

https://dspace.org/

AJIC Issue 20, 2017-Full Issue-Print-on-Demand Version

2017-12-23
http://hdl.handle.net/10539/23580
The African Journal of Information and Communication (AJIC). (2017). Issue 20. https://doi.org/10.23962/10539/23498

Downloaded from a DSpace repository. https://dspace.org/

THE AFRICAN JOURNAL OF INFORMATION AND COMMUNICATION (AJIC)

ISSUE 20, 2017

WITH FOCUS SECTION ON CYBERSECURITY



ARTICLES

Regulatory Imperatives for the Future of SADC's "Digital Complexity Ecosystem" - *Lucienne Abrahams*

Development of a First Aid Smartphone App for Use by Untrained Healthcare Workers - *Chel-Marí Spies, Abdelbaset Khalaf and Yskander Hamam*

Development of a Communication Strategy to Reduce Violence against Children in South Africa: A Social-Ecological Approach - *Mark Edberg, Hina Shaikh, Rajiv N Rimal, Rayana Rassool and Mpumelelo Mthembu*

FOCUS SECTION ON CYBERSECURITY

Guest Editor's Introduction: *AJIC* Focus Section on Cybersecurity - *Kiru Pillay*

Governance of Cybersecurity – The Case of South Africa - *Ewan Sutherland*

An Analysis of Cyber-Incidents in South Africa - *Brett van Niekerk*

Students' Cybersecurity Awareness at a Private Tertiary Educational Institution – *Rajesh Chandarman and Brett van Niekerk*

THEMATIC REPORTS

Potential Contribution of Drones to Reliability of Kenya's Land Information System - *Patricia Kameri-Mbote and Muriuki Muriungi*

Reflections on Legal Uncertainties for e-Commerce Transactions in Cameroon - *Caroline Joelle Nwabueze*

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

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

AJIC 20-21-Jan-18-22h19.indd 1 1/21/2018 10:43:03 PM

The African Journal of Information and Communication (AJIC)

Issue 20, 2017

With Focus Section on Cybersecurity

Published by the LINK Centre, School of Literature, Language and Media (SLLM)
Faculty of Humanities, University of the Witwatersrand (Wits)
Johannesburg, South Africa
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, 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

The journal is supported by an international editorial advisory board, comprising:
Lucienne Abrahams, University of the Witwatersrand, Johannesburg, South Africa
Hatem Elkadi, University of Cairo, Egypt
Nagy K Hanna, author and international development strategist, Washington, DC, US
Joseph Kizza, University of Tennessee, Chattanooga, TN, US
Tawana Kupe, University of the Witwatersrand, Johannesburg, South Africa
Gillian Marcelle, University of the Virgin Islands, St Thomas, US Virgin Islands
Uche M Mbanaso, Nasarawa State University, Keffi, Nigeria
Caroline Ncube, University of Cape Town, South Africa
Ewan Sutherland, University of the Witwatersrand, Johannesburg, South Africa

Editors

Managing Editor: Tawana Kupe, Vice-Principal, Deputy Vice-Chancellor and Professor, University of the Witwatersrand, Johannesburg, South Africa, tawana.kupe@wits.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

Guest Editor, Cybersecurity Focus Section: Kiru Pillay, Visiting Researcher, LINK Centre, University of the Witwatersrand, Johannesburg; and Chief Director Cybersecurity Operations: Department of Telecommunications and Postal Services, Pretoria, South Africa, kiru2010@gmail.com

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

AJIC 20-21-Jan-18-22h19.indd 2-1 1/21/2018 10:43:03 PM

Peer-Reviewing
AJIC acknowledges with gratitude the following peer reviewers of articles in this issue: Lucienne Abrahams, Ufuoma Akpojivi, Chris Armstrong, Nadia Bulbulia, Mark Burke, Nagy Hanna, Manoj Maharaj, Kiru Pillay, Simon Roberts, Carlo Rossotto, Brett Van Niekerk

Production
Sub-editing: LINK Centre
Desktop-publishing: LINK Centre

DOI: https://doi.org/10.23962/10539/23498

Recommended citation:
The African Journal of Information and Communication (AJIC). (2017). Issue 20.
https://doi.org/10.23962/10539/23498

This work is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:
http://creativecommons.org/licenses/by/4.0

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 headquartered at the Wits Tshimologong Digital Innovation Precinct, 41 Juta St., Braamfontein, Johannesburg, www.tshimologong.joburg

Past issues of *AJIC*, and its precursors *The Southern African Journal of Information and Communication* and *The South African Journal of Information and Communication*, are available at www.wits.ac.za/linkcentre/ajic

CONTENTS

ARTICLES

Regulatory Imperatives for the Future of SADC's "Digital Complexity Ecosystem" 1
Lucienne Abrahams

Development of a First Aid Smartphone App for Use by Untrained Healthcare Workers 31
Chel-Marí Spies, Abdelbaset Khalaf and Yskander Hamam

Development of a Communication Strategy to Reduce Violence against Children in South Africa: A Social-Ecological Approach 49
Mark Edberg, Hina Shaikh, Rajiv N Rimal, Rayana Rassool and Mpumelelo Mthembu

FOCUS SECTION ON CYBERSECURITY

Guest Editor's Introduction: *AJIC* Focus Section on Cybersecurity 79
Kiru Pillay

Governance of Cybersecurity – The Case of South Africa 83
Ewan Sutherland

An Analysis of Cyber-Incidents in South Africa 113
Brett van Niekerk

Students' Cybersecurity Awareness at a Private Tertiary Educational Institution ... 133
Rajesh Chandarman and Brett van Niekerk

THEMATIC REPORTS

Potential Contribution of Drones to Reliability of Kenya's Land Information System 159
Patricia Kameri-Mbote and Muriuki Muriungi

Reflections on Legal Uncertainties for e-Commerce Transactions in Cameroon 171
Caroline Joelle Nwabueze

AJIC 20-21-Jan-18-22h19.indd 2-3 1/21/2018 10:43:04 PM

ARTICLES

AJIC 20-21-Jan-18-22h19.indd 4-5 1/21/2018 10:43:04 PM

Regulatory Imperatives for the Future of SADC's "Digital Complexity Ecosystem" [1]

Lucienne Abrahams
Senior Lecturer and Director, LINK Centre, University of the Witwatersrand (Wits), Johannesburg

Abstract
This article uses a "digital complexity ecosystem" framing to delineate the challenges facing regulation of the digital economy in the Southern African Development Community (SADC) region. The digital complexity ecosystem approach, grounded in the field of complexity science – and in particular the study of complex adaptive systems (CASs) – is used to illuminate the sources of uncertainty, unpredictability and discontinuity currently present in the SADC digital sphere. Drawing on examples from three regulatory areas, namely mobile financial services, Internet of Things (IoT) network and services markets, and e-health services, the article argues that SADC regulatory bodies will themselves need to adopt highly adaptive, non-linear approaches if they are to successfully regulate activities in the digital ecosystem moving forward. Based on the findings, recommendations are made on SADC regional regulatory agendas and, at national levels, matters of concurrent jurisdiction.

Keywords
complexity science, complex adaptive systems (CAS), digital economy, digital complexity ecosystem, Southern African Development Community (SADC), electronic communications regulation, economic regulation, social regulation, concurrent regulatory jurisdiction, mobile financial services, Internet of Things (IoT), e-health

DOI: https://doi.org/10.23962/10539/23578

Recommended citation
Abrahams, L. (2017). Regulatory imperatives for the future of SADC's "digital complexity ecosystem". *The African Journal of Information and Communication (AJIC)*, *20*, 1-29. https://doi.org/10.23962/10539/23578

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

1 This article evolved from two conferences papers: (i) a keynote paper delivered at CyberAbuja 2015, the IEEE International Conference on Cyberspace Governance: The Imperative for National and Economic Security, Abuja, 4-7 November 2015 (Abrahams, 2015); and (ii) an unpublished conference paper delivered at the ACER Conference, Livingstone, Zambia, 10-11 March 2016 (Abrahams, 2016).

AJIC 20-21-Jan-18-22h19.indd 6-1 1/21/2018 10:43:04 PM

1. Introduction: The "digital complexity ecosystem" and the SADC region

In the next decade, as the Southern African Development Community (SADC) region shifts to Internet-based life, it will encounter high levels of complexity in economic, social and institutional systems, requiring regulators to anticipate disruptive change and frame regulation for a "digital complexity ecosystem". In this article, the term complexity is used to refer to the uncertainty, unpredictability and discontinuity arising from the interconnectedness of global economic reforms with innovation in digitally-supported communications and transactions, leading to the generation of complex, adaptive forms of digital commerce and digital government. While this article focuses on regulation, it is acknowledged that there is a wider enabling environment acting on and stimulating this ecosystem. These additional enablers include (i) investment appetite and returns with respect to mobilisation of network infrastructures and related services; (ii) digital skills and other innovation factors; and (iii) factors pertaining to the business of each of the major economic sectors, namely the resource-based primary sector, the manufacturing/construction/energy secondary sector, the services-based tertiary sector, and the knowledge-based quaternary sector. Investigating these additional enablers is beyond the scope of this article, but they must be understood as contributing factors to the complex digital transformations taking place.

This introductory section of the article positions the digital economy as a complex adaptive ecosystem, and establishes the need for SADC regulators to respond in a correspondingly complex, adaptive manner. The next section sets out the regulatory dimensions of the digital complexity ecosystem, followed by a section providing an overview of the emerging digital economy in the SADC region. Then, in its core section (Section 4), the article sets out the regulatory imperatives for advancement of the digital complexity ecosystem in the SADC region in respect of the following issues related to digital services access and selected forms of usage: (1) mobile financial services, (2) Internet of Things (IoT) network and services markets, and (3) e-health services. These are all service sectors characterised by elements common to complex adaptive systems, thus producing regulatory uncertainty and discontinuity, emerging from the fact that the choices of whether or not to regulate, and how to regulate, relate more to the balancing of innovation effects (positive and negative), and the re-interpretation of rationales for economic and social regulation, than to utilising existing theoretical foundations for regulation. Furthermore, regulation for cross-sectoral digital transformation engenders contributions from a large number of regulators, not only from electronic communications sector and competition regulators. The article then offers an analysis relevant to SADC regulators, followed by concluding remarks.

The digital complexity ecosystem

The digital complexity ecosystem framework I formulate and apply in this article, following some initial thoughts on the subject (Abrahams, 2015; 2016), borrows

from the field of complexity science. Complexity science is interdisciplinary, and explores the broad terrain (Anderson, 1999; Schneider & Somers, 2006) and application (Akgün, Keskin & Byrne, 2014) of complex adaptive systems (CASs), using a variety of concepts, theories and methodologies for studying such systems (see, for example, Gates (2016), who uses the combined term "systems thinking and complexity science" (STCS)). This article draws on particular concepts from this body of theoretical knowledge as analytical tools, notably those of uncertainty, unpredictability and discontinuity, because they are all closely associated with innovation outcomes. I have observed the presence of these three themes at the current conjuncture of digital innovation and its early effects in the economies of the region, for example the regulatory challenges arising from the introduction of mobile financial services, or MTN Business offering services through IoT platforms in South Africa and Namibia. I have fused notions from complexity science with conceptions of the dynamics of the "digital economy", "digital transformation" and "regulatory imperatives" to arrive at the conception of the "digital complexity ecosystem" presented here.

The value of this kind of conception is its focus on the need for policymakers, regulators and other stakeholders to engage in complexity-oriented, CAS-oriented thinking and analysis, rather than to consider simple solutions to complex challenges, when interacting with emergent digital services. For example, the study of IoT requires complexity science thinking, because IoT artefacts, processes and innovative outcomes are such complex, adaptive (and self-adaptive) applications and systems (see, for example, the work of Moraes do Nascimento & Perreira de Lucena, 2017).

Many features of digital ecosystems can be considered as complex, adaptive systems, whether the feature consists of introducing IoT applications for smart cities, or building out mobile financial services, or a manifestation in the socially oriented arenas of Internet-supported education, digitally enabled health practice, or digital government. Each of these systems is multi-faceted – constantly shifting, adapting and evolving as supply-side and demand-side actors adjust to new services, new competitive advantages or threats, new opportunities, and unexpected outcomes.

Risk for SADC regulators

Given this adaptive complexity inherent in the elements of digital ecosystems, regulation of these ecosystems' core elements – such as electronic communications markets, Internet-based services markets, and digitally supported environments arising from convergence of electronic communications and Internet-based services (e.g. smart cities) – requires advances in the institutional environment towards intensive knowledge formation, in order for regulatory bodies to perform effectively. Regulatory institutions that fail to build and command such knowledge will run the risk of becoming all but irrelevant to the emergent digital ecosystem. This risk is already apparent in the SADC region, where the pace of change is poised to test the

AJIC 20-21-Jan-18-22h19.indd 2-3 1/21/2018 10:43:05 PM

capacity of regulators to advance the supporting regulatory agenda at the required pace.

Some may try to argue that digital complexity ecosystem regulatory challenges are not particularly pressing in a region such as the SADC, where several of the countries' Internet penetration levels are among the lowest in the world, but the converse is true. If the roughly 78% of SADC residents[2] not yet using the Internet are to join the digital complexity ecosystem and participate in a manner that safely enhances their livelihood opportunities, the regulatory imperatives outlined in this article must be at the forefront of the agendas of the region's regulatory authorities. Furthermore, it can persuasively be argued that while African economies are growing in size, they are not growing sufficiently in technological, process or governance complexity, or in the enhancement of "the technical capabilities of people and institutions" (African Center for Economic Transformation, 2013) required for transforming from mainly low-technology-using agricultural and services-based economies to medium- or high-technology-using[3] agricultural and services economies, supported by digitally complex ecosystems. Effective regulation is needed to enhance the effective operation of the supporting digital ecosystem.

It is acknowledged that there are other contemporary regulatory questions pertaining to the digital ecosystem that are not covered in this article – such as regulation for over-the-top (OTT) services, for cloud computing, for smart cities, for cryptocurrencies, and for other forms of digital transformation – and that also need regulatory research and debate. The scope of this article excludes a full review of the current state of SADC regulation for the digital economy. Such further research would be important for designing a formal regulatory agenda and research programme for SADC regulators and regional regulatory associations.

2. Regulation in the digital complexity ecosystem

In the late 1990s and early 2000s, much of the electronic communications sector research focused on the social and economic regulation of the "telecommunications economy", with particular attention to regulatory approaches to guiding telecoms market structures and facilitating transition from monopoly to competition (Boylaud & Nicoletti, 2001; Buigues, 2006; Bourreau & Dogan, 2004; Fredebeul-Krein & Freytag, 1999; Gillwald, 2005; Noll, 1999). The research agenda then expanded to include regulation for fostering the "mobile communications economy" (Gebreab, 2002; Haucap, 2003; Nanevie, 2012), and then for evolution of the "broadband

2 This percentage is based on total estimated population and total estimated Internet access (Internet World Stats, 2017), noting that only a very small age cohort would not need to engage in direct Internet use, but should still have indirect participation in the digital ecosystem.

3 The OECD classifies telecommunications (non-manufacturing) as being among medium-low R&D intensity industries; IT and other information services (non-manufacturing) as being among medium-high R&D intensity industries; and software publishing (non-manufacturing) as being among high R&D intensity industries (Galindo-Rueda & Verger, 2016).

Internet economy" (Fransman, 2007; Kelly, Mulas, Raja, Qiang & Williams, 2009; Czernich, Falck, Kretschmer & Woessman, 2011).

