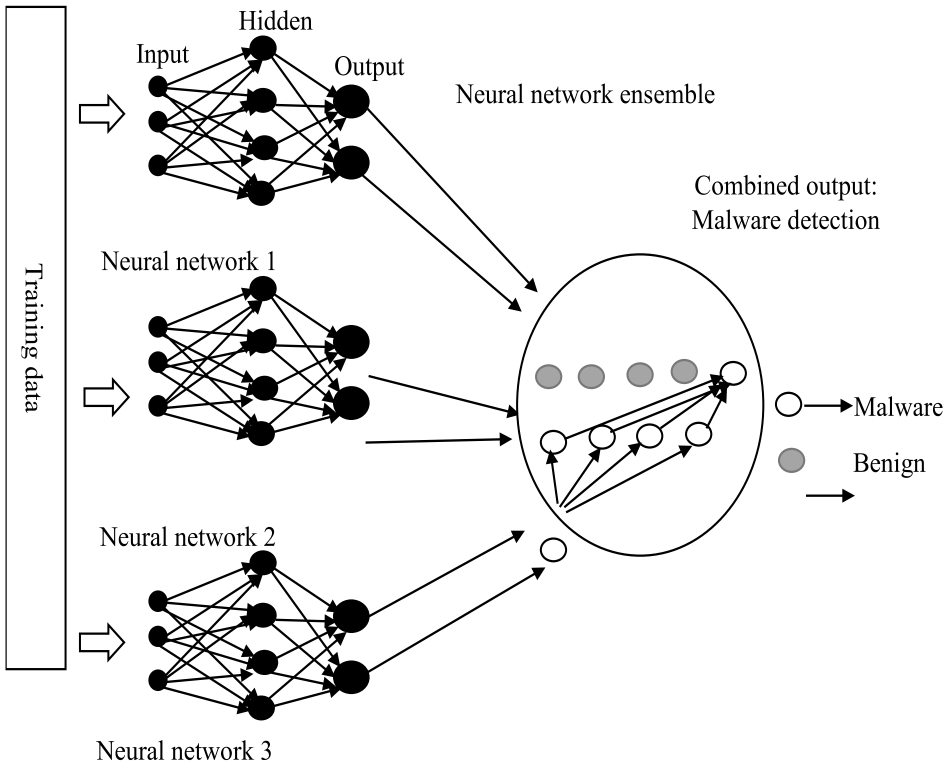
In the tabu search algorithm, solution cycling is prevented via continual improvements until there is attainment of local optimality. The tabu search procedure in Algorithm 2 depicts process steps for local exploitation of the search space with a view to forestalling premature convergence. The procedure exemplifies dynamic local search optimisation, where continual update of the tabu list is conducted. This lends itself to malware detection and search environments, especially in today's environments where malware evolves rapidly. The application of tabu search in optimisation is guided by *weightage* to determine the penalty severity of constraint violations (Dai, Cheng & Guo, 2018). Hard constraints, which are constraints that must be satisfied and applied, carry high weights, and thus large penalties in the case of violations, while soft constraints carry lower weights and smaller penalties.

Neural network ensemble

A neural network is a data-based network that maps inputs to output patterns, or processes inputs to generate output through training processes. The neural network architecture mimics the natural functioning of the brain, in which billions of interconnected neurons transmit signals to each other to generate activity or action for the various functions of the body (Shapshak, 2018). In order to apply this natural phenomenon to computing, artificial neural networks are designed to simulate the neuron structure and processes of the brain, with a view to creating cognitively intelligent computer systems that can be deployed to solve complex problems (Jat, Dhaka & Limbo, 2018).

Neural networks go through training processes to enable them to learn and develop the required capability and mastery to solve various problems. The learning of the neural network is based on the way information travels through networks, as propagated by neurons. The neurons are connected to one other and assigned weight values to indicate the importance and value of each connection. The neural network observes and learns the information flow, and influence, of the neurons. This can be achieved by *feed-forward*, where learning is performed in a forward sequential format from inputs to outputs, or by *back-propagation*, where the optimisation procedure is reversed, starting from the actual outputs and comparing them with the expected output, so as to adjust the connection weights with a view to decreasing the error. Figure 3 illustrates the functioning of a neural network ensemble.

Figure 3: Neural network ensemble, and its application to malware detection



A neural network ensemble represents a blend of individual neural networks that is aimed at combining various models to generate an environment with strong generalised capacity and minimal error (Li et al., 2018). The mathematical formulation of the neural network that we developed and tested is as follows:

From Figure 3, let AA, BB and CC represent neural networks 1,2 and 3, such that $A = (a_1,a_2,\dots,a_n)A = (a_1,a_2,\dots,a_n)$, $B = (b_1,b_2,\dots,b_n)$ $B = (b_1,b_2,\dots,b_n)$ and $C = (c_1,c_2,\dots,c_n).C = (c_1,c_2,\dots,c_n)$.

Let ww denote the weights and DD be the network that represents the combined output of neural networks, A, BA, B and CC. The activation function is used to map inputs to output based on the weights of connections for inputs as well as biases between neurons (Eger, Youssef & Gurevych, 2018), such that $f = (A+B+C).w \rightarrow Df = (A+B+C).w \rightarrow D$. The neural network ensemble in Figure 3 is therefore presented as follows.

$$D = \delta \sum_{i=1}^{n} w * (A+B+C) + b \tag{11}$$

where $\delta\delta$, ww and bb are the activation function, the weight and bias vectors respectively. The bias factor helps to influence the outcome of the neural network, as well as its behaviour by determining the triggering value of the activation function, $\delta\delta$, hence acting as an anchor to the network.

This implies that with this additional parameter, the behaviour of the neural network can be adjusted with a view to achieve optimal learning and performance. In order to get an optimal neural network ensemble, the optimisation of the individual neural networks is vital (Ju, Bibaut & Van der Laan, 2018) and to this end, a memetic algorithm is deployed in this work to optimise the search process by exploitation and exploration of the search space so as to generate high quality trained neural networks that can compose a robust ensemble network.

5. Experiments

The experiments are conducted using the Intel Core i3-4005U @1.70GHz(4 CPUs), 8GB RAM, 64-bit Operating System. R-programming and MATLAB environments are used for the neural network ensemble implementations and analysis. The neuralnet Library in the R platform is utilised to train the neural networks. The environments are also used to perform memetic optimisation, where global search, as well as local search improvements, are done using genetic and tabu search algorithms respectively. A stacking approach is used to combine classifiers, so as to synthesise estimate outputs from various neural networks and achieve high levels of accuracy (Ma, Wang, Gao, Wang & Khalighi, 2018). A single outcome is then produced for the neural network ensemble. The optimisation threshold in the neural net is set at

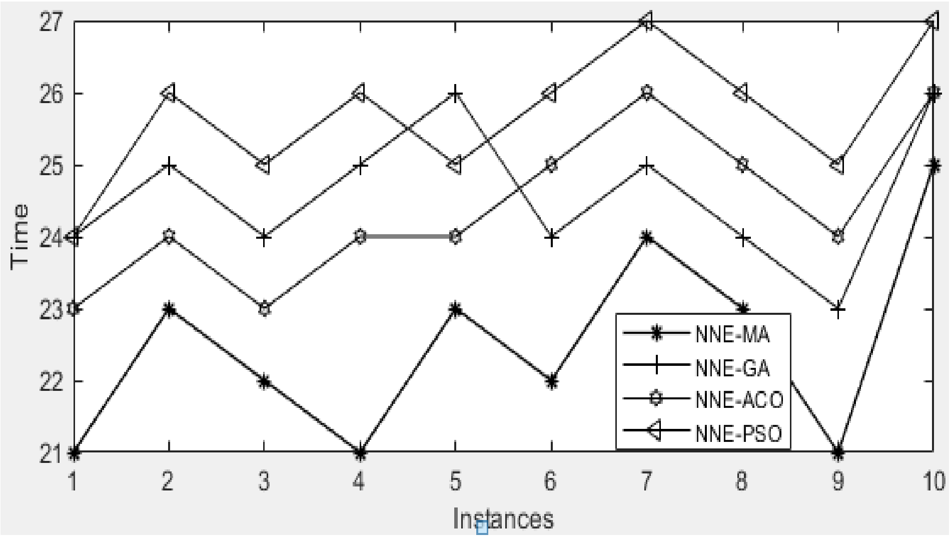
0.1, such that if the $error < 0.1error < 0.1$, the optimisation will automatically stop.

The datasets used are obtained from the Center for Machine Learning and Intelligent Systems (2016). The training datasets are multivariate, with both malicious and benign features labelled as -1 and +1 respectively. Features are extracted, and data is divided into *testing* and *training* sets. The algorithm is first trained on the training dataset before conducting actual tests, so as to be able to detect malware. The mathematical formulation for the training is as follows:

> Let $\sigma\sigma$ be the learning rate at $0.00010.0001$, which controls the rate at which weights update, for each training epoch.