More recently, scholars have enlarged the field to encompass the broad "cyber" or "digital" economy, with myriad dimensions including: regulation of open access telecommunications infrastructure (Krämer & Schnurr, 2014); the role of regulation in stimulating innovation in the telecoms sector (Cave, 2016; Vogelsang, 2017); micro-licensing for future 5G networks (Matinmikko, Latva-aho, Ahokangas, & Seppänen, 2017); advances in spectrum regulation (Lawson, 2014; Basaure, Marianov, & Paredes, 2015); market power in multi-sided digital services markets (Krämer & Wohlfarth, 2017); regulation with respect to applications of the IoT (Brown, 2015); privacy regulation for secure smart city networks (Bartoli, et al. 2012); monitored self-regulation in the field of data protection (Lachaud, 2017); the right to digital identity in law (Sullivan, 2016); financial regulation in Bitcoin markets (Pieters & Vivanco, 2017); and the multitude of cybersecurity regulatory matters (Hinde & Van Belle, 2012; Hutchings, Smith, & James, 2013; Maaref, 2012; Peter, 2017). Hernandez, Leza and Ballot-Lena (2010) discuss "ICT regulation in the digital economy", while Hanna (2015; 2016) draws attention to "transforming to a networked society", and "mastering digital transformation".

Regulators in the SADC region have been mainly engaged in laying the infrastructural foundations for a digital economy, with greater or lesser degrees of success. The emerging phase of digital economy evolution evinces a greater degree of complexity in law-making and rule-making than before, a phase in which greater mastery of the regulatory environment is required. This phase is about more than "ICT regulation"; it is about moving to interconnected jurisdictions and spheres of regulation that will promote the digital business, commerce, trade and services that operate on the foundational infrastructure.

Economic regulation for the electronic communications sector has generally been understood as addressing access, effective competition, and consumer protection (Blackman & Srivastava, 2011, p. 10), noting the distinctions amongst theories of regulation, e.g., public interest, interest group, power of ideas, institutional, and network theories (Baldwin, Cave & Lodge, 2012, pp. 40-67). Economic regulation also addresses sector innovation, as discussed extensively in Blackman and Srivastava (2011) and Baldwin et al. (2012). Meanwhile, s*ocial* regulation for the electronic communications sector has generally been concerned with "achieving socially desirable results", including addressing essential services (Baldwin et al., 2012, pp. 19 and 24).

While much of this important theoretical work on the modalities of electronic communications regulation remains relevant, there are many new features, interpretations and applications of economic and social regulation that are relevant

AJIC 20-21-Jan-18-22h19.indd 4-5 1/21/2018 10:43:05 PM

to digital ecosystem evolution in 2017 – and which will grow in importance and relevance in the next decade, including in SADC region countries. The digital economy of mobile apps; OTT services and other digital platforms; mobile money; utilisation of robotics and social media in banking; gamification in digital education; online entertainment; digital health services; early formations of smart cities (such as the Konza Techno City in Kenya); and many more digital modalities, is one in which the regulatory agendas of African electronic communications sector regulators will need (i) to be refocused and (ii) to be complemented by the efforts of other sector regulators. Without shifts in regulatory focus and practice, African economies will struggle to transition to well-functioning digital economies. To give but one example, definitions of universality now need to include consideration of access to online e-services and mobile services for education, health, banking and finance, and other mobile or Internet-based services.

3. The SADC digital economy

The economy of the region is strongly services-based, with a few economies also having a significant agricultural or manufacturing component (see Table 1 below). As of mid-2016, an estimated 332.5 million people resided in the SADC region (World Bank, 2017; ECA, AfDB Group & AUC, 2017, p. 36), of whom estimates indicate that 147 million or 44% would have mobile subscriptions, 113 million or 34% would have smartphones, and 72 million or approximately 22% had some degree of Internet use, thus constituting approximately 18% of African Internet users (GSMA, 2015a, p.19;[4] Internet World Stats, 2017).

Mobile telephony (voice and text) access on the African continent has increased significantly in recent years, and was estimated at 420 million unique mobile subscribers, or a 43% penetration rate, at the end of 2016. Industry reports suggest that the mobile industry, including mobile broadband, could account for an estimated USD214 billion of Africa's annual GDP by 2020 (GSMA, 2016, p. 6). Mobile penetration in countries in the SADC region ranges from those with penetrations of 60% and above (Botswana, Lesotho, Mauritius, Seychelles, South Africa, Tanzania), to those with penetrations between 50% and 59% (Democratic Republic of Congo, Swaziland, Zambia, Zimbabwe), between 40% and 49% (Mozambique, Namibia), to the low-penetration countries of Angola, Malawi and Madagascar (34%; 35% and 23% respectively) (GSMA, 2017, p. 9; ITU, 2017a, pp. 240-243).

Mobile Internet subscriber penetration is estimated at 28% for the whole of Africa (GSMA, 2017, p. 33) and total Internet penetration at 31% in 2017 (Internet World Stats, 2017), indicating that Internet penetration is largely mobile. SADC region Internet penetration is lower than the continental average and is reported as being highest in Mauritius, The Seychelles,[5] and South Africa, and significant in Botswana,

4 Latest publicly available data for SADC region.
5 Mauritius and The Seychelles are small island states.

Namibia, Swaziland, Zambia and Zimbabwe, while penetration is less than 10% in the Democratic Republic of Congo (DRC), Madagascar and Malawi (Internet World Stats, 2017). There is now a clear trend towards mobile broadband adoption on the continent and it is envisaged that around 60% of subscribers will have mobile broadband Internet access, in other words usable Internet, by 2020 (GSMA, 2017, p. 7).

Table 1: SADC regional economy: Key statistics

Country	Population 2016 (millions)	GDP 2016 (USD billions)	Agriculture as % GDP	Manufac-turing # as % GDP	Services as % GDP	Internet penetration %
Angola	28.8	89.6	10.1*	5.5*	46.5*	22.3
Botswana	2.2	15.2	2.4*	6.4*	64.3*	39.4
Democratic Republic of Congo	78.7	34.9	21.1	17.5	64.3	6.2
Lesotho	2.2	2.1	5.7*	10.7*	62.3*	27.4
Madagascar	24.8	9.9	24.4	13.8	56.5	5.1
Malawi	18.0	5.4	28.3	10.4	55.8	9.6
Mauritius	1.2	12.1	3.5	13.9	74.8*	62.7
Mozambique	28.8	11.0	24.8	9.5	53.6	17.5
Namibia	2.4	10.2	6.7*	9.1*	62.3*	31.0
Seychelles	0.094	1.4	2.6**	8.5**	83.0**	56.5
South Africa	55.9	294.8	2.4	13.4	68.6	54.0
Swaziland	1.3	3.7	9.9*	33.5*	52.2*	33.0
Tanzania	55.5	47.4	31.1	5.9	41.8	13.0
Zambia	16.5	19.5	5.3*	7.9*	59.4*	30.1
Zimbabwe	16.1	16.2	11.2	9.9	64.5	41.1
Total	332.5	573.4				

Sources: ECA, AfDB Group & AUC, 2017; Internet World Stats, 2017; World Bank, 2017
*** latest data 2015**
**** latest data 2014**

 # other industry is not included in order to highlight local manufacturing

Low household incomes and rural modes of subsistence production (WEF, 2017, p. 7) may hold back the pace of adoption of mobile broadband, but adoption is set to continue, given the innovations in digital services for consumers at many income levels. The smartphone adoption trend creates the foundation for a stronger consumer push to a digital economy in the SADC region in the next decade. Four SADC countries appear in the Global Mobile Engagement Index (GMEI) (a measure of frequency of mobile service usage with smartphones and non-smartphones) out of 56 countries surveyed, namely South Africa, Mozambique, Tanzania and DRC with, for example, Tanzania showing significant usage of remittances via mobile money service, online banking and bill payment (GSMA, 2017, p. 27).

AJIC 20-21-Jan-18-22h19.indd 6-7 1/21/2018 10:43:05 PM

While substantial numbers of subscribers, connections and broadband services will mean that network effects (demand-side economies of scale) increase, and while these network effects can create value for rural households – through, for example, benefits of mobile money transfer or access to educational content – this value can only manifest where villages and villagers have reasonable access and quality of service with respect to voice and broadband. Bello, Opadiji, Faruk and Adediran (2016) shed some light on the realities for rural households on the wrong side of the digital divide in villages in rural Nigeria, where access to basic mobile service is low due mainly to lack of network infrastructure and quality of service. There are many such villages across the SADC region, raising critical questions for electronic communications sector regulators with respect to continued major gaps in universality and quality of service in the next decade. In the SADC region, when one looks at the countries with populations above 10 million, one finds that in Angola, an estimated 55% of the population is rural, 57% is rural in the DRC, 83% in Malawi, 67% in Mozambique, 34% in South Africa, 67% in Tanzania, 58% in Zambia, and 67% in Zimbabwe (ECA, AfDB Group & AUC, 2017, p. 37).

The SADC regional economy has a strong bias towards services and agriculture as the largest contributing sectors to GDP, sectors in which innovative digital applications and platforms can be adopted with relative ease, provided that the economic and social environments are reasonably well regulated and governed. IoT applications are already in operation for urban management in a few cities (example Windhoek) (NUST, n.d.), and appetite for mobile financial services has been observed (Mazer & Rowan, 2016; Robb & Vilakazi, 2016).

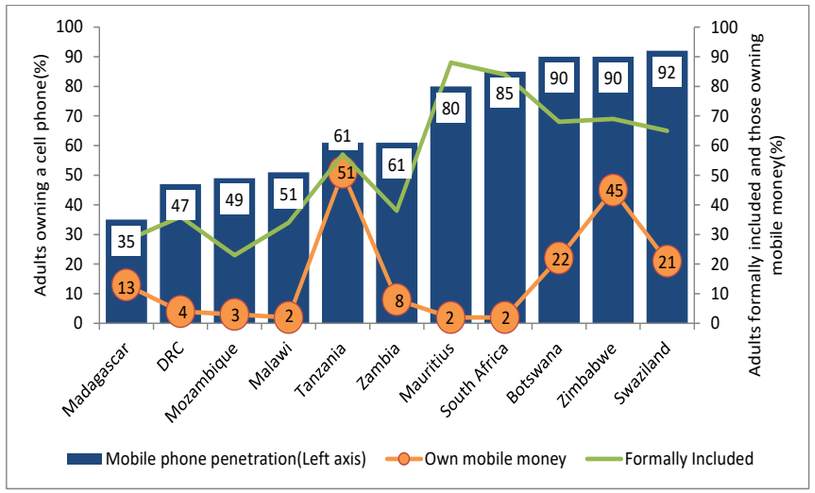
Mobile financial services

In the SADC region, digital technologies and processes are transforming consumer and business markets in the financial sector towards fully-digital banking, including robotic transaction processing and virtual assistants, requiring attention to cybersecurity. Mobile money adoption is significant in Swaziland and Botswana (21% and 22% respectively) and high in Zimbabwe and Tanzania (45% and 51% respectively) (Fanta, Mutsonziwa, Goosen, Emanuel, & Kettles, 2016). Adoption in 2017 is likely to be higher than in the latest survey years. Mobile money statistics for Tanzania are as follows: with a population of 56 million (Internet World Stats, 2017) and 40.2 million mobile subscriptions, there were, in June 2017, 20.2 million mobile money accounts with five mobile money providers (Vodacom M-Pesa, Tigo Pesa, Airtel Money, Ezy Pesa and new entrant Halotel Money) (TCRA, 2017). Furthermore, Tanzania had more than 166,000 mobile money agents in 2016, and one-third of Tanzanians lived within 5km of an agent (CGAP, 2016).

Notwithstanding the quite strong adoption in Tanzania and Zimbabwe, mobile money and mobile financial services are not yet widespread in the SADC region (see

Figure 1 below[6]) (Fanta et al., 2016). In the case of Zambia, a recent study found that 94.3% of rural people did not have a bank account and around 70% of urban adults did not have bank accounts (Banda, 2016), while 9 million or 53% had a mobile phone (GSMA, 2017, p. 9). Noting that mobile money transactions would now be significantly higher than the USD300 million per month estimated in 2014 (GSMA, 2015b, p. 32), these data present a strong case to leverage the deepening mobile penetration rates and extensive ownership of mobile phone devices to enhance financial inclusion through digital innovation, balanced against appropriate levels of regulation.

Figure 1: Mobile money usage across 11 SADC countries



Source: Fanta et al. (2016), p. 7

The mobile financial services basket includes both service processes and mobile money, notably the following types of services: mobile money transfer from person to person; mobile payments including bill and merchant payments; mobile credit and savings with or without a bank account; mobile insurance; and other mobile financial services for the unbanked and the banked, e.g., where supermarket chains or networks of retailers develop products to transfer money across borders, to transfer through the banking system, or to transfer through Internet banking using a smartphone or other connected device.

The 2016 FinMark Trust study (Fanta, et al., 2016, p. 19) indicates that the four main forms of mobile money usage in eight countries in the SADC region are paying bills, buying air-time, sending money and receiving money, with bill payments being a minor proportion of "top four" transactional activity, as compared to the more

6 Formally included means financial inclusion in the banking and financial system.

AJIC 20-21-Jan-18-22h19.indd 8-9 1/21/2018 10:43:06 PM

extensive uses of mobile financial services elsewhere on the continent, including mobile salary disbursements and mobile payments for commercial transactions, education and health services, and transport (GSMA, 2017, p. 27; GSMA, 2015a, pp. 30-35). Mobile financial services bring networks of retailers, banks and mobile operators into competition in the mobile financial services sector, with potential long-term innovation and consumer benefits. Thus, while the current pace of mobile financial inclusion is slow in the SADC region, the potential is great and can be translated into actual financial inclusion through proactive regulation.

In 2014, the cost of intra-regional remittances was comparatively high when using the traditional banking system: the average total cost of sending USD200 within Southern Africa was USD20.47 (approximately 10% of the value of the transaction) for cross-border banks[7]; and USD17.24 for banks operating in a single country (AfDB, 2014, p. 73). By contrast, the cost to the consumer of using mobile money service providers for cross-border remittances is significantly lower. In 2017, Airtel Money Malawi charges 3% of the value of the transaction for cross-border transfers of the equivalent of USD200 in Malawian Kwacha and no cash-out charges are applied, though charges are higher than bank charges in the lowest transaction band (Airtel Money Malawi, 2017). In Tanzania, with respect to Airtel Money tariffs effective from September 2017, there are no charges to the sender for amounts above TZS200,000[8] (approximately USD88) and cash-out charges are low for Airtel Money customers and partner networks, but high for the recipient at the lower transaction bands (Airtel Money Tanzania, 2017), a matter that may require regulatory attention.

The *African Development Report 2014* motivated for the financial integration of retail payment systems across the continent, in order to promote greater economic participation and cross-border trade, noting that mobile financial services innovation was then at the early stages of its evolution (AfDB, 2014). In this context, the review commissioned by the Committee of Central Bank Governors in SADC (CCBG-SADC) with respect to the laws and regulations applicable to national payment systems gave rise, in March 2016, to the publication of SADC Mobile Money Guidelines (FinMark Trust, 2016). The SADC Model Law on Electronic Communications and Transactions, prepared for SADC electronic communications regulators is also relevant, as indicated later.

Internet of Things (IoT) networks and services

IoT applications and services require human-to-machine (H2M), machine-to-machine (M2M), and, ultimately, everything-to-everything (E2E) communication, creating "[a] global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving

7 Cross-border banks operate in more than one African country

8 TZS = Tanzania Shilling, written locally as TSH.

interoperable information and communication" (Brown, 2015). At international level, IoT deployment is significant in applications in smart cities, connected vehicles, and healthcare (Brown, 2015), and is emerging in the fields of industrial maintenance, building information modelling, and the insurance sector (Civerchia, 2017; Gartner, 2016), the latter case interweaving the electronic communications and financial services sectors in another area fostering overlap in regulatory agendas.

With respect to early trends and use cases in IoT adoption in Africa, Ndubuaku and Okereafor (2015) comment on the need to transition, in Nigeria, from IoT being dominated by M2M communication (e.g., point-of-sale devices, fleet management, personal vehicle tracking and security monitoring of oil tankers and vessels), to E2E communication with more advanced IoT applications needed in traffic management, oil pipeline monitoring, wildlife conservation, and tracking of medical equipment (Ndubuaku & Okereafor, 2015). The Hawkes (2017) study presents African examples of the use of IoT applications in energy and utilities (IoT-enabled solar systems in Ghana and Ivory Coast; sensors in water pumps in rural Rwanda; electricity load limiting through smart meters in Johannesburg); IoT applications to foster precision agriculture and "agro based analytics" (IoT in livestock tracking, and the deployment of agricultural drones for data collection to inform usage of scarce agricultural inputs). It comments on the unexploited potential in healthcare (for remote patient monitoring and management, or the management of virus epidemics through extensive data collection and predictive analytics), amongst other uses. South African insurtech startup Naked Insurance is seeking to offer customers a "new generation insurance" experience (Jackson, 2017). New insurance business models include remote sensors and other IoT-connected devices at the insured's premises, sending data to a data centre or warehouse for rapid customer response.

Tech hubs in the SADC region, such as the FABLab Design and Technology Centre in Windhoek, Tshimologong Digital Innovation Precinct in Johannesburg, and a few other tech hubs are participating in IoT innovation to meet local demand and offer IoT services at locally defined prices. For example, FABLab is adapting sensors for localised uses in Namibia, initially focused on environmental sensing, with future interest in water and waste management, parking and transport management, and other applications to urban management (see the Smart Citizen – FABlab Namibia video).[9] Tech hubs and collaborative working spaces are now estimated to number over 300 across Africa, and around 70 in the SADC region, including FABLab, Tshimologong, Bongohive Zambia and Dar es Salaam Innovation Space (Disrupt Africa, 2016; GSMA 2017; World Bank, 2016), potentially spaces for building IoT applications.

9 Smart Citizen – FABlab Namibia video available at http://fablab.nust.na/?q=all-projects-list#cb-p=/?q=project/smart-citizen

AJIC 20-21-Jan-18-22h19.indd 10-11 1/21/2018 10:43:06 PM

While IoT applications can use existing Wi-Fi and other telecoms networks, operators Huawei, MTN, Vodacom and others are also offering new network solutions such as LTE-M (medium bandwidth) and re-using 2G networks for IoT for smart grids and object tracking; as well as introducing low-power and narrow-band networks such as LPWA IoT networks and NB-IoT networks[10] for smart water metering and other solutions (Hawkes, 2017, p. 14). IoT data sensing, capture, storage and communication provide the basis for making available extensive data as the basis for research in data analytics, predictive analytics, and artificial intelligence, leading to enhanced evidence-based decision-making and applications of value to societies and economies. However, sharing the data, and conducting data-driven activities, via the Internet raise significant cyber risk. The SADC Model Law on Data Protection and the SADC Model Law on Computer Crime and Cybercrime are relevant, as indicated later.

e-Health services innovation

Public health advancement places strenous demands on government funding, and on efficient use of the resources available for patient management in hospitals and clinics across the SADC region. Some of the applications to public health management challenges, that can promote greater efficiency in healthcare management, arise from digital innovation (i) in the use of location-specific services for targeted approaches to malaria management and response; or (ii) in the field of data analytics, for example with respect to the management of dread diseases (such as cancer, heart attack and stroke), and chronic diseases such as HIV/AIDS; or (iii) the use of IoT applications ranging from remote health monitoring to facilities management.

Article 7 of the SADC Protocol on Health requires the sharing of health data and the establishment of a regional indicators database (SADC, 1999), requirements that are ever more important as the regional economy becomes more integrated. Health applications of the Internet, including the use of IoT for sharing public-health-related data or anonymised patient data, can be appropriate, relatively low-cost, digital innovations in primary healthcare services. However these innovations are at a nascent stage in the SADC region. Hawkes (2017, p. 5) reports South African start-up Vitls as offering a wearable device that monitors vital signs and "sends the data to the cloud where algorithms create actionable insights for medical staff", noting that IoT applications need healthcare institutions to introduce electronic medical records, which is considered possible in the medium term. IoT applications in healthcare can encourage greater self-management, for example in the treatment of diabetes (Brown, 2015, p. 11) and other diseases of lifestyle. At the same time, there are, in these health applications, concomitant risks of interference with data, as well as privacy risk and ethical risk, all requring regulatory attention. e-Health

10 LPWA IoT network means low power wide area IoT network; NB-IoT network means narrow band IoT network.

regulatory issues overlap with regulating the trust environment to advance the use of IoT platforms and services, as health regulatory issues pertaining to the ethical treatment of patient data by clinicians and health practitioners require privacy and data security with respect to patient personal information and medical records. The SADC Model Law on Data Protection and the SADC Model Law on Computer Crime and Cybercrime are also relevant here, as indicated later.

Seeing the SADC digital economy within a complex adaptive ecosystem

The ways in which regulatory dynamics interact with economic (or social) dynamics lead to an evolving digital ecosystem. The ecosystem influences the economy, and vice versa. As we have seen in the preceding sub-sections, the SADC digital economy demonstrates many of the features that are typical of complex adaptive systems, for example: uncertainty that arises due to the risks experienced in mobile financial services; unpredictability that arises through the emergence of next generation telecoms and IoT infrastructure networks; and discontinuity that arises where regulation rapidly shifts from a focus on telecoms regulation, to electronic communications sector regulation, to digital ecosystem regulation.

4. SADC regulatory imperatives in the digital complexity ecosystem

The SADC regulatory imperatives are discussed below in the following sequence: (i) key challenges in regulating mobile financial services; (ii) key challenges in regulating IoT networks and services; and (iii) key challenges in regulating the e-health services environment.

Regulating mobile financial services

It is widely recognised, at both a global and SADC regional level, that the attention of regulators is required with respect to: competition and interoperability across providers in the mobile money ecosystem (see, for example, Bourreau & Valletti, 2015); cross-border remittances and money transfers (see, for example, Mazer & Rowan, 2016); licensing or approval of service providers (see, for example, Evans & Pirchio, 2015); regulating to advance innovation (see, for example, Blechman, 2016); and regulatory harmonisation with respect to all of these issues within regional and continental blocs. Some of these responsibilities are the role of central banks, some the role of electronic communications sector regulators, and others the role of competition authorities. Furthermore, consistency and harmonisation issues arise with respect to regulatory action across the SADC region, raising the profile of regional regulatory associations in promoting the digital complexity ecosystem.

Competition and interoperability

Given its relative convenience and socioeconomic efficiency, SADC regulators need to research and understand the barriers to extensive mobile money adoption that could be addressed through regulation. Regulatory assurance of, in particular, the promotion of interoperability of mobile money services, is important with respect to

AJIC 20-21-Jan-18-22h19.indd 12-13 1/21/2018 10:43:06 PM

the following (Bourreau & Valletti, 2015): interoperability of the mobile networks that promote mobile money services; interoperability of mobile money agents to serve consumers of any service; and national and regional interoperability across mobile money platforms (at the SADC regional level, these would include Airtel Money, or Vodacom M-Pesa, or another platform).

With respect to regulatory lessons from mobile money services in the SADC region and in Africa, studies are relatively recent. Robb and Vilakazi (2016, pp. 27-28), with reference to Tanzania and Zimbabwe, note that Tanzanian firms embraced interoperability, possibly due to the symmetrical nature of the market; while some Zimbabwean firms encouraged interoperability (NetOne and Telecel) to the benefit of consumers, and others did not (Econet), possibly due to the relatively small market size and Econet being a dominant player. In the Zambian experience (Banda, 2016), competition issues relate to agent exclusivity, interoperability at the agent level for agent sharing (about 50% of 5,000 agents are active), issues around account opening, and network effects. Other regulatory issues Banda notes in the Zambian context are that the National Payment Systems Act 1 of 2007 may have limitations with respect to services beyond payments and transfers; for example, no allowance is made for interest payments on the funds in a mobile money wallet. Some of the just-cited regulatory issues require the attention of competition authorities, others require the attention of the banking regulator. Issues in competition regulation are paramount in respect of the emerging mobile financial payments ecosystem, which includes an array of products and services, including mobile insurance and mobile credit, in addition to the more traditional mobile money products.

Cross-border remittances and money transfers for cross-border trade

Advancing mobile money systems for cross-border trade, to enhance access to income over and above remittances, requires the attention of the general competition and consumer protection regulators, as well as the sector-specific regulators, namely central (or reserve) banks, electronic communications regulators and financial integrity regulators (FinMark Trust, 2016, p. 29). The *ex ante* promotion of competition in mobile money and payments markets by regulators can potentially stimulate interest in fostering the mobile money and mobile payments ecosystem as a means to intra-regional trade.

Licensing

The SADC Mobile Money Guidelines propose that central banks focus on the licensing and licence conditions (or approval) of mobile money service providers (MMSPs), while electronic communications regulators focus on the licensing and licence conditions of the mobile network operators (MNOs) who constitute or support the MMSPs. For example, with respect to approvals, Directive #24 of the Central Bank of the DRC, the country's banking regulator, requires that, "[p]rior to performing any electronic money activity, electronic money institutions, as defined in the Directive, must be approved by the Central Bank" (Di Castri, 2014). Contemplating the take-off of mobile financial services, Evans and Pirchio (2015) suggest that heavy regulation may stifle development, e.g., via a requirement for a banking licence for mobile money transfer even if there is no banking involved, or via the level of personal identification and know-your-customer (KYC) data required for basic transactions where small amounts of money are transferred. In the recent Tanzanian experience (CGAP, 2016; Mazer & Rowan, 2016; Roberts, 2016), the central bank allowed light touch regulation for the three MNOs who held significant mobile money market share, leading to rapid growth in the numbers of registered mobile money users, active users, and active agents.

Regulating to advance innovation

Using lessons from Kenya, a regulatory respondent (personal communication, 2016), explains that the regulator's dilemma is whether to regulate or whether to allow innovation and market evolution before regulating. In the mobile finanical services context, this applies to, among other things, the presence of agents and super-agents; clarifying the relevant market definitions; and consumer protection, e.g., transparency in billing. Focusing on one particular dimension of the dilemma, the respondent commented on regulatory uncertainty (personal communication, Kenyan regulatory respondent, 2016):

> […] while M-Pesa is a success in everyone's eyes, when the innovation came into being, as a regulator you don't know whether the regulation will create competition issues, you don't know whether the innovation works, you don't know where to balance between competition issues and recoupment of the innovation cost, … if it is a competition issue, is it temporal, transitional or permanent?

This draws attention to the question of when and how the regulator steps in, based on its agenda, knowledge, foresight and resources. The regulator has to consider the definition of the relevant (new) market in order to design and conduct market studies. Working through these questions means that SADC regulators will require greater research capacity than is currently available, as well as foresight mechanisms, to adjust to the digitally complex environment.

The same Kenyan respondent explained (personal communication, Kenyan regulatory respondent, 2016):

> […] where Equity Bank came up with Equitel thin-film, SIM-based transfer (you just add an additional SIM and place it on top of existing SIM), Safaricom went to court and said "maybe someone will steal data from our SIM". The Competition Authority allowed rollout and took a wait-and-see approach. One of the main government agencies asked about the risks associated with unauthorised access to people's data. All the

AJIC 20-21-Jan-18-22h19.indd 14-15 1/21/2018 10:43:06 PM

> agencies had their own concerns. The [regulatory approach] could lead to curtailment until Equity Bank can address all the issues, or [the regulator can] let them roll out and understand the challenges […]. The whole problem is not resolved, but particular approaches can resolve particular parts of the dilemma.

This reflection illustrates the multiple concerns of multiple regulators and the inability to make, or inadvisability of making, quick decisions based on past experience when countenancing innovative shifts in technologies, services and markets. As regulating to advance innovation requires the existence and effective action of multiple regulators, SADC countries must act to fill the gaps in the regulatory environment. This will require the attention of those countries who do not yet have competition laws (Angola, DRC, Lesotho), those without competition authorities (DRC, Lesotho, Mozambique) (Ngobese & Kühn, 2017), and those without consumer protection authorities, cybersecurity regulators and other regulatory institutions required to cement the regional digital ecosystem. Beyond filling the gaps with respect to institutions and statutes, future challenges and complexities will include role clarity, i.e., unanticipated, multi-directional, overlapping responsibilities across regulators that require new forms of concurrent jurisdiction and affect the practice of designing new regulation.

Regulatory harmonisation

Regulatory harmonisation in the African telecoms and ICT sector is seen as a way to promote common approaches to common problems, as well as a means to create similar regulatory environments, thereby encouraging investment, competitive regional markets and consumer access (ITU, 2017b). Through the Harmonisation of ICT Policies in Sub-Saharan Africa (HIPSSA) project, a number of guidelines and model laws have been formulated, including three SADC model laws relevant to the mobile financial services environment. The SADC Model Law on Electronic Transactions and Electronic Commerce (ITU, 2013a) provides guidance with respect to legal recognition and legal effect of electronic communications and transactions; attribution of secure electronic signatures; the protection of online consumers; and matters related to online marketing and online safe harbours. Other relevant model laws are the SADC Model Law on Data Protection and the SADC Model Law on Cybercrime. With this guidance, each SADC country enacts its own laws and publishes its own related regulations, enabling the effective regulation of mobile financial services as a key component of the digital economy in the region.

With respect to the payments system environment, the Office of the Committee of Central Bank Governors in SADC (CCBG-SADC), the regional regulatory office for the banking sector, has established a Payments System Project under its Payments Subcommittee, which attends to matters of exchange control and banking supervision. The Payment Systems Project is interested in three key objectives

(SADC BA, n.d.), namely (i) an environment of harmonised, inclusive, and sustainable banking services; (ii) co-operation with national regulators to achieve integrity and credibility with respect to banking services; and (iii) improved technical and regulatory capacity of member associations to make their financial markets more attractive to regional and international investors. Meanwhile, the SADC Mobile Money Guidelines, commissioned by the CCBG, include commentary on (i) regulatory approaches necessary to create an enabling environment for vibrant mobile money markets; (ii) the ecosystem and the mobile money role players engaged in the formulation of regulations; (iii) common technical and operational standards for possible implementation by central banks, telecommunications regulators and other mobile money stakeholders; and (iv) domestic and regional interoperability through regulatory harmonisation (FinMark Trust, 2016, p. 2).

With respect to the just-listed SADC Model Laws and to the SADC Mobile Money Guidelines, central banks and electronic communications sector regulators have significant responsibilities, many of which are still to be acted on in ways that can create a strong regulatory environment for mobile money, mobile credit, mobile insurance, mobile payments and other mobile financial services.

Regulating IoT networks and services markets

SADC regulators must acknowledge the transformative nature of IoT infrastructures and applications, with respect to their contribution to economic organisation and advancement, and their provision of data for enhanced decision-making, as discussed above. The effective evolution and formation of IoT networks and services in the SADC region will require attention to a series of connected regulatory agendas and measures, within individual regulators and across multiple regulators. Many IoT use cases will present regulators with new issues for attention with respect to matters such as: competition and barriers to entry in IoT network infrastructure markets (requiring the attention of electronic communications regulators and competition authorities); and data privacy and cybersecurity (requiring the attention of cybersecurity regulatory bodies, information privacy regulatory bodies, and health professions councils where patient records are involved).