Feature selection is conducted by memetic algorithm, which helps to avoid premature convergence and to reduce data dimensionality and computational resource use, in order to achieve faster convergence. The neural network ensemble using a memetic algorithm (NNE-MA) is compared with well-known optimisation techniques on a similar set of datasets. The techniques are genetic algorithm (GA) (Amjad et al., 2018), ant colony optimisation (ACO) (Xu et al., 2018), and particle swarm optimisation (PSO) (Liu, Li & Zhu, 2019). The neural network ensemble is then combined with each of these techniques for feature selection optimisation, which results in, respectively, the NNE-GA, NNE-ACO, and NNE-PSO convergence comparisons, as shown in Figure 4.

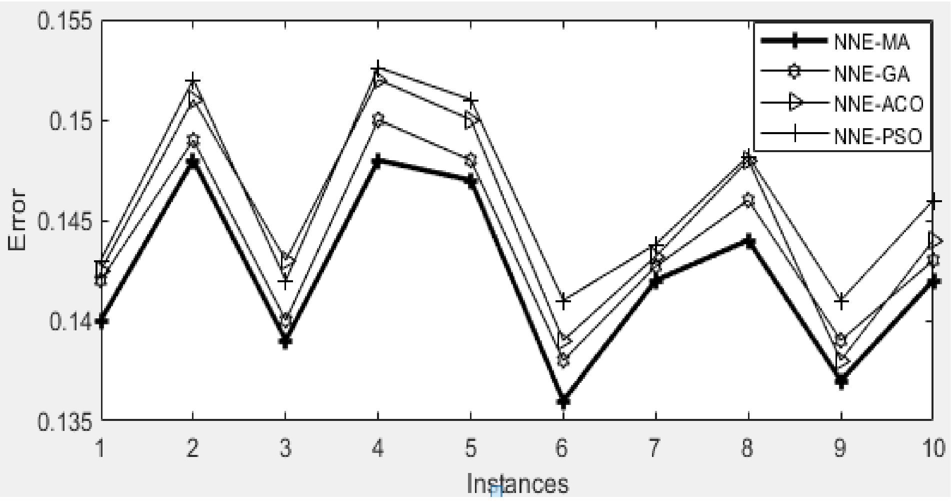
Figure 4: Convergence comparisons between NNE-MA and NNE with existing algorithms



The training error as defined in Equation (9) (presented earlier, in section 3) represents the difference between the current output and the desired output, as per the labels. The actual output is defined in Equation (11) (presented earlier, in section 4), based on weights and bias of neural networks. The error that is generated is measured by the difference between the expected and obtained outputs based on the specific threshold value.

The neural network ensemble using a hybrid search (NNE-MA) produces the least error across all epochs, as shown in Figure 5. This can be ascribed to the improvement in the search mechanism embedded in the memetic algorithm to improve the fitness of solutions, as well as to provide a balance between intensification and diversification of the search. The tabu search, as presented in section 4, is applied to the solutions in the sample, so as to search the neighbourhood of each solution for better fitness individuals.

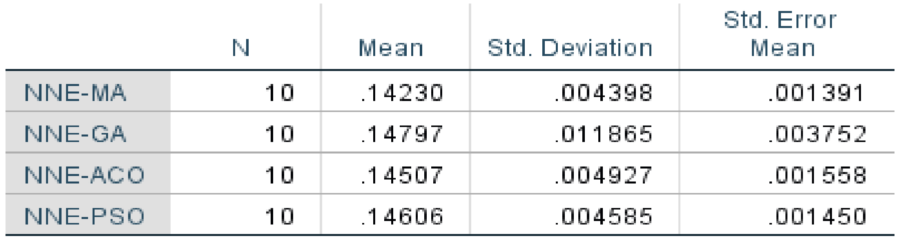
Figure 5: Error comparisons between NNE-MA and NNE with existing algorithms



Once a better solution is obtained, the current individual is replaced with the new solution and this ultimately leads to more accuracy and better quality of the final output for the neural network ensemble, which is demonstrated in Figure 5.

The statistical output in Figure 6 demonstrates a low error mean for the proposed algorithm, compared to other methods. There is also less variability in data when NNE-MA is applied, as shown by comparisons in the standard deviation. N represents the dataset sample.

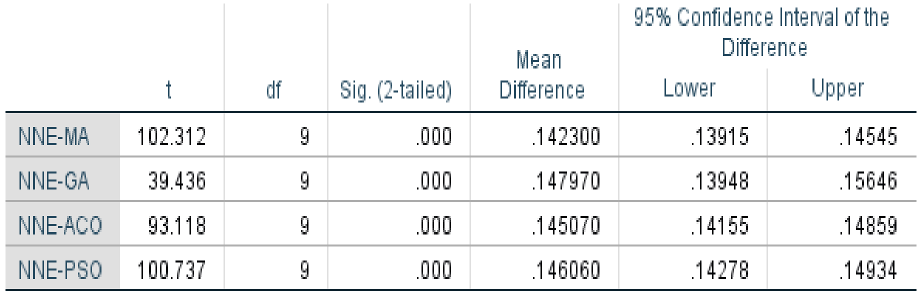
Figure 6: One-sample statistical analysis



	N	Mean	Std. Deviation	Std. Error Mean
NNE-MA	10	.14230	.004398	.001391
NNE-GA	10	.14797	.011865	.003752
NNE-ACO	10	.14507	.004927	.001558
NNE-PSO	10	.14606	.004585	.001450

The degrees of freedom, which subtract one from the valid sample and the mean ratio, are represented by df and t respectively, as shown in Figure 7. Based on the t distribution, the p-value in Sig. (2-tailed) indicates a level that is less than the 0.05 threshold value for determining the significance of the results (Shaffer, 2019). It can therefore be inferred that there exists a significant difference between experimental results generated by the algorithms in this work.

Figure 7: One-sample test analysis



					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
NNE-MA	102.312	9	.000	.142300	.13915	.14545
NNE-GA	39.436	9	.000	.147970	.13948	.15646
NNE-ACO	93.118	9	.000	.145070	.14155	.14859
NNE-PSO	100.737	9	.000	.146060	.14278	.14934

6. Conclusions

In this article, we have made the case for a neural network ensemble, based on a hybrid search mechanism, for malware detection. The approach combines global search and local search heuristics, through a memetic evolutionary search process. The tabu search algorithm is used as the local search technique, to improve the quality and fitness of solutions through scouring the neighbourhood of each solution for better individuals.

After training the model on malware datasets to learn both benign and malicious features, the proposed model is able to detect malicious software and achieve faster convergence when compared with existing techniques. In addition, a proper balance between diversification and intensification of the search is achieved, which enables the algorithm to achieve strong accuracy levels. The experimental results we have presented in this article thus indicate that combining several neural networks in an ensemble generates strong performance, especially when a memetic algorithm is applied to develop solutions and produce optimal outcomes.

Future work will include creating more algorithmic synergies to improve the ability of the search technique to converge towards high-quality solutions, which is necessary in today's rapidly changing and increasingly risk-ridden cyberspace environments.

References

Abiodun, O., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. *Heliyon, 4*(11), 1–41. https://doi.org/10.1016/j.heliyon.2018.e00938

Acarali, D., Rajarajan, M., Komninos, N., & Zarpelao, B. B. (2019). Modelling the spread of botnet malware in IoT-based wireless sensor networks. *Security and Communication Networks, 2019*, 1–13. https://doi.org/10.1155/2019/3745619

Alsulami, B., & Mancoridis, S. (2018). Behavioral malware classification using convolutional recurrent neural networks. In *13th International Conference on Malicious and Unwanted Software* (pp. 103–111). https://doi.org/10.1109/MALWARE.2018.8659358

Altaher, A., & Barukab, O. M. (2017). Intelligent hybrid approach for Android malware detection based on permissions and API calls. *International Journal of Advanced Computer Science and Applications, 8*(6), 60–67. https://doi.org/10.14569/IJACSA.2017.080608

Amjad, M. K., Butt, S. I., Kousar, R., Ahmad, R., Agha, M. H., Faping, Z., Anjum, N., & Asgher, U. (2018). Recent research trends in genetic algorithm based flexible job shop scheduling problems. *Mathematical Problems in Engineering, 2018*, 1–32. https://doi.org/10.1155/2018/9270802

Barriga, J. J., & Yoo, S. G. (2017). Malware detection and evasion with machine learning techniques: A survey. *International Journal of Applied Engineering Research, 12*(18), 7207–7214.

Bereta, M. (2019). Baldwin effect and Lamarckian evolution in a memetic algorithm for Euclidean Steiner tree problem. *Memetic Computing, 11*(1), 35–52. https://doi.org/10.1007/s12293-018-0256-7

Center for Machine Learning and Intelligent Systems (2016). Machine learning repository [Website]. University of California, Irvine. Retrieved from https://archive.ics.uci.edu/ml/datasets.php?format=&task=other&att=&area=&numAtt=&numIns=&type=&sort=nameUp&view=table

Chaimanee, A., & Supithak, W. (2018). A memetic algorithm to minimize the total sum of earliness tardiness and sequence dependent setup costs for flow shop scheduling problems with job distinct due windows. *Songklanakarin Journal of Science and Technology, 40*(5), 1203–1218. doi:10.14456/sjst-psu.2018.148

Chen, H., Su, J., & Qiao, L. (2018). Malware collusion attack against SVM: Issues and countermeasures. *Journal of Applied Sciences, 8*(10), 1–20. https://doi.org/10.3390/app8101718

Choi, J. Y., & Lee, B. (2018). Combining LSTM network ensemble via adaptive weighting for improved time series forecasting. *Mathematical Problems in Engineering*, *2018*, 1–8. https://doi.org/10.1155/2018/2470171

Dai, H., Cheng, W., & Guo, P. (2018). An improved tabu search for multi-skill resource-constrained project scheduling problems under step-deterioration. *Arabian Journal for Science and Engineering, 43*(6), 3279–3290. https://doi.org/10.1007/s13369-017-3047-4

Dash, T. (2017). A study on intrusion detection using neural networks trained with evolutionary algorithms. *Soft Computing, 21*(10), 2687–2700. https://doi.org/10.1007/s00500-015-1967-z

Eger, S., Youssef, P., & Gurevych, I. (2018). Is it time to swish? Comparing deep learning activation functions across NLP tasks. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing* (pp. 4415–4424). Association for Computational Linguistics. https://doi.org/10.18653/v1/D18-1472

Gu, Q., Li, X., & Jiang, S. (2019). Hybrid genetic grey wolf algorithm for large-scale global optimization. *Complexity, 2019*, 1–18. https://doi.org/10.1155/2019/2653512

Hassan, M., & Hamada, M. (2017). A neural networks approach for improving the accuracy of multi-criteria recommender systems. *Applied Sciences, 7*(9), 1–18. https://doi.org/10.3390/app7090868

Jat, D. S., Dhaka, P., & Limbo, A. (2018). Applications of statistical techniques and artificial neural networks: A review. *Journal of Statistics and Management Systems, 21*(4), 639–645. https://doi.org/10.1080/09720510.2018.1475073

Jerlin, A. M., & Marimuthu, K. (2018). A new malware detection system using machine learning techniques for API call sequences. *Journal of Applied Security Research, 13*(1), 45–62. https://doi.org/10.1080/19361610.2018.1387734

Ju, C., Bibaut, A., & Van der Laan, M. (2018). The relative performance of ensemble methods with deep convolutional neural networks for image classification. *Journal of Applied Statistics, 45*(15), 2800–2818. https://doi.org/10.1080/02664763.2018.1441383

Kabanga, E. K., & Kim, C. H. (2018). Malware images classification using convolutional neural network. *Journal of Computer Science and Communications, 6*(1), 153–158. https://doi.org/10.4236/jcc.2018.61016

Kalaimannan, E., John, S. K., DuBose, T., & Pinto, A. (2017). Influences on ransomware's evolution and predictions for the future challenges. *Journal of Cyber Security Technology, 1*(1), 23–31. https://doi.org/10.1080/23742917.2016.1252191

Kendrick, P., Criado, N., Hussain, A., & Randles, M. (2018). A self-organising multi-agent system for decentralised forensic investigations. *Journal of Expert Systems with Applications, 102*, 12–26. https://doi.org/10.1016/j.eswa.2018.02.023

Khammas, B. (2018). Malware detection using sub-signatures and machine learning technique. *Journal of Information Security Research, 9*(3), 96–106. https://doi.org/10.6025/jisr/2018/9/3/96-106

Khoshhalpour, E., & Shahriari, H. R. (2018). BotRevealer: Behavioral detection of botnets based on botnet life-cycle. *The ISC International Journal of Information Security, 10*(1), 55–61.

Le, H., Pham, Q., Sahoo, D., & Hoi, S. C. (2017). URLNet: Learning a URL representation with deep learning for malicious URL detection. In *Proceedings of ACM Conference* (pp. 1–13). Washington, DC. Retrieved from https://arxiv.org/pdf/1802.03162.pdf

Le, Q., Boydell, O., Namee, B. M., & Scanlon, M. (2018). Deep learning at the shallow end: Malware classification for non-domain experts. *Digital Investigation, 26*, 118–126. https://doi.org/10.1016/j.diin.2018.04.024

Lee, T., & Kwak, J. (2016). Effective and reliable malware group classification for a massive malware environment. *International Journal of Distributed Sensor Networks, 2016*, 1–6. https://doi.org/10.1155/2016/4601847

Li, H., Wang, X., & Ding, S. (2018). Research and development of neural network ensembles: A survey. *Journal of Artificial Intelligence Review, 49*(4), 455–479. https://doi.org/10.1007/s10462-016-9535-1

Liu, Z., Li, H., & Zhu, P. (2019). Diversity enhanced particle swarm optimization algorithm and its application in vehicle lightweight design. *Journal of Mechanical Science and Technology, 33*(2), 695–709. https://doi.org/10.1007/s12206-019-0124-5

Lucay, F. A., Galvez, E. D., & Cisternas, L. A. (2019). Design of flotation circuits using tabu-search algorithms: Multispecies, equipment design, and profitability parameters. *Minerals, 9*(3), 1–22. https://doi.org/10.3390/min9030181

Ma, Z., Wang, P., Gao, Z., Wang, R., & Khalighi, K. (2018). Ensemble of machine learning algorithms using the stacked generalization approach to estimate the warfarin dose. *PLoS ONE, 13*(10), 1–12. https://doi.org/10.1371/journal.pone.0205872

Mahrin, M. N., Chuprat, S., Subrarao, A., Ariffin, A. F., Talib, M. Z., Darus, M. Z., & Aziz, F. A. (2018). Malware prediction algorithm. *Journal of Theoretical and Applied Information Technology, 96*(14), 4660–4676.

Martinelli, F., Marulli, F., & Mercaldo, F. (2017). Evaluating convolutional neural network for effective mobile malware detection. *Procedia Computer Science, 112*, 2372–2381. https://doi.org/10.1016/j.procs.2017.08.216

Mohammadi, S., & Namadchian, A. (2017). A new deep learning approach for anomaly base IDS using memetic classifier. *International Journal of Computers Communications & Control, 12*(5), 677–688. https://doi.org/10.15837/ijccc.2017.5.2972

Nguyen, P. T., & Sudholt, D. (2018). Memetic algorithms beat evolutionary algorithms on the class of hurdle problems. In *Proceedings of the Genetic and Evolutionary Computation Conference* (pp. 1071–1078). Kyoto: ACM. https://doi.org/10.1145/3205455.3205456

Ojha, V. K., Abraham, A., & Snasel, V. (2017). Metaheuristic design of feedforward neural networks: A review of two decades of research. *Engineering Applications of Artificial Intelligence, 60*, 97–116. https://doi.org/10.1016/j.engappai.2017.01.013

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary memetic models for malware intrusion detection: A comparative quest for computational solution and convergence. *International Journal of Computer Applications, 179*(39), 34–43. https://doi.org/10.5120/ijca2018916586

Rad, B. B., Nejad, K. H., & Shahpasand, M. (2018). Malware classification and detection using artificial neural network. *Journal of Engineering Science and Technology, 13*, 14–23.

Razak, M. F., Anuar, N. B., Othman, F., Firdaus, A., Afifi, F., & Salleh, R. (2018). Bio-inspired for features optimization and malware detection. *Arabian Journal for Science and Engineering, 43*(12), 6963–6979. https://doi.org/10.1007/s13369-017-2951-y

Ren, B., Liu, C., Cheng, B., Guo, J., & Chen, J. (2018). MobiSentry: Towards easy and effective detection of android malware on smartphones. *Mobile Information Systems, 2018*, 1–14. https://doi.org/10.1155/2018/4317501

Rhode, M., Burnap, P., & Jones, K. (2018). Early-stage malware prediction using recurrent neural networks. *Computer Security, 77*, 578–594. https://doi.org/10.1016/j.cose.2018.05.010

Schweidtmann, A., & Mitsos, A. (2019). Deterministic global optimization with artificial neural networks embedded. *Journal of Optimization Theory and Applications, 180*(3), 925–948. https://doi.org/10.1007/s10957-018-1396-0

Selvaganapathy, S., Nivaashini, M., & Natarajan, H. (2018). Deep belief network based detection and categorization of malicious URLs. *Information Security Journal: A Global Perspective, 27*(3), 145–161. https://doi.org/10.1080/19393555.2018.1456577

Shaffer, L. K. (2019). Before p < 0.05 to beyond p < 0.05: Using history to contextualize p-values and significance testing. *The American Statistician, 73*(1), 82–90. https://doi.org/10.1080/00031305.2018.1537891

Shah, A. A., Ehsan, K. M., Ishaq, K., Ali, Z., & Farooq, M. S. (2018). An efficient hybrid classifier model for anomaly intrusion detection system. *International Journal of Computer Science and Network Security*, *18*(11), 127–136.