Competition in IoT networks and services

New challenges arise for access to the digital economy with respect to emerging IoT network infrastructure (for example, LWPA IoT and NB-IoT) availability, pricing and penetration. Digital access concerns also relate to the IoT-enabled services that can improve livelihoods and lifestyles. Since the existing SADC mobile network operators are in a strong position to create IoT network and service markets, this presents possible barriers to entry for new players and potentially high prices for business and household consumers, requiring regulatory attention. Key IoT regulatory issues (Brown, 2015, pp. 19-20) that will need to be investigated by SADC

AJIC 20-21-Jan-18-22h19.indd 16-17 1/21/2018 10:43:06 PM

regulators include spectrum licensing and management to foster IoT networks and uses, noting also the new uses for 2G networks; addressing and numbering for "globally addressable things"; and competition regulation to address abuse of dominance where it arises.

Data privacy, cybersecurity and cybercrime
Converged IoT payments systems mean that payments can be made over an IoT platform, from your mobile device, or from your watch, or from your car, raising personal data protection and cybersecurity risks. The SADC Model Law on Data Protection (ITU, 2013b) provides guidance on the establishment of national data protection authorities, rules applicable to the processing of personal data, rights of the data subject, and transborder data flows. The SADC Model Law on Computer Crime and Cybercrime (ITU, 2013c) provides guidance on what would constitute cybercrime offences – including illegal access, illegal data interference, and data espionage – as well as on matters of criminal liability.

In terms of these two SADC Model Laws, each SADC country must enact its own data protection and cybersecurity laws and publish its own related regulations. In the Hawkes (2017) study, an industry expert argues that regulation in Africa is lagging the early initiatives in IoT deployment, noting that while existing legislation for personal data protection could potentially be extended to IoT, this may not suffice for the range of new IoT use cases. The same expert notes that few SADC countries have enacted the relevant data protection legislation. Similarly, few countries in the region have effective (or any) cybersecurity legislation, designed with the specific intent of addressing risks in IoT services markets, as the basis for regulation. For example, South Africa's privacy and data protection law, the Protection of Personal Information (POPI) Act was passed in 2013, before entry of IoT network and service providers, and only signed into law in 2017. And South Africa's cybersecurity/cybercrime law has not yet been enacted. Botswana, Mauritius and Zambia have laws that address some aspects of cybersecurity and cybercrime, but these laws need to be updated to address, inter alia, matters relating to IoT-based services (personal communication, cybersecurity specialist, South African government, 2017).

Regulating e-health services
Regulatory issues that arise in respect of e-health services for electronic communications regulators and for health regulators include: availability of broadband and IoT networks; pricing of broadband and IoT services; privacy and trust with respect to the storage of anonymised personal health data in the cloud; and security pertaining to sharing of health data as the basis for data analytics services.

Availability of broadband and IoT networks and pricing of services
Introducing and utilising e-health services requires availability of broadband infrastructure in hospitals and clinics, in order to effectively collect and communicate

patient health data from clinics and hospitals to decision-making structures, with a reasonable degree of accuracy and validity. Promoting broadband access is already on the regulatory agenda for electronic communications regulators, though progress is slow in many SADC countries. New regulatory challenges relate to the emerging market structures for low-power or narrow-band networks; competition and abuse of dominance; and universal access to these networks and related services at prices that are affordable for public hospitals and clinics.

Data privacy, trust and security
In the healthcare system, patient confidentiality and the protection of personal information are of equal importance to the potential value generated by gathering and analysing of big data generated through IoT applications. Here, information privacy regulators, cybersecurity regulators and health regulators all have roles to play. Noting that historical health regulations may create barriers to digital transformation in public health, it is necessary to study the health regulatory environment from the perspective of digital advances. Detailed investigation is required on matters that require concurrent jurisdiction, or parallel jurisdiction (discussed further below), by the health professions and the electronic communications sector regulators, as well as on matters that require self-regulation by e-health service providers.

The issues presented in this section 4 offer some perspective on uncertainty, discontinuity and unpredictability with respect to regulatory decision-making in the digitally complex ecosystem.

5. Analysis: Reorienting regulation for the SADC digital ecosystem

Analysis of the emerging SADC digital ecosystem indicates a regulatory environment characterised by uncertainty, unpredictability and discontinuity, one that is in need of complex adaptive responses. Drawing on the points that ensue from the discussion above, at least four key complex adaptive responses are required. First, there is a need for a shift in the regulatory agendas of sector-specific regulators to include attention to the new regulatory challenges discussed here and those discussed by other authors. Second, there is a need for regional regulatory harmonisation. Third, a multiplicity of regulators are engaged in addressing different facets of the regulatory environment for digital services, leading to the requirement to manage and coordinate interwoven regulatory agendas. Fourth, attention must be paid to the greater need for self-regulation – by operators, service providers and consumers – and co-regulatory arrangements.

New regulatory agendas and challenges
It is apparent that SADC regulators must adapt their agendas to include new items in respect of competition, data protection, cybersecurity and cybercrime. SADC countries will also need to establish new regulators, or, where possible, revise the mandates of existing regulators. In this respect, a key role of regional regulatory

AJIC 20-21-Jan-18-22h19.indd 18-19 1/21/2018 10:43:07 PM

bodies is to advance the knowledge required among SADC national regulatory authorities for future-oriented regulation. For example, IoT supply can only advance effectively and productively to meet local and regional demand where regulatory reviews and appropriate, timely *ex ante* regulation are part of the IoT ecosystem. Regulatory studies are required to understand the extent to which existing legislation may provide an initial foundation for conducting reviews and guiding regulatory decisions. In addition, research-based studies must guide how matters such as IoT licensing, data privacy, and cybersecurity will be regulated. This is necessary to inform the practices of regulatory authorities, identify priority areas for attention, and clarify the roles of various regulators and any areas of possible concurrent jurisdiction. It is also necessary to provide clarity for market entrants, for example, with respect to encouraging IoT market formation. In practical terms, the Communications Regulators' Association of Southern Africa (CRASA) can make an important contribution to fostering advances in regulatory agendas and practices for SADC regulators.

Regulatory harmonisation

Important topics for regulatory harmonisation include mobile money and mobile payments; approaches to the formation of IoT markets and services; and the related issues of cyberspace risk and governance. These and other fields of enquiry are knowledge-intensive fields of regulation, requiring the existing SADC regional regulatory associations, CRASA and the CCBG-SADC, to act in ways that further advance the value of model laws, codes and regulatory guidelines. Greater effort is required to promote the establishment of new regulators for data protection and cybersecurity/cybercrime across the SADC region, so as to create the necessary foundations for regulatory harmonisation in this sphere.

Concurrent and parallel jurisdiction

Effective regulation for the future evolution of cyberspace requires the attention of multiple regulators and regional regulatory associations (in, inter alia, banking and finance, competition, consumer protection, cybersecurity, electronic communications, health professions, transport) to advance (i) regulation of mobile money and mobile payments markets; (ii) evolution of IoT markets; (iii) evolution of data analytics and other digital services; and, ultimately to foster (iv) interconnected digital markets across the SADC region. Some matters will require concurrent jurisdiction across regulators, which will in turn require clarification of roles and responsibilities, drafting of memoranda of agreement, and preparation and finalisation of country-level regulations based on model laws or guidelines for regulatory harmonisation.

Creating an ecosystem approach requires more than just concurrent jurisdiction. The converged services of digital financial services and digital healthcare, to give but two of many possible examples, create the need for parallel jurisdiction, with greater

emphasis than before on simultaneous, cross-sectoral, collaborative and, occasionally, integrated regulation with respect to operator behaviour, consumer behaviour, and the behaviour of many service providers (for example, hosts of cloud services, and other unique stakeholders in particular sectors, such as health professionals or e-health service providers). Recognition of parallel jurisdiction means that distinct regulators understand their individual, respective contributions to fostering an effective digital ecosystem, and they seek to create complementarity through their decision-making. They seek to understand each other's contributions and identify where and how to address the gaps arising from the early stages of formulating regulatory decisions for the complex digital ecosystem.

A case in point, at regional level, is the need for a regular interface amongst CRASA, the CCBG-SADC, the COMESA[11] Competition Commission (eight SADC countries are members of COMESA), and the signatories to the SADC Memorandum of Understanding on Inter-Agency Cooperation in Competition Policy, Law and Enforcement (for a brief overview of this MoU, see Ngobese and Kühn, 2017, pp. 3-4). Extended forms of mutual discussion, collaboration, and formulation of formal arrangements for concurrrent and/or parallel jurisdiction among these institutions are necessary to push forward the boundaries of cyberspace for consumers and users of mobile money services in the region.

In the SADC, the number of regulators needing to engage with the broad field of mobile and Internet-based services (read electronic communications, mobile financial services, IoT networks and services, e-health services) would be close to 100 regulators (or more) if each country were to have the types of regulators recommended in model laws and guidelines. These would include banking and financial services regulators (central banks), competition regulators, electronic communications sector regulators, data protection or information privacy regulators, cybersecurity regulators, general consumer rights regulators, health professions regulators, and others. Given the size of the regulatory community and the complexity of its regulatory agenda, the regulatory community itself needs to become a complex adaptive system, as regulators cannot possibly address the range and complexity of issues by applying "tried and tested" regulatory approaches where new innovative approaches are needed.

Self-regulation and co-regulation

Self-regulation is an important field of exploration for SADC policymakers and regulators, in order to encourage greater self-management by operators and service providers, with respect to activities of minimum risk, or areas where self-regulation would remove an unnecessary burden on regulators. Where possible, user communities and provider communities can create and sign up to applicable codes of

11 COMESA is the Common Market for East and Southern Africa.

AJIC 20-21-Jan-18-22h19.indd 20-21 1/21/2018 10:43:07 PM

conduct. Also relevant are co-regulatory approaches, where regulators publish codes of conduct and monitor compliance, a modality that is much less onerous than direct regulation.

6. Conclusions: The complex adaptive system of regulation for the SADC digital economy

This article has sought to introduce a discussion of SADC regulation within a complex digital world. The specific discussion points reflect the uncertainty and unpredictability of the regulatory landscape, and the points of discontinuity with a regulatory history largely focused on the silos of telecoms, or banking, or health services. Over the coming decades, deep structural economic change is inevitable in the SADC region, whether due to endogenous or exogenous influences. Regulators must confront, rather than shy away from, the complexity enshrined in the digital future.

Important considerations for addressing complexity include non-linear thinking (Anderson, 1999; Schneider & Somers, 2006) and non-linear regulatory design; regulatory approaches that understand the digital economy as a complex adaptive system (Akgün, Keskin & Byrne, 2014); and the application of methodologies for studying such systems (Gates, 2016). Non-linear thinking can and should be applied by regulatory organisations in the content of the regulatory agenda and in the design of approaches to regulation. In other words, it may not be possible or advisable to promote continuity in regulatory approaches – such as applying general competition theory to mobile financial services regulation and addressing the traditional issues of dominance and abuse of dominance – where the nature of the regulatory challenges is significantly dissimilar to historical trends or completely new (e.g., the issues of provider-based and agent-based interoperability).

Regulators must consider the best possible regulatory approaches based on the characteristics and relevant factors pertaining to the matter at hand, thinking about regulation as part of shaping the future of systems of communication as an adaptive, interpretive exercise, rather than as simply a rule-driven exercise based solely on past experience and historical trends.

It would be advantageous for SADC regulators to consider each new challenge in relation to its own specific characteristics and influencing factors, rather than to simply look to past regulatory approaches for answers. Regulators can, accordingly, consider the nature of the system changes and innovations taking root, and design regulation that strongly encourages innovation, while balancing the interests of industry development and consumer welfare. Furthermore, regulators will need to consider and adopt particular methodologies for studying complex adaptive systems in the digital sphere, such as STCS evaluation methodologies (Gates, 2016) or research methods for studying virtual communities (Aguirre, 2011), and other

methodologies applicable to regulating in a context of digital complexity.

The article has touched on some of the key emergent regulatory dimensions in this SADC digital complexity ecosystem, in the context of mobile financial services regulation, regulation of IoT networks and services markets, and regulation of e-health services. However, it has not touched on many other important emerging phenomena, notably cloud computing, spectrum management, or issues of the intellectual property rights of entrepreneurs and start-ups in high technology hubs where tech developers and entrepreneurs are engaged in digital innovation and digitally enabled innovation. With respect to these manifestations of digital complexity, additional concerns arise for a future regulatory agenda for the digital services ecosystem. Moreover, it is noted that, beyond regulation, private firms and governments will need to pay attention to factors in the wider enabling environment, including new infrastructure investment, significantly heightened skills development, technology and process innovation, and strategy and leadership relevant to the digital transformation of business, government and civil society. Most importantly, the need for regulation must always be balanced against the need for innovation and investment in this domain. SADC regulators need to take a broad view of the many challenging emerging regulatory issues in their jurisdictions and construct a regulatory agenda that includes in-depth studies of the many new phenomena arising in the digital sphere.

References

Abrahams, L. (2015). Framing the digital complexity economy. Keynote paper delivered at CyberAbuja 2015, the IEEE International Conference on Cyberspace Governance: The Imperative for National and Economic Security, Abuja, 4-7 November 2015, https://doi.10.1109/CYBER-Abuja.2015.7360506

Abrahams, L. (2016). ICT regulation for fostering the digital complexity economy in the SADC region 2016-2030. Unpublished conference paper delivered at the ACER Conference, Livingstone, Zambia, 10-11 March. Retrieved from https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/56f133dff8baf390241b01cc/1458648033943/Luci+Abrahams_ICT+regulation+for+the+digital+complexity+economy+SADC.pdf

African Center for Economic Transformation. (2013). *Growing rapidly – transforming slowly: Preview of the 2013 African transformation report*. Accra: African Center for Economic Transformation (ACET). Retrieved from http://www.thebrokeronline.eu/content/download/56269/504798/version/1/file/ACET+Africa+Transformation+combined+low-res+0524.pdf.

African Development Bank. (2014). *African development report 2014: Regional integration for inclusive growth*. Tunis: African Development Bank. Retrieved from http://www.afdb.org

Aguirre, J. L. (2011). Studying social capital in the new communitarian horizon: A multi-method research strategy. In *Handbook of research on methods and techniques for studying virtual communities: Paradigms and phenomena* (pp. 753-765). Hershey, PA: IGI Global. Available from http://www.igi-global.com/chapter/studying-social-capital-new-communitarian/50374

AJIC 20-21-Jan-18-22h19.indd 22-23 1/21/2018 10:43:07 PM

Airtel Money Malawi. (2017). Airtel Money cross-border transfer. Retrieved from http://www.africa.airtel.com/wps/wcm/connect/AfricaRevamp/malawi/airtel_money/home/airtel-money-cross-border

Airtel Money Tanzania. (2017). Airtel Money tariffs – English (August 2017). Retrieved from http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/Tanzania/Airtel_Money_NEW/Home/Service/Airtel-Money-Tariffs

Akgün, A., Keskin, H., & Byrne, J. (2014). Complex adaptive systems theory and firm product innovativeness. *Journal of Engineering and Technology Management, 31*, 21-42. https://dx.doi.org/10.1016/j.jengtecman.2013.09.003

Anderson, P. (1999). Perspective: Complexity theory and organization science. *Organization Science, 10*(3), 216–232. https://doi.org/10.1287/orsc.10.3.216

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford: Oxford University Press.

Banda, B. (2016). Mobile money: Key competition and regulatory issues in a dynamic sector. Presentation to panel session, 2nd Annual Competition and Economic Regulation (ACER) Week, Southern Africa, Avani Victoria Falls Resort, Livingstone, Zambia, 11-12 March.