Shapshak, P. (2018). Artificial intelligence and brain. *Bioinformation, 14*(1), 38–41. https://doi.org/10.6026/97320630014038

Sheng, W., Shan, P., Mao, J., Zheng, Y., Chen, S., & Wang, Z. (2017). An adaptive memetic algorithm with rank-based mutation for artificial neural network architecture optimization. *IEEE Access, 5*, 18895–18907. https://doi.org/10.1109/ACCESS.2017.2752901

Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. *Journal of Human-centric Computing and Information Sciences, 8*(3), 1–22. https://doi.org/10.1186/s13673-018-0125-x

Wang, Z., Liu, C., Qiu, J., Tian, Z., Cui, X., & Su, S. (2018). Automatically traceback RDP-based targeted ransomware attacks. *Wireless Communications and Mobile Computing, 2018,* 1–13. https://doi.org/10.1155/2018/7943586

World Economic Forum (WEF). (2018). *The global risks report 2018.* Geneva. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Xiao, F., Lin, Z., Sun, Y., & Ma, Y. (2019). Malware detection based on deep learning of behavior graphs. *Mathematical Problem in Engineering, 2019*, 1–10. https://doi.org/10.1155/2019/8195395

Xu, H., Pu, P., & Duan, F. (2018). Dynamic vehicle routing problems with enhanced ant colony optimization. *Discrete Dynamics in Nature and Society, 2018,* 1–13. https://doi.org/10.1155/2018/1295485

Xu, Y., Wu, C., Zheng, K., Wang, X., Niu, X., & Lu, T. (2017). Computing adaptive feature weights with PSO to improve Android malware detection. *Security and Communication Networks*, *2017*, 1–14. https://doi.org/10.1155/2017/3284080

Xue, Y., Jia, W., Zhao, X., & Pang, W. (2018). An evolutionary computation based feature selection method for intrusion detection. *Security and Communication Networks*, *2018,* 1–10. https://doi.org/10.1155/2018/2492956

Yan, J., Qi, Y., & Rao, Q. (2018). Detecting malware with an ensemble method based on deep neural network. *Security and Communication Networks, 2018,* 1–16. https://doi.org/10.1155/2018/7247095

Yin, W., Zhou, H., Wang, M., Jin, Z., & Xu, J. (2018). A dynamic malware detection mechanism based on deep learning. *International Journal of Computer Science and Network Security, 18*(7), 96–102.

Zarras, B. K., Webster, G. D., & Eckert, C. M. (2016). Deep learning for classification of malware system call sequences. In *Australasian conference on artificial intelligence* (pp. 137–149). Wellington, New Zealand: Springer. https://doi.org/10.1007/978-3-319-50127-7_11

Zhirou, Y., & Jing, L. (2018). A memetic algorithm for determining the nodal attacks with minimum cost on complex networks. *Physica A: Statistical Mechanics and its Applications, 503*, 1041–1053. https://doi.org/10.1016/j.physa.2018.08.132

Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC)

Morné Pretorius
Snr. Embedded Security Researcher, Modelling and Digital Science, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0002-7665-4778

Hombakazi Ngejane
Security Researcher, Modelling and Digital Science, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0003-0376-9176

Abstract

The South African Government's National Cybersecurity Policy Framework (NCPF) of 2012 provides for the establishment of a national computer security incident response team (CSIRT) in the form of the National Cybersecurity Hub—more correctly referred to as an information security incident management capability (ISIMC). Among other things, the National Cybersecurity Hub is mandated to serve as a high-level national ISIMC that works in collaboration with sector ISIMCs to improve South Africa's critical infrastructure security. In this article, we identify standards, policies, procedures and best practices regarding the establishment of ISIMCs, and we provide recommendations for South Africa's deployment of an ISIMC collaboration network.

Keywords
cybersecurity, information security, cyber threats, CSIRT, national ISIMC, confidentiality, integrity, availability, standards, intrusion, protection, detection, incident management, incident handling, incident response

DOI: https://doi.org/10.23962/10539/28656

Recommended citation

Pretorius, M., & Ngejane, H. (2019). Best practices for establishment of a national information security incident management capability (ISIMC). *The African Journal of Information and Communication (AJIC)*, 24, 1-20.
https://doi.org/10.23962/10539/28656

1. Introduction

Today's computer networks involve many entities and components, and not all of them are held liable when security breaches occur. During an attack, there is the owner of the network who has to defend it, there is the company who sold the network owner (one or multiple) potentially vulnerable network defence solutions, there is the attacker who exploits the said vulnerability, and there is the person who wrote the tool used by the attacker. Today, 100% of the cost of an attack falls on the network owner, and this situation needs to change (Schneier, 2000). Accordingly, the South African Cybercrimes and Cybersecurity Bill (Department of Justice and Constitutional Development, 2016) attempts to enforce and spread liability across participants. Pressure to enter the market rapidly leads many entities to invest only minimally in security, and to release, for example, network security solutions, which sometimes fail and cause attacks, with no-liability legal agreements. With so many problematic systems in existence, the cybersecurity sector has had to evolve from a focus on protection/prevention through firewalls in the 1990s, to a focus on detection via monitoring tools in the early 2000s, to the current era's focus on response (Schneier, 2014). This has led to the establishment of the following modalities and entities that function as networked teams to detect and respond to cyber attacks and serve a constituency or client:

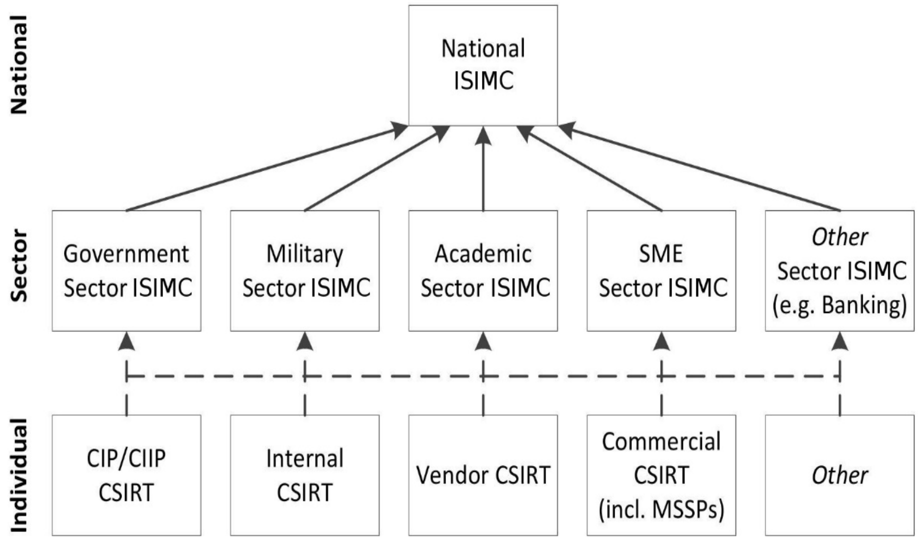
- a security operations centre (SOC)
- a cybersecurity operations centre (CSOC)
- an incident handling team (IHT)
- an incident response centre or incident response capability (IRC)
- an incident response team (IRT)
- a security incident response team (SIRT)
- a security emergency response team (SERT)
- a computer emergency response team (CERT)
- a computer incident response capability or centre (CIRC)
- a computer incident response team (CIRT)
- a computer security incident response capability or centre (CSIRC)
- a computer security incident response team (CSIRT)
- an information security incident management capability (ISIMC).

The term "team" in the above acronyms has been found to be restrictive (Alberts, Dorofee, Killcrece, Ruefle & Zajicek, 2004), due to variation across organisations regarding location, structure, responsibilities and services offered to one or multiple constituencies. We also view the term "response" to be restrictive, because some national or sector-level CSIRTs do not necessarily respond to incidents and might merely coordinate other entities; some CSIRTs can end up serving each other, in which case they also become a constituency; and some CSIRTs can also serve other CSIRTs or constituencies across other sectors.

We prefer and adopt the more appropriate ISIMC acronym (see, for example, Stikvoort, 2010; and Haller, Merrell, Butkovic & Willke, 2011), which refers to national or sector-based teams where national ISIMCs should ideally be responsible for aiding the establishment of other lower-level capabilities or CSIRTs (see Figure 1). An ISIMC provides services and support to a constituency or client by preventing, detecting and responding to information security incidents. It also undertakes partial liability by endeavouring to protect critical assets and separating security services from network infrastructure owners/providers.

Figure 1 does not represent the physical reality and is conceptual at best. Due to variation across the different kinds of possible ISIMC implementations, assumptions cannot be made regarding the physical locations and relationships within Figure 1. An ISIMC is not necessarily a building with people in it, and neither is the constituency or client being served necessarily based in a physical entity. An ISIMC is simply a group of people, regardless of location, who have the capability to provide better visibility, incident response, and other services (e.g., alerts), to another group of people known as the constituency or client. The constituency, in this context, can be broadly defined as "the group of users, sites, networks or organisations served by the team" (Brownlee & Guttman, 1998, p. 17).

Figure 1: Example of typical network of ISIMCs



Source: Adapted from Mooi and Botha (2015, p. 4)

Note: This figure is an abstraction and does not seek to represent physical relationships.

The concept of an ISIMC traces its roots back to the late 1980s, with Carnegie Mellon University in the US serving as a pioneer (ENISA, 2006). ISIMCs consistently face challenges due to the always expanding landscape of network security. They require a wide spectrum of tools—e.g., intrusion detection systems (IDS), security information and event management (SIEM) software, digital forensics kits—with no single tool covering the entire spectrum of requirements. These tools need to be combined with people and processes, which is challenging without proper guidelines or standards.

In the context of the challenges involved in ISIMC establishment, in this article we identify and discuss available standards, policies, procedures and best practices regarding the establishment and operation of national and sector-based ISIMCs. We aim to be largely generic, and we do not seek to be exhaustive.

2. Information security

Incident management and response alone will not provide adequate or 100% information security. An information security system must continually adapt and learn, via periodic assessment, where three requirements should be addressed (Schneier, 2014):

- *protection*: mostly covered by technology with assistance from people and process;
- *detection*: needs equal amounts of people, process, and technology (33% each); and
- *response*: mostly addressed by people with assistance from process and technology.

Protection, detection and response are enhanced by confidentiality, integrity and availability (CIA), i.e., the information security system must:

- protect information's confidentiality and integrity by preventing unauthorised access, using cryptography and access control;
- detect a change in information's integrity by verifying that it is not modified by unauthorised entities while in transit or at rest; and
- respond to an attack against information or service integrity and availability by blocking or banning unauthorised access and/or restoring the system.

Also, confidentiality increases integrity by preventing unauthorised interception and tampering, which in turn increases availability. Importantly, these requirements apply to all parties involved in ISIMC collaboration networks since the chain is only as strong as its weakest link—with attackers exploiting weaker entities to gain access to others. Mechanisms that can be deployed to implement CIA are as listed below, and it is important for all people who build any information system (e.g., website, database, desktop computer workstation) to identify where CIA fits into the design.

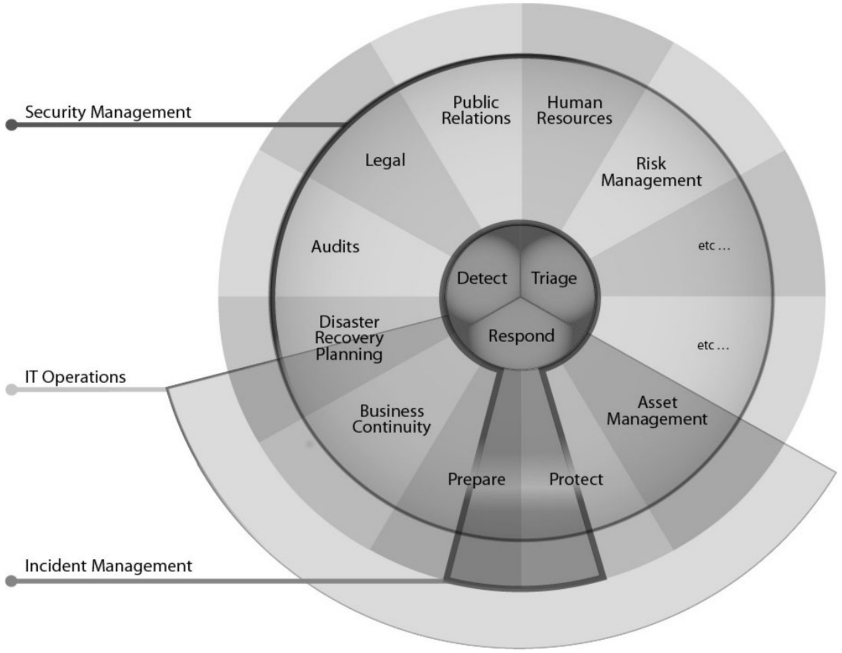
- *confidentiality*: access-control-lists (ACLs), file permissions, usernames, passwords, encryption, encryption key management, safes, gates, doors, locks, keys, access cards, biometrics;
- *integrity*: change management, version control, cryptographic hash functions, digital signatures; and
- *availability*: high availability clusters, fail-over redundancy systems such as disaster recovery backups and image-based network boot systems.

Incident management, handling and response

It is important to distinguish between *events* and *incidents* (Alberts et al., 2004; Brownlee & Guttman, 1998; Shirey, 2000). According to (Shirey, 2000, pp. 150–151), an *event* is "an occurrence in a system that is relevant to the security of the system", while an *incident* is "any adverse event which compromises some aspect of computer or network security". There can be many events in systems that track human actions on a network, but only events that compromise CIA can be classified as incidents.

Figure 2 (from Alberts et al., 2004) shows how incident management forms a sub-component of security management. Incident management establishes and maintains capabilities such as patch management, configuration management, and security policies. These capabilities are utilised (not established) by incident management to accomplish its goals.

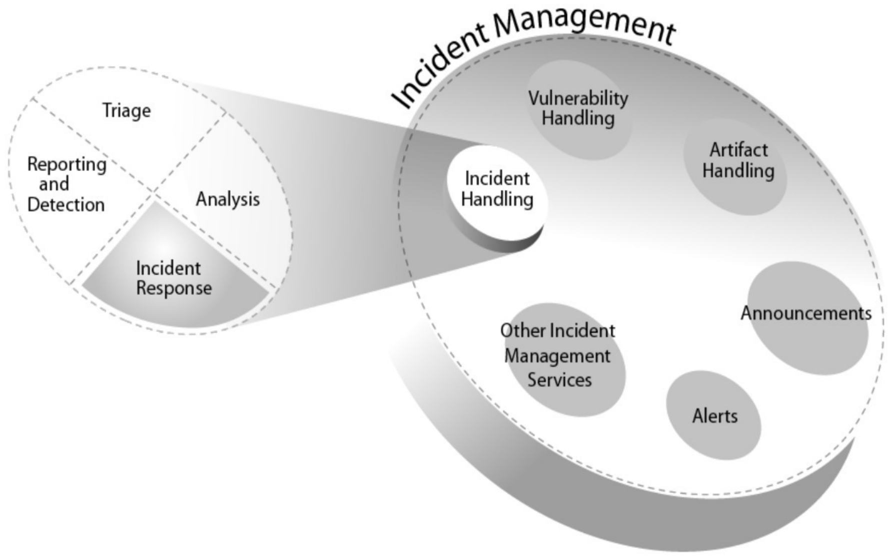
Figure 2: Incident management as a sub-component of security management



Source: Alberts et al. (2004. p. 26)

Figure 3 (also from Alberts et al., 2004) further expands incident management into two core sub-components: the service known as incident handling, and the function within incident handling known as incident response.

Figure 3: Incident handling and response as sub-components of incident management



Source: Alberts et al. (2004. p. 4)

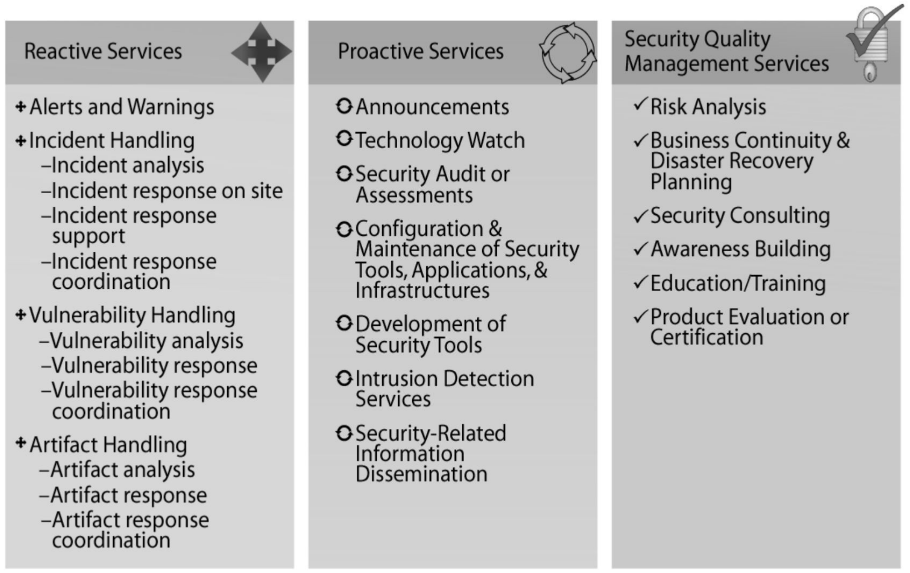
According to the SysAdmin, Audit, Network and Security (SANS) Internet Storm Centre (ISC) (De Beaupré, 2009):

- *incident management* combines the core service—incident handling—with additional services present at higher-level ISIMCs, and is proactive and reactive;
- *incident handling* relates to the communications, coordination, logistics, planning and escalation activity required for resolving an incident calmly and efficiently; and
- *incident response* relates to any lower-level technical activity that is required to contain and analyse an incident.

The core service—incident handling, and its sub-function, incident response—can be done by the same person/team, but it is better to have each done by a separate person/team, to reduce the time spent inside the handling process. It should also be noted that handling and response have different skill requirements: incident handling requires strong communication and project management skills, while incident response requires strong technical networking, log analysis and forensics.

Key incident management service definitions are shown in Figure 4 (again taken from Alberts et al., 2004).