Bartoli, A., Hernandez-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2012). *On the ineffectiveness of today's privacy regulations for secure smart city networks*. Washington, DC: Smart Cities Council. Retrieved from https://smartcitiescouncil.com

Basaure, A., Marianov, V., & Paredes, R. (2015). Implications of dynamic spectrum management for regulation. *Telecommunications Policy*, *39*, 563-579. https://doi.org/10.1016/j.telpol.2014.07.001

Bello, O., Opadiji, J., Faruk, N., & Adediran, Y. (2016). Opportunities for universal telecommunication access in rural communities: A case study of 15 rural villages in Nigeria's Kwara State. *The African Journal of Information and Communication (AJIC)*, *17*, 139-163. https://doi.org/10.23962/10539/21625

Blackman, C., & Srivastava, L. (Eds.) (2011). *Telecommunications regulation handbook*. Tenth anniversary edition. Washington, DC: World Bank, infoDev, International Finance Corporation, International Telecommunication Union. Retrieved from https://openknowledge.worldbank.org/handle/10986/13278

Blechman, J. (2016). Mobile credit in Kenya and Tanzania: Emerging regulatory challenges in consumer protection, credit reporting and use of customer transactional data. *The African Journal of Information and Communication (AJIC), 17,* 61-88. https://doi.org/10.23962/10539/21628

Boylaud, O. & Nicoletti, G. (2001). *Regulation, market structure and performance in telecommunications*. Organisation for Economic Co-operation and Development (OECD) Economics Department Working Papers, No. 237. Paris: OECD Publishing. http://dx.doi.org/10.1787/601531871521

Bourreau, M. & Dogan, P. (2004). Service-based vs. facility-based competition in local access networks. *Information Economics and Policy, 16*(2), 287-306. http://dx.doi.org/10.1016/j.infoecopol.2003.05.002

Bourreau, M. & Valletti, T. (2015). *Enabling digital financial inclusion through improvements in competition and interoperability: What works and what doesn't?* CGD Policy Paper 065, Washington DC: Center for Global Development. Retrieved from http://www.cgdev.org

Brown, I. (2015). *Regulation and the Internet of Things*. Discussion paper for the Global Symposium for Regulators. Geneva: ITU. Retrieved from https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf

Buigues, P. (2006). Competition policy versus sector-specific regulation in network industries: The EU experience. Submitted to UNCTAD's 7th Session of the Intergovernmental Group of Experts on Competition Law and Policy. Geneva: UNCTAD. Retrieved from http://unctad.org/sections/wcmu/docs/c2clp_ige7p14_en.pdf

Cave, M. (2017). 40 years on: An account of innovation in the regulation of UK telecommunications, in 3½ chapters. *Telecommunications Policy*, *41*(10), 904-915. https://doi.org/10.1016/j.telpol.2016.10.006

Civerchia, F., Bocchino, S., Salvadori, C., Rossi, E., Maggiani, L. & Petracca, M. (2017). Industrial Internet of Things monitoring solution for advanced predictive maintenance applications, *Journal of Industrial Information Integration, 7*, 4-12. https://doi.org/10.1016/j.jii.2017.02.003

Consultative Group to Assist the Poor (CGAP). (2016). Infographic: Tanzania's mobile money revolution. Retrieved from https://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution

Czernich, N., Falck, O., Kretschmer, T., & Woessman, L. (2011). Broadband infrastructure and economic growth. *The Economic Journal, 121*(552), 505-532. https://dx.doi.org/10.1111/j.1468-0297.2011.02420.x

Di Castri, S. (2014). *Enabling mobile money policies in the Democratic Republic of Congo*. London: GSMA. Retrieved from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/04/Enabling-Mobile-Money-Policies-in-the-Democratic-Republic-Of-Congo.pdf

Disrupt Africa. (2016). *The year in African tech hubs – 2016*. Retrieved from http://disrupt-africa.com/2016/12/the-year-in-african-tech-hubs-2016/

ECA, AfDB Group, & AUC. (2017). *The Africa competitiveness report 2017: Addressing Africa's demographic dividend*. Addis Ababa: Economic Commission for Africa (ECA); Abidjan: African Development Bank Group (AfDB Group), Addis Ababa; African Union Commission (AUC). Retrieved from https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/African_Statistical_Yearbook_2017.pdf

Evans, D. & A. Pirchio. (2015). *An empirical examination of why mobile money schemes ignite in some developing countries but flounder in most*. Coase-Sandor Institute for Law and Economics Working Paper No 723. Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/chigaco%20law%20school%20article%20mobile%20money.pdf

Fanta, A. B., Mutsonziwa, K., Goosen, R., Emanuel, M., & Kettles, N. (2016). *The role of mobile money in financial inclusion in the SADC region: Evidence using Finscope surveys*. Policy research paper No. 3/2016. Midrand, South Africa: FinMark Trust. Retrieved from http://www.finmark.org.za/wp-content/uploads/2016/12/mobile-money-and-financial-inclusion-in-sadc.pdf

FinMark Trust. (2016, March 31). *SADC mobile money guidelines*. Prepared for the Committee of Central Bank Governors in SADC (CCBG-SADC). Midrand, South Africa: FinMark Trust. Retrieved from http://www.finmark.org.za/wp-content/uploads/2017/04/sadc-mobile-money-guidelines.pdf

AJIC 20-21-Jan-18-22h19.indd 24-25 1/21/2018 10:43:07 PM

Fransman, M. (2007). *The new ICT ecosystem: Implications for policy and regulation*. Cambridge, UK: Cambridge University Press.

Fredebeul-Krein, M. & Freytag, A. (1999). The case for a more binding WTO agreement on regulatory principles in telecommunications markets. *Telecommunications Policy, 23*(9) 625-644. https://doi.org/10.1016/S0308-5961(99)00047-6

Galindo-Rueda, F. & Verger, F. (2016). *OECD taxonomy of economic activities based on R&D intensity*. OECD Science, Technology and Industry Working Papers, 2016/04. Paris: OECD Publishing. http://dx.doi.org/10.1787/5jlv73sqqp8r-en

Gartner. (2016). Gartner's 2016 hype cycle for ICT in Africa shows Internet of Things to have the most beneficial impact on local businesses in two to five years. Press release. Retrieved from http://www.gartner.com/newsroom/id/3406118

Gates, E. (2016). Making sense of the emerging conversation in evaluation about systems thinking and complexity science. *Evaluation and Program Planning*, *59*, 62-73. https://doi.org/10.1016/j.evalprogplan.2016.08.004

Gebreab, F. (2002). *Getting connected: Competition and diffusion in African mobile telecommunications markets*. Policy research working paper no. 2863, Washington D.C.: World Bank. Retrieved from http://hdl.handle.net/10986/14261

Gillwald, A. (2005). Good intentions, poor outcomes: Telecommunications reform in South Africa. *Telecommunications Policy, 29*(7), 469-491. https://doi.org/10.1016/j.telpol.2005.05.005

GSM Association (GSMA). (2015a). *The mobile economy: Sub-Saharan Africa 2015*. London. Retrieved from https://gsmaintelligence.com/research/?file=721eb3d4b80a36451202d0473b3c4a63&download

GSMA. (2015b). *State of the industry report: Mobile money*. London. Retrieved from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/04/SOTIR_2015.pdf

GSMA. (2016). *The mobile economy: Africa 2016.* London. Retrieved from http://www.gsma.com/mobileeconomy/africa/

GSMA. (2017). *The mobile economy: Sub-Saharan Africa 2017*. London. Retrieved from https://www.gsma.com/mobileeconomy/sub-saharan-africa-2017/

Hanna, N. (2016). *Mastering digital transformation: Towards a smarter society, economy, city and nation.* Bingley, UK: Emerald.

Haucap, J. (2003). *The economics of mobile telephone regulation*. Discussion Paper No. 4, Department of Economics, University of the Federal Armed Forces, Hamburg. Available at http://www.hsu-hh.de/download-1.5.1.php?brick_id=xlx9yAvk9tT6DYqd

Hawkes, A. (Ed.) (2017). *African.IoT 2017*. Johannesburg: Liquid Telecom Group. Retrieved from http://origin.misc.pagesuite.com/pdfdownload/80c0d4eb-24d0-4bbb-ab23-d066e9f5ee4e.pdf

Hernandez, J., Leza, D., & Ballot-Lena, K. (2010). *ICT regulation in the digital economy*. Discussion Paper for the Global Symposium for Regulators. Geneva: ITU. Retrieved from https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR10/documents/GSR10-ppt2.pdf

Hinde, C., & Van Belle, J-P. (2012). Cloud computing in South African SMMEs: Risks and rewards for playing at altitude. *International Research Journal of Computer Science Engineering and Applications, 1*(1), 32-41. Retrieved from http://www.academia.edu/3036522/Cloud_Computing_in_South_African_SMMEs_Risks_and_Rewards_for_Playing_at_Altitude

Hutchings, A., Smith, R., & James, L. (2013). *Cloud computing for small business: Criminal and security threats and prevention measures*. Trends & Issues in Crime and Criminal Justice No. 456. Canberra: Australian Institute of Criminology. Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi456.pdf

Kelly, T., Mulas, V., Raja, S., Qiang, C., & Williams, M. (2009). What role should governments play in broadband development? Paper prepared for infoDev/OECD workshop on Policy Coherence in ICT for Development, Paris, 10-11 September. Retrieved from http://www.oecd.org/ict/4d/43631862.pdf

Internet World Stats. (2017). Internet user statistics for Africa: Africa Internet usage, 2017 population stats and Facebook subscribers. Retrieved from http://www.internetworldstats.com/stats1.htm

International Telecommunication Union (ITU). (2013a). *Electronic communications and electronic transactions: South African Development Community (SADC) model law*. Geneva. Retrieved from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

ITU. (2013b). *Data protection: South African Development Community (SADC) model law*. Geneva. Retrieved from http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

ITU. (2013c). *Computer crime and cybercrime: South African Development Community (SADC) model law*. Geneva. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

ITU. (2017a). *Measuring the information society report 2017, Volume 1.* Geneva. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

ITU. (2017b). HIPSSA project: Support for the harmonization of the ICT policies in Sub-Saharan Africa. Geneva. Retrieved from http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

Internet World Stats. (2017, June 30). Internet user statistics for Africa: Africa Internet usage, 2017 population stats and Facebook subscribers. Retrieved from http://www.internetworldstats.com/stats1.htm

Jackson, T. (2017, October 30). *SA insurtech startup Naked raises $1.4m*. Disrupt Africa. Retrieved from http://disrupt-africa.com/2017

Krämer, J., & Schnurr, D. (2014). A unified framework for open access regulation of telecommunications infrastructure: Review of the economic literature and policy guidelines. *Telecommunications Policy*, *38*, 1160-1179. https://doi.org/10.1016/j.telpol.2014.06.006

Krämer, J., & Wohlfarth, M. (2017). Market power, regulatory convergence, and the role of data in digital markets. *Telecommunications Policy* (2017). https://doi.org/10.1016/j.telpol.2017.10.004

Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law and Security Review: The International Journal of Technology Law and Practice* (2017). https://doi.org/10.1016/j.clsr.2017.09.002

AJIC 20-21-Jan-18-22h19.indd 26-27 1/21/2018 10:43:07 PM

Lawson, P. (2014). Telecommunications regulation: Creating order and opportunity in UK digital terrestrial television Whitespace. *Computer Law and Security Review*, *30*, 375-391. https://doi.org/10.1016/j.clsr.2014.05.004

Maaref, S. (2012). *Cloud computing in Africa: Situation and perspectives*. Geneva: International Telecommunication Union (ITU). Retrieved from http://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-e.pdf

Matinmikko, M., Latva-aho, M., Ahokangas, P., & Seppänen, V. (2017). On regulations for 5G: Micro licensing for locally operated networks. *Telecommunications Policy* (in press, corrected proof). https://doi.org/10.1016/j.telpol.2017.09.004

Mazer, R., & Rowan, P. (2016). Competition in mobile financial services: Lessons from Kenya and Tanzania. *The African Journal of Information and Communication (AJIC), 17,* 39-59. https://doi.org/10.23962/10539/21629

Moraes do Nascimento, N., & Pereira de Lucena, C. (2017). FIoT: An agent-based framework for self-adaptive and self-organizing applications based on the Internet of Things. *Information Sciences, 378*, 161-176. https://doi.org/10.1016/j.ins.2016.10.031

Nanevie, F. (2012). *The effects of government regulations on the mobile communication telephony in Ghana*. MBA thesis, Institute of Distance Learning, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana. Retrieved from http://ir.knust.edu.gh/bitstream/123456789/4331/1/Frederick%20A.%20Nanevie.pdf

Ndubuaku, M., & Okereafor, D. (2015). State of Internet of Things deployment in Africa and its future: The Nigerian scenario. *The African Journal of Information and Communication, 15*, 114-119. https://doi.org/10.23962/10539/20335

Ngobese, M., & Kühn, A. (2017). Regional competition enforcement: Co-operation between SADC competition authorities in the investigation of cross-border cartels. Retrieved from http://www.compcom.co.za/wp-content/uploads/2017/09/Cooperation-between-agencies-in-the-SADC-region-draft-1.pdf

Namibia University of Science and Technology (NUST). (n.d.) Smart citizen – FABlab Namibia. [YouTube video]. Retrieved from http://fablab.nust.na/?q=all-projects-list#cbp=/?q=project/smart-citizen

Noll, R. (1999). *Telecommunications reform in developing countries*. Working Paper 99-10. AEI-Brookings Joint Center for Regulatory Studies. Retrieved from http://papers.ssrn.com/abstract=181030

Peter, A. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, *17*, 49-59. https://doi.org/10.1016/j.ijcip.2017.03.002

Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy*, *39*, 1-14. https://doi.org/10.1016/j.infoecopol.2017.02.002

Robb, G. , & Vilakazi, T. (2016). Mobile payments markets in Kenya, Tanzania and Zimbabwe: A comparative study of competitive dynamics and outcomes. *The African Journal of Information and Communication (AJIC), 17,* 9-37. https://doi.org/10.23962/10539/21630

Roberts, S. (2016). Mobile money: Key competition and regulatory issues in a dynamic sector. Presentation to panel session, 2nd Annual Competition and Economic Regulation (ACER) Week, Southern Africa. Avani Victoria Falls Resort, Livingstone, Zambia, 11-12 March.