Figure 4: Incident management services



Reactive Services

- + Alerts and Warnings
- + Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- + Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- + Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

- ○ Announcements
- ○ Technology Watch
- ○ Security Audit or Assessments
- ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ○ Development of Security Tools
- ○ Intrusion Detection Services
- ○ Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Source: Alberts et al. (2004, p. 4)

A national or sector ISIMC should aspire to providing as many of the services shown in Figure 4 as possible. However, it is best to start small, and master the core service offerings while designing the organisational structures for future services. Typical national and sector ISIMC services include, according to Haller et al. (2011):

- incident handling services;
- incident analysis;
- forensic services;
- network monitoring services;
- malicious code analysis;
- vulnerability assessments;
- research services;
- training, education, and awareness; and
- coordination of responses

3. Methods

We conducted initial searches to identify relevant synonyms that describe incident management and response entities. We then constructed multiple search queries by combining the identified ISIMC synonyms into search combinations using "OR" and "AND". Among the keywords used in the searches were: best practice, good practice, standards, accreditation, certification, bodies, and body.

Due to the multidisciplinary nature of information security, we constructed additional non-information security searches relevant to ISIMC establishment, using terms connected to organisational design, tool selection, effectiveness, performance measurement, and human behavior during incident response.

We issued the search queries across IEEE Xplore, Scopus, Science Direct, Google Scholar and Google Search, and filtered the returned sources according to their title, abstract/summary and conclusion relevance. We traversed the citations forwards and backwards to identify subsets of literature, and also filtered these subsets according to relevance.

We also interviewed representatives at two South African sector ISIMCs, namely the South African National Research Network (SANReN) and the South African Banking Risk Information Centre (SABRIC), in order to determine their tooling, processes, standards and practices, and also to determine whether they experienced similar challenges to those outlined in our identified literature.

4. Incident management standards

Maturity standards

Maturity standards aim to build trust so that an international network of trusted ISIMCs can be linked together once maturity is achieved. ISIMC maturity standards also help emerging ISIMCs to measure and increase maturity by offering best practices for governance, organisation and operations. The key maturity standards listed by the Trusted Introducer (TI) accreditation and certification body are the following:

- *Security incident management maturity model (SIM3)* (Stikvoort, 2010): provides 44 high-level parameters/requirements that measure efficient ISIMC operations and help teams to think about problems typically faced when establishing ISIMCs;
- *RFC2350 Appendix D* (Brownlee & Guttman, 1998): fill-out form template that is completed by ISIMCs, requiring them to state their services, whom they serve, and how they can be contacted (compulsory for TI certification since May 2009);
- *TI CSIRT Code of Practice (CCoP)* (Cormack, Kossakowski, Maj, Parker & Stikvoort, 2017): provides good practice guidance regarding ethics for ISIMCs and prescribes interactions between ISIMCs and their constituents;
- *eCIRT.net Incident Taxonomy* (Stikvoort et al., 2015): supersedes the older taxonomy classification by Arvidsson, Cormack, Demchenko and Meijer (2001) and defines incident taxonomy via 11 main classifications (with sub-classifications) and guides teams towards configuration of information sharing- and ticket/issue-tracking systems; and
- *Traffic light protocol (TLP)*: A Forum for Internet Response and Security Teams (FIRST) protocol that provides an intuitive schema for indicating when and how sensitive information is shared, facilitating effective collaboration (FIRST, 2016). E-mail subjects and document headers/footers must be labelled as follows when shared between entities:
  - TLP:RED = not for disclosure, restricted to participants only;
  - TLP:AMBER = limited disclosure, restricted to participants' organisations;
  - TLP:GREEN = limited disclosure, restricted to the community; and
  - TLP:WHITE = disclosure is not limited.

These documents constitute certification measurement, whereby accreditation needs to be achieved followed by certification. Once maturity is reached, certified teams remain within the TI-accredited community for three years, after which they need to recertify and prove maintained or improved quality. Certification can take three to 12 months. As of May 2019—from an international total of 385 TI-associated teams—163 had been accredited, one was an accreditation candidate, two had had their accreditation suspended, 15 had been certified, 10 were re-certification candidates, seven were certification candidates, 11 were re-listing/re-registration candidates, 42 were being re-listed, three were listing candidates, and 131 were listed (Trusted Introducer, n.d).

Process and procedure standards

The International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) 27035 (ISO, 2016) and National Institute of Standards and Technology Special Publication (NIST- SP) 800-61 (Cichonski, Millar, Grance & Scarfone, 2012) international standards provide guidance on incident management for large and medium-sized organisations. Smaller organisations can use basic sets of documents, processes and routines described in ISO/IEC 27035 and NIST-SP 800-61, depending on size, business type and risk. ISO/IEC 27035 is composed of three separate documents:

- Part 1: Principles of incident management (ISO/IEC 27035-1-2016) describes this general process:
  - *Plan and prepare*: establish an information security incident management policy, form an incident response team, source funding, get senior management commitment, establish services to be provided, select and configure tooling to be used, establish software quality plan, testing plan, maintenance plan, establish staff rotation and training plan, document all processes;
  - *Detection and reporting*: observe and report events that might escalate into incidents;

  - ○ *Assessment and decision*: assess the situation to determine whether it is in fact an incident;
  - ○ *Responses*: contain, eradicate, recover from and investigate incidents, where appropriate; and
  - ○ *Lessons learned*: make improvements where required as per incidents experienced.
- Part 2: Guidelines to plan and prepare for incident response (ISO/IEC 27035-2-2016)
- Part 3: Guidelines for incident response operations (ISO/IEC 27035-3-2016).

Similar to ISO/IEC 27035, NIST-SP 800-61, entitled Computer Security Incident Handling Guide, seeks to assist organisations with incident risk mitigation by providing guidelines for efficient incident response, management process establishment, and information-sharing. NIST-SP 800-61 groups incident response management into four phases:

- *Preparation*: establish and train an incident response team and acquire necessary tools and resources;
- *Detection and analysis*: implement step-by-step instructions and strategies for handling every incident type, its documentation, its analysis and its reporting;
- *Containment, eradication, and recovery*: choose containment strategies, gather and handle evidence, identify attacker hosts, eradicate and recover; and
- *Post-incident activity*: learn from collected incident data and retained evidence.

5. ISIMC challenges and requirements

Establishing a countrywide nodal-point ISIMC network should ideally happen in a top-down fashion, beginning with the national ISIMC, followed by sector-based and lower-level ISIMCs (Figure 1), to ensure methodology consensus and efficient interaction. This is seldom the case, however, as bottom-up approaches usually play out in practice because of cybersecurity staff scarcity and lack of public awareness. It is therefore common to find lower-level ISIMCs established first, followed by coordination efforts from high-level national ISIMCs. Problems then occur when higher-level ISIMCs attempt to join existing entities, resulting in requirement changes that require multi-directional collaboration.

There also tend to be insufficient security considerations (i.e., CIA considerations) by most organisations, which means that in addition to implementing cybersecurity correctly and keeping incident information confidential, ISIMCs are also faced with the task of making people collaborate in teams by optimising processes that cover multiple types of attacks. Also, no widely adopted standard for sharing actionable incident information between ISIMC teams exists (Bourgue, Budd, Homola, Wlasenko & Kulawik, 2013). ISIMC teams find themselves in classical military observe-orient-decide-act (OODA) loops where people assume tools or technologies will save them when in fact there is a shortage of tools that maximise human capability in the loop. Incident management and response require human intelligence, and the security industry is not used to this (Schneier, 2014).

Moving past fundamental security requirements, the problem is one of defining a process similar to OODA that conforms to ISO/IEC 27035 or NIST-SP 800-61 and that synchronises available capabilities so as to produce conducive outcomes during attacks. ISIMCs need to be able to share threat and attack information with other ISIMCs and constituents, securely and confidentially, where information structures should be standardised and with duplication avoided to alleviate the alert fatigue often experienced (Van der Kleij, Kleinhuis & Young, 2017). False-positive elimination and attack escalation are challenging and cause the most fatigue (Van der Kleij et al., 2017) and, if automated, teams can maximise efficiency.

Also, ISIMCs need to pursue and measure effectiveness, since time is scarce during attacks. Surveys show that teams tend to be unaware of effectiveness levels because measurement is neglected in ISIMC communities (Van der Kleij et al., 2017), a phenomenon attributable to a lack of goal definitions against which to measure. As noted by Mooi and Botha (2015), additional challenges faced when establishing ISIMCs are:

- unclear mandate or mission;
- lack of management support;
- finding investments;
- selecting a revenue model; and
- interacting with, and coordinating, external or constituency parties.

There are a multitude of ISIMC requirements, and they vary according to the particular ISIMC. In our analysis, the best model to follow for ISIMC requirements is the aforementioned SIM3 model proposed by Stikvoort (2010), which sets out four categories:

- organisational requirements;
- human requirements;
- process requirements; and
- tool requirements.