Southern African Development Community (SADC). (1999). Protocol on health in the Southern African Development Community. Retrieved from http://www.sadc.int/files/7413/5292/8365/Protocol_on_Health1999.pdf

SADC BA. (n.d.). SADC BA: Who we are. Web page. Retrieved from http://www.sadcbanking.org/about.aspx

Schneider, M., & Somers, M. (2006). Organizations as complex adaptive systems: Implications of complexity theory for leadership research. *The Leadership Quarterly, 17*, 351-365. https://doi.org/10.1016/j.leaqua.2006.04.006

Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law and Security Review*, *32*, 474-481. https://doi.org/10.1016/j.clsr.2016.02.001

Tanzania Communications Regulatory Authority (TCRA). (2017). Quarterly communications statistics report: April-June 2017 quarter. Dar es Salaam. Retrieved from https://www.tcra.go.tz/images/documents/telecommunication/TelCom-Statistics-June-2017.pdf

Vogelsang, I. (2017). The role of competition and regulation in stimulating innovation – Telecommunications. *Telecommunications Policy* (in press). https://doi.org/10.1016/j.telpol.2016.11.009

World Bank. (2017). *World development report 2016: Digital dividends*. Washington, DC. doi:10.1596/978-1-4648-0671-1

World Economic Forum (WEF). (2017). *The Africa competitiveness report 2017*. Geneva. Retrieved from https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/Africa_Competitiveness_Report_2017.pdf

AJIC 20-21-Jan-18-22h19.indd 28-29 1/21/2018 10:43:08 PM

Development of a First Aid Smartphone App for Use by Untrained Healthcare Workers

Chel-Mari Spies
Junior Lecturer, Department of Computer Systems Engineering, Tshwane University of Technology (TUT), Pretoria

Abdelbaset Khalaf
Senior Lecturer, Department of Computer Systems Engineering, Tshwane University of Technology (TUT), Pretoria

Yskandar Hamam
Professor, Department of Electrical Engineering, Tshwane University of Technology (TUT), Pretoria

Abstract
In the sub-Saharan African context, there is an enormous shortage of healthcare workers, causing communities to experience major deficiencies in basic healthcare. The improvement of basic emergency healthcare can alleviate the lack of assistance to people in emergency situations and improve services to rural communities. The study described in this article, which took place in South Africa, was the first phase of development and testing of an automated clinical decision support system (CDSS) tool for first aid. The aim of the tool, a mobile smartphone app, is that it can assist untrained healthcare workers to deliver basic emergency care to patients who do not have access to, or cannot urgently get to, a medical facility. And the tool seeks to provide assistance that does not require the user to have diagnostic knowledge, i.e., the app guides the diagnostic process as well as the treatment options.

Keywords
first aid, emergency treatment, m-health, smartphone app, clinical decision support system (CDSS), rural healthcare, resuscitation, rule-based algorithms, artificial intelligence (AI), Africa, South Africa

DOI: https://doi.org/10.23962/10539/23577

Recommended citation
Spies, C., Khalaf, A., & Hamam, Y. (2017). Development of a first aid smartphone app for use by untrained healthcare workers. *The African Journal of Information and Communication (AJIC), 20*, 31-47. https://doi.org/10.23962/10539/23577

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

AJIC 20-21-Jan-18-22h19.indd 30-31 1/21/2018 10:43:08 PM

1. Introduction

Medical emergencies are a daily occurrence in human life the world over. More often than not, other people are nearby and the onus of lending a helping hand then falls on them. If these bystanders were trained in first aid, defined as "emergency care or treatment given to an ill or injured person before regular medical aid can be obtained",[1] they would be able to assist with the necessary knowledge and urgency required to meet the needs of the patient.

The British Red Cross reported in 2009 that only 1 in 13 (i.e., only 7.7% of) trained first-aiders in Britain felt comfortable in carrying out first aid (*BBC News*, 2009). If these unsure first-aiders could have something to reassure them, they would more likely be willing to help instead of simply being bystanders.

Companies such as the American Red Cross (2016b), Phoneflips (2015), SusaSoftX (Google Play, 2016a), and St John Ambulance (Google Play, 2016b) have developed first aid applications that run on at least one of the more readily available mobile phone platforms (Android, BlackBerry, and iOS). One characteristic these applications have in common is that their use assumes a certain degree of prior medical knowledge. The user is required to make a diagnosis based on what he/she sees before the application provides steps to be followed in an emergency situation. It is assumed that the user can identify symptoms or diagnose medical conditions. These assumptions limit the efficacy of the applications in line with the limitations of the users' medical expertise. If the user makes an incorrect diagnosis, incorrect treatment will be applied, which may have negative effects on the patient's health.

Even though past research clearly indicates the advantages of training people in first aid, as well as the value of applying correct procedures in first aid situations, there appears to be a gap in the literature regarding research into mobile first aid applications that do not require the user to make diagnosis and instead use the patient's symptoms to guide the user in appropriate and safe assistance.

In the study that is the focus of this article, which took place in South Africa, we developed the prototype of an automated clinical decision support system (CDSS) smartphone app for use by untrained healthcare workers in emergency medical situations, particularly in under-served rural areas. The study aims to achieve the following research objectives:

- to evaluate the WHO IMAI guidelines as basis for algorithm creation and investigate various algorithms for use in the proposed system;
- to investigate and identify the most appropriate software specification(s) to develop an m-health first aid system to be used as a guide in medical emergencies; and

1 See http://www.merriam-webster.com/dictionary/first%20aid

- to verify the validity of the outcomes proposed by the system by comparing its outcomes with the actions of medical professionals.

The article is structured as follows: The next section reviews literature on first aid and communication technology in healthcare (including artificial intelligence and CDSSs), and describes the workings of two existing first aid smartphone apps. Section 3 describes the study: the development, testing, and refinement of of the prototype first aid mobile app. Section 4 provides results from an evaluation questionnaire on the tool, as completed by medical professionals. And Section 5 provides conclusions and future research directions.

2. First aid and the role of communication technologies

According to the St John Ambulance Association's statement about the purpose of first aid, it should (1) preserve life, (2) prevent deterioration, and (3) promote recovery (St John Ambulance, 2016). Two of the many possible examples available in the literature, of cases where bystander first aid was needed, are the following:

- a 17-year-old boy was in a motorcycle accident with no serious injuries, his heart stopped, and no bystander performed CPR, resulting in the boy's death (St John Ambulance, 2010)
- a 4-year-old boy suffered a swimming pool accident and was resuscitated by young, off-duty lifeguards (American Red Cross, 2016a)

Shortages of healthcare workers

It is not only the lack of first aid training and confidence among the general public that poses a risk. There are also significant shortages of healthcare workers in many parts of the world, particularly in developing countries. According to the Global Health Council (GHC, 2011), 15 sub-Saharan African countries do not have the recommended 20 physicians per 100,000 people. These countries have 5 or fewer physicians for every 100,000 people. And 17 sub-Saharan African countries have 50 or fewer nurses for every 100,000 people, far below the recommended minimum of 100 for every 100,000 people.

In South Africa, the "shortage of trained human resources" (Cherry, 2012) was highlighted by the National Health Research Committee at a summit in July 2011 as one of seven possible areas in which healthcare in South Africa can be improved Research shows that nearly 25% of doctors trained in South Africa work in other countries (Gevers, 2011).

The lack of healthcare provided by trained and qualified medical personnel in African countries (*Health-e News*, 2012), particularly in rural areas where access to trained personnel and hospitals or other medical facilities is particularly scarce, poses great risks for the local people. The simple process of symptom recognition and resuscitation can often mean the difference between life and death (Razzak & Kellerman, 2002) if properly, expertly and timeously delivered.

AJIC 20-21-Jan-18-22h19.indd 32-33 1/21/2018 10:43:08 PM

Communication technology in healthcare

e-Health refers to healthcare practices that make use of electronic processes and information and communication technology (ICT) in a cost-effective and secure manner (Hockstein, 2013). Besides use in emergency medicine, other examples of uses for e-health systems include patient treatment, diagnosis, prognosis, image-processing, health management, and health worker education (WHO, n.d.c).

Professionally trained healthcare workers in first world countries at large welcome and adopt the progress and implementation (Shekar, 2012), however, its use across Africa is still minimal. As an example, we can take note of the study done in Nigeria to determine the use of mobile technology in the distribution of reproductive health information (Ezema, 2016), but in contrast to that countries such as Kenya, Uganda and Zambia are eager to try new technologies that support healthcare with an open-mindedness for possible technologies that might have a future common platform (Shekar, 2012). Even with this in mind, the use of e-health technologies in developing countries is not widely accepted. It has been met with scepticism as it is not perceived to have the same personal interaction as would be the experience with a human healthcare worker. In some instances it is seen as a technological replacement of the human factor and only an aid in training and development of healthcare workers, rather than a trusted aid in actual emergency situations (Van Gemert-Pijnen, Wynchank, Covvey, & Ossebaard, 2012).

Mobile technology

In Africa, the number of mobile phone users was 557 million in 2015, and is expected to reach 725 million by 2020 (GSMA, 2016). When considering mobile technology in healthcare, it is noted that key goals are to improve access to, and the quality of, care (Qiang, Yamamichi, Hausman, Miller, & Altman, 2012). Treatment of people in rural areas where there is a great shortage of healthcare workers (Lemaire, 2011) links directly to these goals.

Artificial intelligence (AI)

The use of artificial intelligence (AI) in healthcare has been gaining momentum over the last decade, and while there are human aspects which cannot be replaced by a computer, machines are able to analyse massive amounts of data and recognise patterns that are impossible for humans to detect (Hernandez, 2014). To take a simple example, storing and retrieving medical record details via machines is far more reliable than human mental recollection (Hernandez, 2014). So it is evident that, even though machines are not able to function independently in all scenarios of healthcare, AI does have its rightful place in the healthcare industry.

Clinical decision support systems (CDSSs)

Decision support systems (DSS) are "computerized information system[s] that support decision-making activities" (Power, Sharda, & Burstein, 2015). In the clinical

decision support system (CDSS) context, Perreault and Metzger (1999) state that one of the core functions of a CDSS is to support diagnosis and a treatment plan, and that it should aim to promote "best practices, condition-specific guidelines, and population-based management". By implementing such a system, a healthcare worker can start working independently sooner, allowing for an increase in the number of active healthcare workers in the field. Distinguishable advantages provided by a CDSS include less time spent on training and less mistakes when healthcare worker is unsure about procedures (Van der Walt, 2016).

Existing first aid mobile applications

We now provide a basic comparison between two of the available mobile first aid applications.

St John Ambulance First Aid app

Figures 1 and 2 below shows two screens from the St John Ambulance First Aid app as it existed in mid-2016. The screen in Figure 1 gives the user options on treatments for what the app classifies as "major" emergencies. There are 12 options, 10 of which are available at first glance. The remaining two options can be reached by scrolling down. On the same screen, links can be found to treatment "techniques" (6 sub-sections), "minor" emergencies (6 sub-sections) and "St John Info" (with information on the company, training, calling for help, and tips on a proper first aid kit).

Figures 1 and 2: St John Ambulance (2016b) First Aid mobile app

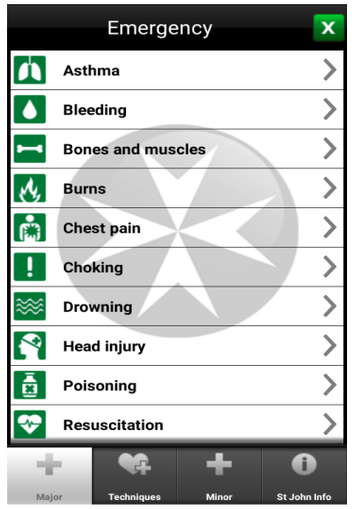


Figure 1: "major" emergencies screen

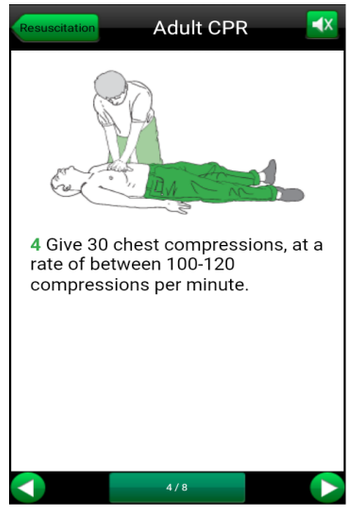


Figure 2: "adult CPR" diagram, with text and audio

AJIC 20-21-Jan-18-22h19.indd 34-35 1/21/2018 10:43:08 PM

The user is expected to decide whether an emergency qualifies as "major" or "minor", and then identify treatments under the "techniques" tab, such as "treating shock", "opening airways" and "recovery position". The initial steps for "assessing the situation" (danger, response, airway, breathing, circulation) are also available under "techniques". Various diagrams are included to make the instructions easy to follow, with the diagrams accompanied by text and audio (as shown in Figure 2).

The St John Ambulance First Aid mobile app is available on the Android, BlackBerry and iOS platforms. No registration is necessary before the application can be used.

Netcare Assist App

Figures 3 and 4 below shows two screens from the Netcare Assist App as it existed in mid-2016. (Netcare is a South African private hospital network). One the home screen, there is a slider button that can be used to call the Netcare emergency line. The user can also document potential "Personal Emergencies", e.g., issues such as asthma or epilepsy can be stated, along with any contact person(s) and contact numbers of whom to call in each instance of occurrence. Figure 3 (the "First Aid" screen) shows a listing of a variety of situations requiring first aid, for which instructions (as per the example in Figure 4) are given.

Figures 3 and 4: Netcare Assist App (Netcare 911 (n.d.))

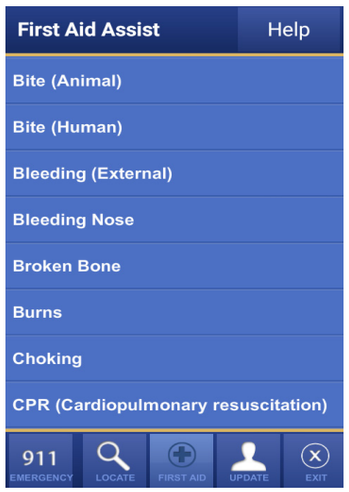


Figure 3: "First Aid" screen



Figure 4: CPR instructions

There are also tabs located along the bottom of every screen, with which the user can navigate to "locate", "first aid", and "update" pages. With "locate", the user can find

the physical location of hospitals, pharmacies, medical centres, and doctors' rooms. On the update page, personal information can be changed and stored. Under "first aid", the user can select from a list of 13 treatments. Each treatment is explained by means of text and pictures, and audio instructions are also available. The application is available for Android, BlackBerry and iOS phones. The user needs to register before the application can be used.

As with the St John Ambulance app, the Netcare app is dependent on the user making a diagnosis before any treatment steps can be requested.

3. The research: Development and testing of a CDSS emergency first aid app

The first core component of our research was development of an automated CDSS tool – an electronic emergency treatment guide app – which can communicate to healthcare workers the procedures and steps to follow in an emergency situation. Our aim was to identify AI protocols similar to protocols applied by healthcare workers during emergency medical assistance and build them into the app, so that such protocols could be imitated by the app.

It must be noted that this study did not include development of an interface to enter patient information and vital readings into the system. For the purpose of this study, that data entry was done manually. Also, a specific database for electronic health records was not developed as part of the study, and data security was not considered. Other parameters decided upon were:

- that there must be provision for limitations found in rural areas (e.g., lack of equipment availability): the tool must not exclude the user from using it if blood pressure cannot be measured at the time; and
- that no patient data would be stored.

Choice of medical guidelines

Various guidelines were considered for this project, and it was ultimately decided that the guide for emergency medical treatment set up by the World Health Organisation (WHO) should be the guidance document. These WHO guidelines are the Integrated Management of Adolescent and Adult Illness (IMAI) Quick Check and Emergency Treatments for Adolescents and Adults (WHO, 2011). The IMAI guidelines are already implemented in more than 30 countries (WHO, n.d.b) and extension to several other countries, including India, China and Vietnam (WHO, n.d.a) was underway at the time of our research. After it was determined that the WHO IMAI guidelines were the most appropriate to use as a foundation for the tool, a basic "decision tree" structure was followed in the development of the tool.

Feedback from validators

Based on recommendations from validators, the IMAI procedure for the treatment of a pneumothorax was revised, and a basic cardio pulmonary resuscitation guidelines were added. Additional recommendations from validators were to: make the display

AJIC 20-21-Jan-18-22h19.indd 36-37 1/21/2018 10:43:09 PM

of emergency and priority signs be more easily readable, e.g., via the use of bulleted points; revise medications to be suited to the South African market; and add diagrams to illustrate the procedures.

The appropriate app model was prototyped, using rules-based algorithms, AI protocols, and ontology modelling.

Selecting a viable testing platform

The two most likely options identified for testing the electronic emergency treatment guide were: 1) to create an application with a database that must be stored on a user's smart device; or 2) to use a web-based platform with a database that the user must connect to in order for it to be used. The advantages and disadvantages of each, and the eventual platform selection, are now discussed.

A smart-device application

The advantage of a smart-device application with a connected database is that no Internet connectivity is needed, but the disadvantages – which, in our analysis, outweigh the advantages – are: that the application must be installed on a device prior to use, and it needs to store information in a database. Also, for testing purposes, the stored database must be retrieved or, in cases where users do not have devices, such devices must be provided to users, and later collected for data to be accessed.

An Internet platform

Advantages of running an Internet application are that the information can be uploaded immediately, and no storage of information is necessary on the user's device, so none of the user's storage space is occupied. Alternatively, if it is a device lent to the user for the means of inputting data, there is no need to retrieve the device at a later stage. The one major drawback of this route is that the user will need Internet connectivity.

Selection of platform

After considering the advantages and disadvantages, the decision was made to use the Google Forms Internet platform to create the emergency treatment guide tool for users to use during the testing of the concept. We determined that the advantages of using Google Forms are that: no website is necessary; no database needs to be created; live updates can be done without having to recall older versions; a full report is generated containing all the options exercised by the user; the report is accessible by the creator in the form of an Excel spreadsheet; a high maximum number of questions (255) is allowed; and an unlimited number of users is allowed.

Stages of development and testing of the tool

We decided on the following stages:

- develop the first version of the tool on the Internet platform;
- conduct field visit to observe trained emergency medical technicians in action, and address shortcomings of the tool;
- enter actual, documented medical emergency cases from literature to test the tool, and address deficiencies;
- have healthcare professionals test the tool and evaluate it by means of a questionnaire, and then make adjustments where necessary;
- have untrained healthcare workers use the tool for data collection purposes; and
- have the inputs from the untrained healthcare workers validated by medical professionals to verify the validity of the tool.

The final two stages just listed were not performed in the first phase that is the subject of this article.

Basic operation of the tool

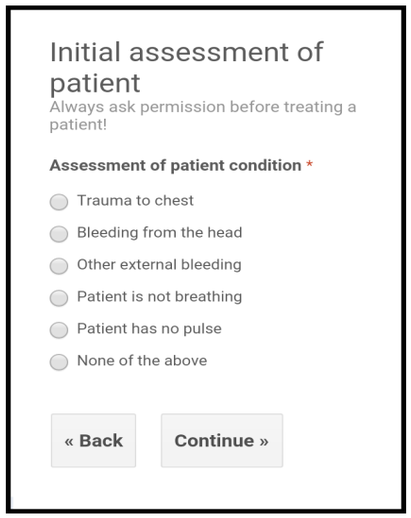
In order to place users into categories according to their qualifications, and thus the medical procedures they could be allowed to perform), the user is first asked to indicate her or his level of qualification. The options are:

- No formal medical training
- First Aid Level 1 or 2 / Medical student
- First Aid Level 3
- Basic Ambulance Assistant / Basic Life Support
- Ambulance Emergency Assistant / Intermediate Life Support
- Emergency Care Technician
- Advanced Life Support / Critical Care Assistant / Emergency Care Practitioner / Nurse / Doctor

By selecting an option, the user is screened and only receives instructions for procedures that she or he is permitted to perform. Once the user is screened, she or he is guided through a series of questions and steps according to her or his choice of answers. After each instruction or question, the user must give an indication that she or he is ready to continue to the next step (or return to the previous step), as shown in Figure 5 below.

AJIC 20-21-Jan-18-22h19.indd 38-39 1/21/2018 10:43:09 PM

Figure 5: Available options and back/continue buttons



The first prompt is for the user to identify any primary symptoms from a list: "trauma to the chest"; "bleeding from the head"; "other external bleeding"; "patient is not breathing"; "patient has no pulse"; or "none of the above". The user must choose the appropriate response in order to receive further instructions relating to that specific condition. If none of the primary signs can be identified, the user is offered the choice of other emergency signs, e.g., "respiratory distress"; "circulation/shock"; "trauma (and neglected trauma)"; "convulsions/unconsciousness". If none of the emergency signs prevail, the user can choose from a list of priority signs, e.g., "pale/fainting/very weak", "bleeding; fracture/deformity.

Refinement of the tool

As development of the app continued, several issues emerged and were addressed. It was decided that the user would give input by means of selecting one or more appropriate options. Checkboxes were initially used in a limited number of questions, but the questions were later revised to allow for radio buttons only. Dropdown lists proved to be too small for handheld devices and as a result were not implemented. The decision was made to keep text input questions to a minimum, due to the limited screen size of certain models of smart devices. Instead of requiring text inputs, the needed information in all but three question was divided into viable sections, such as a range depicting low values, normal values, and high values representing the possibilities. In the app in its current form, the only questions requiring text input are: (1) "enter diastolic blood pressure (lower value) {optional}"; (2) "enter patent's age {optional}"; and (3) "an identification code the health worker assigns to himself/herself". (The third question just listed is one of the six questions included for research data organisation purposes, and all six of these questions will be removed from the final version of the tool.

The manner in which the user is guided, by means of a series of options to select from and instructions based on the options selected, is shown in Figures 6 and 7 below.

Figures 6 and 7: Examples of options and instructions in the tool



Figure 6: Options available to the user

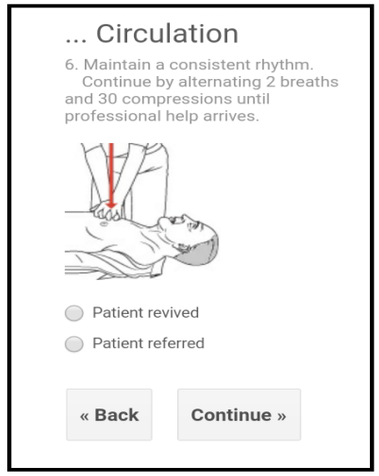


Figure 7: Step-by-step instructions for CPR

Improvements after field visit

A field visit was conducted in order to observe trained paramedics. The major concern expressed was that multiple medical issues might present themselves simultaneously in certain situations, and that, accordingly, there had to be clearer distinctions made in the options given in the tool so that the user can choose, and attend to, the condition that is most threatening. It was thus required that additional options be given throughout the instructional process to allow the user to return to other issues (after treating the most pressing conditions) that need to be addressed before referring the patient to a medical professional or medical facility. It was also noted that verbal permission must be obtained from the patient (if he/she is conscious) before any treatment can be given. An instruction to do so was included in the tool.

Testing of tool against documented cases

A key step in testing of the tool was to use specific documented cases to compare the tool's IMAI-based suggested steps with steps actually followed by medical professionals. We used 20 documented cases for this testing, and after comparing the elements of each procedure, a 69.5% correlation was found between the steps suggested by the tool and the steps actually followed by medical professionals. It was found that:

- the lowest correlation for steps in a single case was 33%;
- the highest correlation for a single case was 100%; and

AJIC 20-21-Jan-18-22h19.indd 40-41 1/21/2018 10:43:09 PM

- the order in which the steps were performed had a 100% correlation across the 20 cases.

However, in the process of entering the 20 cases, some difficulties were encountered. It was noticed that too many unnecessary steps were required to reach certain procedures. (As a result, more options were provided in earlier steps in order to reach said procedures directly.) It was also found that two of the methods for administering medication were too vague. And three instances that called for vital signs to be entered became a "dead-end" if the vitals were not known, e.g., if they couldn't be measured (and those instances thus needed an "unknown" option). These deficiencies were addressed.

It was then decided that more cases, as well as cases of a more diverse nature, should be utilised in order to get a more comprehensive idea of the scope of efficiency of the application. The number of cases drawn from the literature was increased from 20 to 30. It was found that this larger case load, with increased diversity of medical cases, produced a slightly lower correlation than with 20 cases – 65.6% instead of 69.5% – and that:

- the lowest correlation for steps in a single case was 17% (down from 33% when there were 20 cases);
- the highest correlation for a single case was 100%; and
- the order in which the steps were to be performed was matched in 28 of the 30 cases (a 93% correlation, down from the 100% correlation with 20 cases).

Testing by healthcare professionals

The tool was also given to two doctors, three nurses, three emergency medical technicians (EMTs) and two pharmacists, so that they could scrutinise the tool and look for inconsistencies between the tool's information and IMAI guidelines. Feedback was received from two of the doctors, one nurse, and two EMTs. The feedback from the responding professionals called for refinement of approaches provided by the app to: certain medical procedures; restrictions on which medical personnel could form certain procedures; administering of certain medications, certain locally available medications; and provision of appropriate scales for inputting vital signs (instead of having the user type the values). Based on this feedback, the tool was further refined – with the help and input of one doctor (Van Aswegen, 2016) and one EMT (Rossouw, 2016). It was decided that of particular urgency was incorporating limitations into the tool in terms of procedures healthcare workers would be allowed to perform, and these were duly built into the app before any further testing was done.

4. Evaluation survey

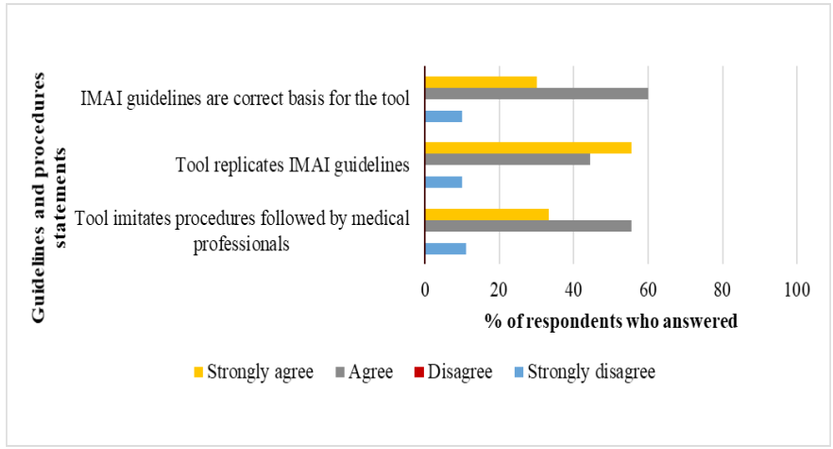
For a more formal method of feedback collection, a questionnaire was drawn up to gather input from medical professionals. The questionnaire was administered

electronically, and feedback from three medical doctors, three EMTs, two pharmacists and one emergency care practitioner (ECP) was received. All the feedback was considered and the tool was adjusted to reflect the recommendations. The core areas of interest in this questionnaire were: the IMAI guidelines; the medical procedures; usability; opinions on assistance offered by the app, efficiency in training, healthcare delivery, and suitability of the tool; security; completeness; participant demographics; and comments on overall perception. The feedback is discussed below.

The tool's guidelines and medical procedures

Figure 8 below shows the survey data from the medical professionals' responses to the questions regarding: (1) the choice of IMAI guidelines as the basis for the guidance provided by the app; (2) whether the app succeeds in replicating the IMAI guidelines; and (3) whether the tool succeeds in imitating the procedures followed by medical professionals.

Figure 8: Survey findings on tool's guidelines and medical procedures

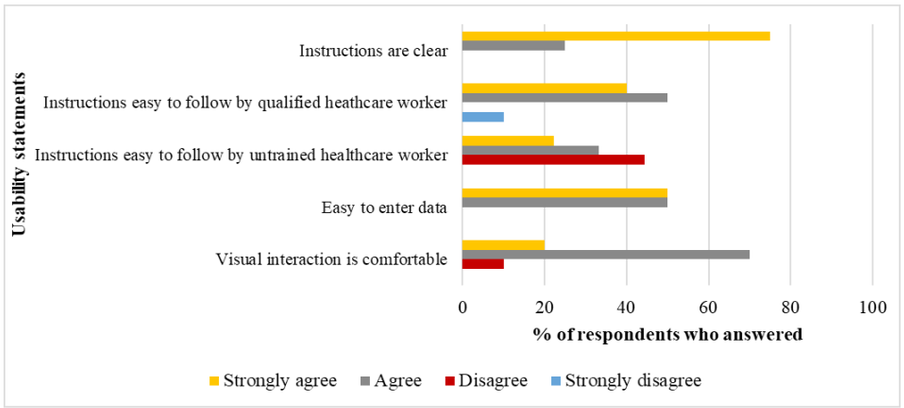


Usability of the tool

Figure 9 below represents the medical professionals' inputs on the usability of the tool, in terms of: (1) clarity of instructions; (2) ease of following instructions for qualified healthcare workers; (3) ease of following the instructions for untrained healthcare workers; (4) ease of data entry; and (5) comfort of visual interaction.

AJIC 20-21-Jan-18-22h19.indd 42-43 1/21/2018 10:43:09 PM

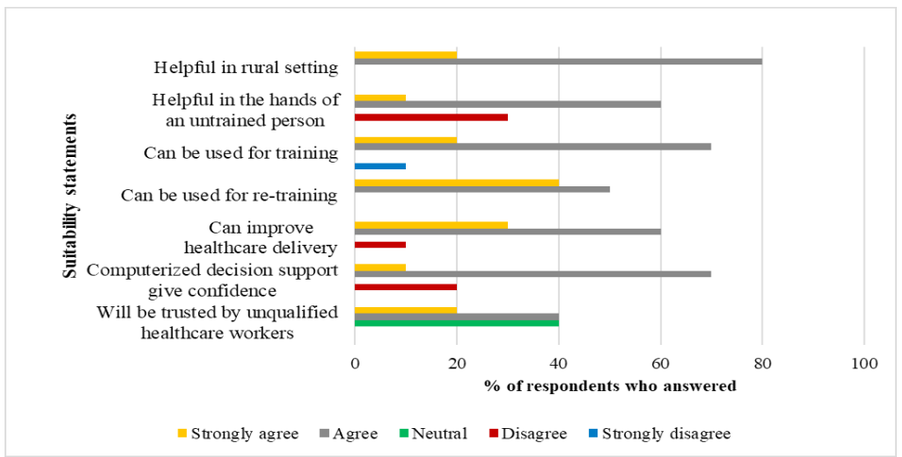
Figure 9: Survey findings on usability of the tool



General opinions on suitability of the tool

Figure 10 shows the opinions of the respondents on the following aspects: (1) the degree to which the tool can be helpful in a rural setting where there are no trained medical professionals nearby; (2) the degree to which the tool can be helpful in the hands of an untrained person; (3) usefulness in training of healthcare workers; (4) usefulness in re-training of healthcare workers; (5) usefulness for improvement of healthcare delivery; (6) enhancement of user confidence via computerised clinical decision support system (CCDS); (7) the trust that an unqualified healthcare worker might place in the outcome proposed by the tool.

Figure 10: General opinions on suitability of the tool



At the general level, the survey found that 90% of the respondents felt the tool was complete and that no additions needed to be made. Among the 10% of respondents who felt additions were needed, suggestions included: addition of diagrams and pictures to assist people in rural areas who may have low levels of English comprehension or be illiterate; revision of clinical procedures in line with the most recent version of the IMAI guidelines. There was also a suggestion that all the CPR instructions be on the same page, instead of the user having to choose "continue" or "back" to move between instructions.

5. Conclusions and future work

The core aims of this initial study were to develop and test the first version of an m-health first aid tool that makes procedural recommendations in response to symptoms – instead of expecting the user to diagnose the patient and treat according to said diagnosis.

In this first phase of testing, relatively good correlations were found between the steps recommended by the tool and the steps taken by medical professionals in documented cases. The tool was refined on the basis of inputs from – and with direct help from – a small group of medical professionals. After refinement of the instrument, a broader survey of medical professionals' views on the tool was performed, and the tool received relatively strong scores in terms of its ability to replicate IMAI guidelines, its ability to imitate the procedures followed by medical professionals, and in terms of usability general suitability matters.