Organisational requirements

It is sometimes assumed that agile structures can be adopted at scale, forgetting that bringing in more people introduces collaboration complexity. Human capacity to collaborate is by no means infinite, as expressed by what has come to be known as "Dunbar's number": the argument that an individual's capacity to meaningfully collaborate cannot go beyond approximately 150 individuals (Dunbar, 1992; Wang, Gao, Zhou, Hu & Tian, 2016). No matter which organisational structures are adopted, Dunbar's number should not be exceeded per department. With respect to funding, selling information security is difficult, because there is a tendency to avoid losses by choosing uncertain risk (i.e., via insufficient information security expenditure) over certain loss (i.e., sufficient information security expenditure). Many executives take the risk and gamble on the prospect that a breach will not occur. It is thus crucially important to communicate the importance of information security to all stakeholders.

Human requirements

Response is mostly human-centric and cannot be fully automated, so technology should not replace humans. Technology should, rather, automate as many repetitive tasks as possible, so as to maximise human capability and efficiency inside the response loop (Schneier, 2014). A generally accepted software development philosophy in this context is the "don't repeat yourself (DRY)" principle (e.g., write log parser engines that generate incident tickets from logs, instead of humans generating tickets manually).

Process requirements

Both the ISO/IEC and NIST-SP standards outlined above suggest protection, detection and response as core incident management processes, with *preparation* and *learning* as the beginning and end processes, respectively (where a process is covered by both standards, it is up to the ISIMC implementer to choose one of the two standards for the particular process—either ISO/IEC or NIST-SP—and adhere to it):

- *Prepare*: Establish an ISIMC (requirements elicitation, information gathering, premises, documentation, hardware, software, staff etc.) and implement protection mechanisms discussed in section 2 to alleviate response workload.
- *Detect and analyse*: Continually monitor and analyse physical, digital and network systems, including their performance, from multiple sources (anti-virus software, logs, human feedback). Collected information is classified, prioritised, filtered and internet correlated to maximise context/visibility. Malicious events are escalated into incident software tickets/issues. In OODA terms, this represents "observe" and "orient".
- *Decide*: This step is difficult and can include containment sub-steps necessary to buy decision-making time for eradication and recovery. Depending on severity, incident tickets are escalated to executives or passed on to responders. A historical database is maintained to facilitate the "learn" phase.
- *Respond or act*: Action is taken depending on the type of incident, whereby staff with the corresponding skills resolve and/or recover affected systems and update the incident's status. If it is a typical incident, its status is updated to reflect resolution. If the type of incident has not been encountered before, it is also passed on to the "*learn*" phase.

- *Learn*: New incident types are analysed as a post-incident resolution activity, in order to feed back into the "*prepare*" phase to determine trends and protect against emerging attacks. This learn phase potentially triggers risk re-assessments and adjustments to systems and procedures. This is followed by a return to the "*prepare*" phase.

Tool requirements

A problem with information security tools is that there are too many of them to allow for easy comparison and selection, and they are scattered across the requirements spectrum. There are tools for prevention, detection, response, visualisation and collaboration, and tools that facilitate combinations of these, but there are few that scale easily (Bourgue et al., 2013). Having many tools introduces problems of configuration maintenance, whereas one comprehensive tool can introduce a single point of failure and possibly impair scalability (Bourgue et al., 2013). It is therefore a challenge to select tools that adhere to standards—and that, at the same time, are easy to use, configure and scale—while providing appropriate SIM3 maturity.

6. Recommendations

In line with the ISIMC requirements set out in the aforementioned SIM3 model (Stikvoort, 2010), we now set out some initial recommendations for establishment of a national or sector ISIMC that could integrate into a larger national or international network of ISIMCs since it is focused on achieving standardisation. This design is generic in the sense that it can be adapted easily to achieve many possible collaboration hierarchies in addition to the one depicted above in Figure 1. For illustrative purposes, we set out the recommendations in alignment with the depiction in Figure 1.

Organisational structure

In the potential collaboration hierarchy depicted in Figure 1, the ISIMC network (points-of-contact) design needs to establish a national ISIMC that coordinates and collaborates with sector ISIMCs, with the national and sector ISIMCs sharing threat intel with each other in order to build attack awareness and improve critical system/infrastructure security. It is assumed that requirements will be canvassed and a standardised set of computer systems and software adopted in order to reduce workload regarding detection automation, and to reduce development costs. Standardised interactions between nodal points reduce uncertainty, which in turn aids automation and improves mean time to repair/response/resolution (MTTR). Another assumption is that all the ISIMCs agree to use easily integrable tools that facilitate incident management (see Figure 3) and interaction between ISIMCs and their constituents.

With those assumptions laid down, we now present a structure that could facilitate the network depicted in Figure 1. The aim is to design a baseline that could be expanded to eventually provide all the services outlined in Figure 4, if practical.

Concretely put, the mandate is for each nodal point to share incident intelligence with other nodal points participating in the network, and to collaborate on computer security incident response and provide alerts and warnings to the public and other nodal points.

A widely adopted initial document used in the ISIMC community, as referred to above, is the RFC2350 Appendix D (Brownlee & Guttman, 1998). Since Confluence (Atlassian, n.d.-a) (see "Tools" sub-section below) makes use of web spaces/pages that can be templated, each team in the network will create a web space from a RFC2350 Appendix D template and document team information within Confluence.

Another constituency-space template will be created to interface with the serving ISIMC, providing easy access to contact details. Each constituent's space/page will link to and display all their incident and alert data, services utilised, communication methods, minimum reaction time, elasticsearch logstash kibana (ELK) index/database number (see "Tools" sub-section below), and authorised team actions—and constituent network layout if they agree to provide one. Roles and permissions (ACLs) will be configured to allow only constituency and responding team access to the constituency space/page. All page information will be searchable within Confluence, which will reduce MTTR as all data can be easily located by responders during incidents.

As represented in Figure 1, this ISIMC network resembles a campus model, where a national nodal point acts as the leader and develops and shares auto-detection software modules with other constituents and/or sector ISIMCs. These detector modules will be configured at the constituencies' premises (if they agree) to feed the ELK stack (Cyphon's backend—see "Tools" sub-section below) with necessary information and to assign an ELK index/database per constituency. Detector modules will be configured with read-only permissions through the constituency computer systems' user and group ACLs.

Each ISIMC will be split into detection and response offices, in the same building. If co-location is not possible, the two offices should still be able to collaborate via Jira (Atlassian, n.d-b), when improving detector modules, as per responder team feedback. All premises will be access-controlled and a Cyphon (Dunbar Security, n.d.) auto-detection module will be written to be triggered by unauthorised access incidents. The decision whether to decentralise Cyphon's hosting per constituent, or to centralise hosting in one location, can be dependent on requirements and the people implementing the capability—provided that all secrets (e.g., database credentials, external application programming interface (API) keys, and credentials for service-oriented communication) are managed with a tool such as Vault.

Since this design aims for maturity at inception by adopting SIM3 requirements, introduction into a worldwide trusted CSIRT or ISIMC network should be possible after being audited by accreditation and certification bodies.

Human elements

During preparation, it is not necessary to be fully staffed, and thus it will probably be best to start with minimal personnel to lay the groundwork. As our recommendation is to automate detection, it will be necessary to hire security-conscious software developers, and initially two software developers will be needed with some experience in the following:

- network security;
- operating system security;
- penetration testing;
- web and database development security;
- software development; and
- quality management.

Since the Python programming language, Django web framework and ELK stack are underlying technologies behind Cyphon (see "Tools" sub-section below), the developers will require experience in them. One developer can research detection strategies while the other implements and tests the detection modules. They can also alternate between research and development, to avoid boredom and to maximise staff retention. For tool configuration and maintenance, at least one employee will be required with skills and experience specific to:

- ELK stack (Cyphon-specific context would be advantageous); and
- collaboration through Confluence and Jira, and their configuration and maintenance.

Incident responder staff are also required. These individuals need technical experience, strong analytical ability, and good writing and verbal skills. Staff requirements depend on whether the constituency provides a critical web service or merely a web-independent product. For example, if the constituency served by the ISIMC requires a continually available web service, then 24/7 incident responder staff rotation is important. But if the constituency builds a hardware product that does not use web services, normal operating hours will be sufficient as only their office systems will require monitoring.

In the example we are contemplating, 24-hour, 7-days-a-week incident response is required, and a staff availability/rotation policy is documented using Confluence. Staff members who work on detection software occupy normal full-time employee schedules, whereas incident responder staff will divide hours between them to ensure 24/7 availability. This will initially be minimally accomplished by four responder staff members: two manning the war room by day and two at night. On public holidays, one responder will be on call, via virtual private network (VPN) access to the constituency's network and the war room's incident visualisation dashboard.

Staff retention will be boosted through automation, which alleviates the workload often placed on incident responders. A human resources team will periodically survey responders and detection developers to ensure staff retention, and Confluence's maintainer will enrol and train human resources staff in creation of the survey task tickets that guide the process.

All staff will be trained in Confluence and Jira, since this is where all documentation, staff/constituency details, and workflows (ticket types) reside. The CCoP (Cormack et al., 2017) and TLP (FIRST, 2016) standards will be documented within Confluence and included as staff training. Staff will also be notified, during induction, that they should avoid e-mail or telephone communication, and should rather use Slack, which is encrypted (see "Tools" sub-section below). All staff must study the policies and procedures to which they are granted access on Confluence.