But even after refinement, the tool in its current form is not without limitations. Perhaps the most significant of these limitations is the one alluded to near the end of the previous section: the lack of visual elements such as pictures and diagrams. For the application to be usable by people who are not fluent in English or who even be illiterate, descriptions of procedures, not matter how accurate, will not suffice. This element will be addressed at a later stage. Another likely limitation in use of the tool is that it consumes valuable time to refer to the screen during use, i.e., when actually treating a patient. Inclusion of voice commands may be a positive addition to the final version. Additionally, rollout and convincing people to choose this tool over other smartphone applications may be difficult as it is a new product.

The next phase will be to validate the system against cases in the field. Untrained healthcare workers will have to participate in the study, to test the guidance aspect of the tool. After untrained healthcare workers have entered their responses, the responses will need to be checked by professionally trained medical personnel to confirm the correctness of the actions suggested by the tool. Correlation factors, relevance and accuracy will then be studied to determine the significance of the data and the support lent by the tool. The ultimate goal, after all development and testing are done, is to generate a viable product.

AJIC 20-21-Jan-18-22h19.indd 44-45 1/21/2018 10:43:09 PM

References

American Red Cross. (2016a, February 29). CPR saves: Stories from the Red Cross. Retrieved from http://www.redcross.org/news

American Red Cross. (2016b). First aid – American Red Cross. Android application. Retrieved from https://play.google.com/store/apps/details?id=com.cube.arc.fa

BBC News. (2009, September 10). Many "lacking first aid skills". Retrieved from http://news.bbc.co.uk/2/hi/health/8246912.stm

Cherry, M. (2012). Purposeful support for health research in South Africa. *South African Journal of Science, 108*(5/6), 1. https://doi.org/10.4102/sajs.v108i5/6.1268

Ezema, I. J. (2016). Reproductive health information needs and access among rural women in Nigeria: A study of Nsukka Zone in Enugu State. *The African Journal of Information and Communication (AJIC)*, *18*, 117-133. https://doi.org/10.23962/10539/21788

Gevers, W. (2011). Fleeing the beloved country. *South African Journal of Science, 107* (3/4). https://doi.org/10.4102/sajs.v107i3/4.649

Global Health Council (GHC). (2011). Health care workers. Retrieved from http://globalhealth.ie

Google Play. (2016a). First aid. Retrieved from https://play.google.com/store/apps/details?id=com.max.firstaid

Google Play. (2016b). St John Ambulance first aid. Retrieved from https://play.google.com/store/apps/details?id=an.sc.sja

GSM Association (GSMA). (2016). Number of unique mobile subscribers in Africa surpasses half a billion, finds new GSMA study. Retrieved from https://www.gsma.com/newsroom

Health-e News (2012, July 9). World needs 3.5-m health workers. Retrieved from http://www.health-e.org.za/2012/07/09/world-needs-3-5-m-health-workers

Hernandez, D. (2014, June 2). Artificial intelligence is now telling doctors how to treat you. *Wired*. Retrieved from http://www.wired.com/2014/06/ai-healthcare

Hockstein, E. (2013, Sept. 4). The promise of eHealth in the African region. Press release Retrieved from http://www.afro.who.int/en/media-centre/pressreleases/item/5816-the-promise-of-ehealth-in-the-african-region.html

Lemaire, J. (2011). *Scaling up mobile health elements necessary for the mHealth in developing countries.* Actevis Consulting Group. Retrieved from https://www.k4health.org/sites/default/files/ADA_mHealth%20White%20Paper.pdf

Netcare 911. (n.d.). Netcare apps. Retrieved from http://www.netcare911.co.za/Netcare-Apps

Perreault, L., & Metzger, J. (1999). A pragmatic framework for understanding clinical decision support. *Journal of Healthcare Information Management, 13*(2), 5-21. Retrieved from http://www.openclinical.org/dss.html#perreault

Phoneflips. (2015). Emergency first aid & treatment guide. Retrieved from http://www.phoneflips.com

Power, D. J., Sharda, R., & Burstein, F. (2015). Decision support systems. In Wiley (Ed.), *Wiley encyclopedia of management*. doi: 10.1002/9781118785317.weom070211

Qiang, C.Z., Yamamichi, M., Hausman, V., Miller, R., & Altman, D. (2012). *Mobile applications for the health sector.* World Bank. Retrieved from http://documents.worldbank.org/curated/en/751411468157784302/pdf/726040WP0Box370th0report00Apr020120.pdf

Razzak, L.A. & Kellerman, J.A. (2002). Emergency medical care in developing countries: Is it worthwhile? *Bulletin of the World Health Organization, 80*(11), 900-905.

Rossouw, V. (2016, April 4). Personal communication. Interviewed by C. Spies.

Shekar, M. (2012, June 18). ICTs to transform health in Africa: Can we scale up governance and accountability? Retrieved from http://blogs.worldbank.org/health/print/icts-to-transform-health-in-africa-can-we-scale-up-accountability-in-health-care

St John. (2016a). What is first aid? Retrieved from http://www.stjohn.org.za/First-Aid/First-Aid-Tips

St John Ambulance. (2016b). Free mobile first aid apps. Retrieved from http://www.sja.org.uk/sja/first-aid-advice/free-mobile-first-aid-app.aspx

St John Ambulance. (2010). Dramatic numbers dying from lack of first aid. Retrieved from https://www.sja.org.uk/sja/about-us/latest-news/news-archive/news-stories-from-2010/april/lack-of-first-aid-costs-lives.aspx

Statistics Portal. (2016). *Number of smartphone users sold to end users world wide from 2007 to 2015*. Retrieved from http://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

Van Aswegen, P. (2016, Feb.). Personal communication. Interviewed by C. Spies.

Van der Walt, L. (2016). Mobile decision support system. *South African Journal of Science and Technology, 35*(1), 1409-1410. https://doi.org/10.4102/satnt.v35i1.1409

Van Gemert-Pinjen, J. E. W. C., Wynchank, S., Covvey, H.D. & Ossebaard, H. C. (2012). Improving the credibility of electronic health technologies. *Bulletin of the World Health Organization, 90*(5), 321-400. https://doi.org/10.2471/blt.11.099804

World Health Organisation (WHO). (2011). Quick check and emergency treatments for adolescents and adults. WHO IMAI Project. Retrieved from http://www.who.int/influenza/patient_care/clinical/IMAI_Wall_chart.pdf

WHO. (n.d.a). Countries showcase benefits of scaling up HIV/AIDS services using WHO approach. Retrieved from http://www.who.int/hiv/capacity/IMAI-ICASA/en/

WHO. (n.d.b). How IMAI (and IMCI) support national adaptation and implementation of task shifting. Retrieved from http://www.who.int/hiv/pub/imai/IMAI_IMCI_taskshifting_brochure.pdf

WHO. (n.d.c). eHealth. Retrieved from http://www.who.int/topics/ehealth/en

AJIC 20-21-Jan-18-22h19.indd 46-47 1/21/2018 10:43:10 PM

Development of a Communication Strategy to Reduce Violence against Children in South Africa: A Social-Ecological Approach

Mark Edberg
Associate Professor, Center Director, Milken Institute School of Public Health, The George Washington University, Washington, DC

Hina Shaikh
Director of Program Management and Research Operations, Center for Social Well-Being and Development, Milken Institute School of Public Health, The George Washington University, Washington, DC

Rajiv N Rimal
Professor and Chair, Department of Prevention and Community Health, Milken Institute School of Public Health, The George Washington University, Washington, DC

Rayana Rassool
Communication for Development Specialist, UNICEF South Africa, Pretoria

Mpumelelo Mthembu
Managing Director, Gosiame Research and Marketing, Johannesburg

Abstract
Research on violence against children, though extensive, has not been effectively deployed for the development and tailoring of communication efforts aimed at specific national, local and cultural contexts within which such violence occurs. This article presents a staged, multi-sectoral communication strategy to reduce the incidence of violence against children in South Africa. Drawing on formative data collected through a literature review, key informant interviews, focus groups, and a stakeholder review meeting, the research team, in collaboration with UNICEF South Africa, formulated a communication strategy aimed at combatting violence against children. The data analysis and strategy development within a social-ecological framework sought to identify factors at multiple levels that contribute to violence against children in the South African context. The communication strategy is designed to achieve positive social and behaviour change outcomes in South Africa with respect to the treatment of children, and also to provide an approach as well as specific elements that are potentially replicable to some extent in other countries.

Keywords
violence against children, behaviour change, prevention, South Africa, communication strategy, social-ecological approach

DOI: https://doi.org/10.23962/10539/23576

AJIC 20-21-Jan-18-22h19.indd 48-49 1/21/2018 10:43:10 PM

Recommended citation
Edberg, M., Shaikh, H., Rimal, R. N., Rassool, R., & Mthembu, M. (2017). Development of a communication strategy to reduce violence against children in South Africa: A social-ecological approach. *The African Journal of Information and Communication (AJIC)*, *20*, 49-76. https://doi.org/10.23962/10539/23576



This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

1. The scope of violence against children and gaps in communication approaches to address the issue

Violence against children is a multifaceted problem and globally widespread (UNICEF, 2014). At the same time, the accumulation of research and practice in public health communication has a great deal to contribute in preventing such violence, though it has not yet been applied in any significant way to this issue. Hence, relatively little is known about effective communication approaches for designing, implementing, and evaluating campaigns to address a problem that is at once ubiquitous, hard to define, and often hidden. Our working assumption in this article is that a communication framework can serve as a valuable tool for change in large audiences, as well as for future research. Based on the development of a communication-for-development (C4D) strategy for UNICEF to reduce violence against children in South Africa, we present a communication framework that, we hope, can be adapted for application both in South Africa and in analogous settings. Communication-for-development refers to a broad term employed by United Nations agencies to describe a social process aimed at promoting dialogue within communities and between communities and policymakers, to facilitate the achievement of human development goals (UNDP, 2011).

Violence against children as a global problem

Violence against children manifests in different forms, including physical violence (fatal and non-fatal), sexual violence, exploitation, violent discipline/corporal punishment, emotional violence, neglect and negligent treatment, and bullying, both physical and psychological (UNICEF, 2014; WHO, 2012; Pinheiro, 2006). In 2012, approximately one in five homicide victims worldwide were children and adolescents under the age of 20 (UNICEF, 2014). Moreover, violence against children is commonplace, and it intersects with other factors, including disabilities, ethnicity and gender (UNICEF, 2014; UN, 2014). The problem occurs in numerous settings ranging from the home, schools, work places, communities, institutional care sites, juvenile justice systems, and via the Internet in the form of cyber-bullying (UNICEF, 2014). Social and cultural norms and beliefs, religious imperatives, socioeconomic status, non-existent or weak legislative and enforcement frameworks, and under-reporting are all contributing factors (Pinheiro, 2006; Landers, 2013). Children are also subjected to violence in trafficking, armed conflict (including the exploitation of children by gangs and opposition movements), and by harmful, sometimes fatal, practices such as female genital cutting and child marriage (UN ECOSOC, 2008).

United Nations efforts

In cooperation with host countries, UNICEF has been at the forefront of worldwide efforts to develop and implement a range of approaches to child protection. These efforts, including communication interventions, are grounded in a human rights foundation, based on the 1989 United Nations Convention on the Rights of the Child, and are tied to the following elements: (1) strengthening national protection systems; (2) supporting social change; and (3) promoting child protection in conflict and natural disasters. Crosscutting areas include (1) evidence-building and knowledge management; and (2) convening and catalysing agents of change (UN ECOSOC, 2008).

Other global and UN agencies also have taken on this issue. The prevention of violence against children, particularly gender-based violence, was included in multiple efforts to meet the 2000-2015 Millennium Development Goals (Fehling, Nelson, & Venkatapuram, 2013). The seminal 2002 UN World Health Organisation (WHO) report on violence and health concluded that violence against children and women is a global priority, and called for a public health, science-based approach to complement criminal justice and human rights responses (WHO, 2002). Further, the 2006 UN *World Report on Violence against Children* called on governments to prioritise prevention and allocate sufficient resources to address risk factors and underlying causes (Pinheiro, 2006). WHO continues to advocate for a public health-based, preventive approach to child maltreatment (WHO, 2013). Finally, in pursuit of the global targets set out in the Sustainable Development Goals for 2030, UNICEF promulgated An Agenda for #EVERYChild 2015 in which the first item calls for an end to violence against children (UNICEF, 2015).

Existing research insufficient

A brief summary of relevant research literature is useful as a point of reference, with a caveat that the literature often conflates communication and other types of violence-prevention interventions. Important for the strategy discussed in this article, key factors hindering the effectiveness of interventions to prevent violence against children, including communication efforts, have been knowledge gaps and the implementation of approaches that are not well-tailored for the intended

AJIC 20-21-Jan-18-22h19.indd 50-51 1/21/2018 10:43:10 PM

audience or that lack a sufficient evidence base. Additionally, data suggest there is insufficient dialogue in low- and middle-income country settings between work in early child development and work in violence prevention – dialogue that could help harmonise efforts to address these two intersecting phenomena and balance the current predominance of such research and evidence from high-income countries (UBS Optimus Foundation & WHO, 2013).

Few evidence-based communication or community-based efforts to change the social norms that support violence against children exist, and fewer still are sufficiently tailored to a particular country or community context (UBS Optimus Foundation & WHO, 2013; Fulu, Kerr-Wilson, & Lang, 2014). In fact, a large majority (90%) of studies on violence prevention, early child development, and parenting interventions have been published in high-income countries, specifically, the United States and Canada (Knerr, Gardner, & Cluver, 2011; UBS Optimus Foundation & WHO, 2013). Moreover, a review of a sample of UNICEF country programs showed that data on violence against children are also hampered by "differences in terminology, variations in cultural/social interpretations, and the validity, representativeness and coverage of data, including baseline data which is often absent" (Landers, 2013, pp. 23-24). In short, there is a weak and fragmented evidence base on this important topic (Landis, Williamson, Fry, & Stark, 2013; Bott, 2014).

In addition to the lack of reliable and representative data, evaluations of intervention effectiveness are often flawed and do not even measure decreases in violence as an outcome (Fulu, Kerr-Wilson, & Lang, 2014). Within the spectrum of possible intervention points, programming focused on prevention derives from a stronger evidence base (Bott, 2014). Recent research has recommended that a public health, social-ecological approach through the life cycle be incorporated in developing, monitoring and evaluating efforts to prevent violence against children (Chan, 2013; Fegert & Stötzel, 2016; Sood, 2015; UBS Optimus Foundation & WHO, 2013; Van Niekerk & Makoae, 2014). A social-ecological approach means to identify and address contributing factors that extend beyond the individual, through multiple levels including family, community, and the broader socio-cultural context, drawing on Bronfenbrenner's ecological model of human development (1979) and subsequent public health applications (Stokols, 1992, 1996; see also USCDC, n.d.). Using a social-ecological approach through the life cycle refers to the identification of the multi-level contexts salient at different life stages, and their incorporation in program design and evaluation (see, for example, Edberg et al., 2011).

The UNICEF-sponsored effort to address violence against children in South Africa

This article describes an effort to utilise formative research in the development of a tailored, multi-component, phased strategy as a guide for a UNICEF and government

of South Africa collaborative campaign, using a C4D intervention, to reduce violence against children. Working with UNICEF, the research team conducted a literature review, formative qualitative research, and stakeholder meetings as a foundation for the strategy. The aim was to understand the forms and contexts in which South African children face violence, and to identify specific approaches, channels, and messages – both informational and persuasive – that would be suitable for both national and local communication interventions.