Processes

The ISO/IEC 27035 standard details event-to-incident escalation by either human or automated means. Our recommendation is an *automated* process, via modular software units that connect to Cyphon. This transfers the detection, analysis and triage responsibility to staff members who continually research attacks and implement attack detection in software, thus simplifying the handling process while using Confluence to document all processes and actions. Response staff will meet regularly with detection developers to share ideas on improvements and standardisation.

The response process will vary per incident type definition (Stikvoort et al., 2015), and will be documented alongside escalation procedures according to chains of command within the constituency's organisation. High-risk areas and assets are identified and documented using threat models so that detection developers correctly triage events to be displayed to responders within Cyphon. This prevents confusion when escalating high-risk incidents to executive levels. The escalation policy will list at least two contacts (e.g., manager plus executive), in case one of the contacts is unavailable.

Incident escalation will flow from Cyphon to Jira, which automatically links to the constituent's Confluence webspace. Users report incidents by registering them directly through the constituent's web space using task items that require critical information population into customisable ticket fields. A Jira support ticket is then created by ISIMC staff. The protection policy specifies CIA mechanisms/tools regarding assets (e.g., servers, war room, employee computers) and lists associated risk levels. The constituency is enrolled on Confluence and notified through Confluence and Slack chat/voice encrypted channels, as per escalation policy, when high-risk incidents occur. By configuring access rights per ticket type or priority, Confluence's ACLs prevent unauthorised staff from viewing and responding to confidential incidents. The same ACL mechanism can be used to protect confidential documentation that resides on the same system. All incident statistics will be extracted from the Jira ticket database and directed towards the constituency's Confluence page, and constituency support requests will be initiated through the same information page. Communications with ISIMCs outside of Confluence and the national nodal-point network will flow through encrypted e-mail.

The ISIMC response office will define response processes per incident type using customisable ticket workflows that ensure process enforcement. Information required by incident types will be communicated to the detection office, ensuring correct ticket construction. The detection office will provide monthly feedback to protection staff, to potentially harden protection mechanisms. Finally, a fallback/resiliency policy will be specified to detail how tools are backed up and redundantly deployed, to ensure availability in case they fail.

Tools

Many existing systems can address the above-mentioned high-level requirements, but one needs to select tools with the maximum requirements coverage. Below is a list of commonly used issue tracking/ticketing and SIEM-type systems that could facilitate incident management:

- Request Tracker for Incident Response (RTIR)
- Demisto community edition
- Open Technology Real Services (OTRS)
- Fast Incident Response (FIR)
- iTop
- Cyphon
- Redmine
- osTicket
- TheHive
- Vtenext community edition
- Sandia Cyber Omnia Tracker (SCOT)

The selected tools should be able to define custom tickets/workflows, due to varying department tasks and varying attack resolution processes. Mechanisms that aggregate events from multiple sources (e.g., from endpoint agents, network traffic, anti-virus logs, firewall logs, threat intel feeds, social media, e-mail attachments and logs, user reported input, vulnerability scan logs, internet of things (IoT) events) must also be available. Tools that automatically classify, triage, and filter false positives through developer-defined rules and create incident tickets, to improve MTTR, are also needed. These tools should also be able to allow read-only access to internal or external ISIMCs or other external entities, since established services could be provided to other ISIMCs or organisations in the future.

In summary, the selected tools need to be scalable, configurable, and able to absorb changing requirements. Fortunately, there are appropriate tools available, and one such tool that we have identified is Cyphon, by Dunbar Security. Cyphon deals with the lower-level detection and response tasks and has the ability to create incident issues/tickets inside higher-level collaboration tools such as Jira and Confluence, both developed by Atlassian. By combining Confluence, Jira and Cyphon, much of the lower-level detection automation and orchestration can be addressed, along with higher-level collaboration required by non-technical staff and the served constituency. Cyphon utilises the ELK stack (Elastic, n.d), which is flexible and scalable, provided that dedicated staff attend to its configuration and maintenance.

The CIA of the tools' information needs to be ensured during deployment, and their hosting can be outsourced to security-conscious cloud services. Confluence facilitates listing and searching all staff, assets, policies and supporting documentation, whereas Cyphon provides constituency network monitoring and visibility. Cyphon can integrate many existing tools, such as Splunk and even security camera events e.g., office movement when staff members are on leave. Confluence can interface with constituencies by creating publicly accessible web spaces/pages, where alerts, announcements, and technology watch information (Figure 4) can be published without manual web development, reducing the need for email. Team communications via Slack chat can be integrated into Confluence, provided all staff have screen authentication/lock activated on their mobiles (as documented in an acceptable use policy).

References

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs: A work in progress*. Report Number CMU/SEI-2004-TR-015. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. https://doi.org/10.21236/ADA453378

Arvidsson, J., Cormack, A., Demchenko, Y., & Meijer, J. (2001). *Terena's incident object description and exchange format requirements*. RFC No. 3067. RFC Editor. https://doi.org/10.17487/rfc3067

Atlassian. (n.d.-a). Confluence is an open and shared workspace. Retrieved from https://www.atlassian.com/ software/confluence

Atlassian. (n.d.-b). Jira: The #1 software development tool used by agile teams. Retrieved from https://www. atlassian.com/software/jira

Bourgue, R., Budd, J., Homola, J., Wlasenko, M., & Kulawik, D. (2013). *Detect, SHARE, protect: Solutions for improving threat data exchange among CERTs*. European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

Brownlee, N., & Guttman, E. (1998). *Expectations for computer security incident response*. BCP No. 21. RFC Editor. https://doi.org/10.17487/rfc2350

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-61r2

Cormack, A., Kossakowski, K.-P., Maj, M., Parker, D., & Stikvoort, D. (2017). *CCoP - CSIRT Code of Practice* (Standard No. CCoPv2.4/2005-2017). Retrieved from https://www.trusted-introducer.org/TI-CCoP.pdf

De Beaupré, A. (2009). *Incident response vs. incident handling*. SysAdmin, Audit, Network and Security (SANS) Internet Security Centre (ISC) InfoSec Forums. Retrieved from https://isc.sans.edu/forums/diary/Incident+Response+vs+Incident+Handling/6205

Department of Justice and Constitutional Development (2016). Cybercrimes and Cybersecurity Bill. Pretoria: Government of South Africa.

Dunbar Security. (n.d). Cyphon: An open source incident management and response platform. Retrieved from https://www.cyphon.io/

Dunbar, R. (1992). Neocortex size as a constraint on group size in primates. *Journal of Human Evolution*, *22*(6), 469–493. https://doi.org/10.1016/0047-2484(92)90081-J

Elastic. (n.d). What is the ELK stack? .Retrieved from https://www.elastic.co/elk-stack

European Union Agency for Cybersecurity (ENISA). (2006). *A step-by-step approach on how to setup a CSIRT*. Retrieved from https://www.enisa.europa.eu/publications/csirt-setting-up-guide

Forum of Incident Response and Security Teams (FIRST). (2016). *Traffic light protocol (TLP). FIRST standards definitions and usage guidance – version 1.0*. Retrieved from https://www.first.org/tlp/

Haller, J., Merrell, S., Butkovic, M., & Willke, B. (2011). *Best practices for national cyber security: Building a national computer security incident management capability, version 2.0*. Technical Report No. CMU/SEI-2011-TR-015. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9999

International Organisation for Standardisation (ISO). (2016). *Information technology — Security techniques — Information security incident management*. Standard No. ISO/IEC 27035:2016. Geneva. Retrieved from https://www.iso27001security.com/html/27035.html

Mooi, R., & Botha, R. A. (2015). Prerequisites for building a computer security incident response capability. In IEEE (Ed.), *2015 Information Security for South Africa (ISSA)*. https://doi.org/10.1109/ISSA.2015.7335057

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world* (1st ed.). New York: John Wiley & Sons.

Schneier, B. (2014). The future of incident response. *IEEE Security Privacy*, *12*(5), 95–96. https://doi.org/10.1109/MSP.2014.102

Shirey, R. (2000). *Internet security glossary, version 2.* RFC No. 2828. RFC Editor. Retrieved from https://tools.ietf.org/html/rfc4949

Stikvoort, D. (2010). SIM3: Security incident management maturity model. Retrieved from https://www. terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

Stikvoort, D., Arvidsson, J., Cormack, A., Jansen, X., Moens, A., & Peters, P. (2015). *Incident classification/incident taxonomy according to ecsirt.net – adapted international version*. Standard No. 1.0. Forum of Incident Response and Security Teams (FIRST).

Trusted Introducer. (n.d). Listed, accredited and certified teams directory. Retrieved from https://www.trusted-introducer.org/directory/teams.html

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, *8*, 1–8. https://doi.org/10.3389/fpsyg.2017.02179

Wang, Q., Gao, J., Zhou, T., Hu, Z., & Tian, H. (2016). Critical size of ego communication networks. *EPL (Europhysics Letters)*, *114*(5), 1–6. https://doi.org/10.1209/0295-5075/114/58004

The African Journal of Information and Communication (AJIC)

Published by the LINK Centre
University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

LINK centre

UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG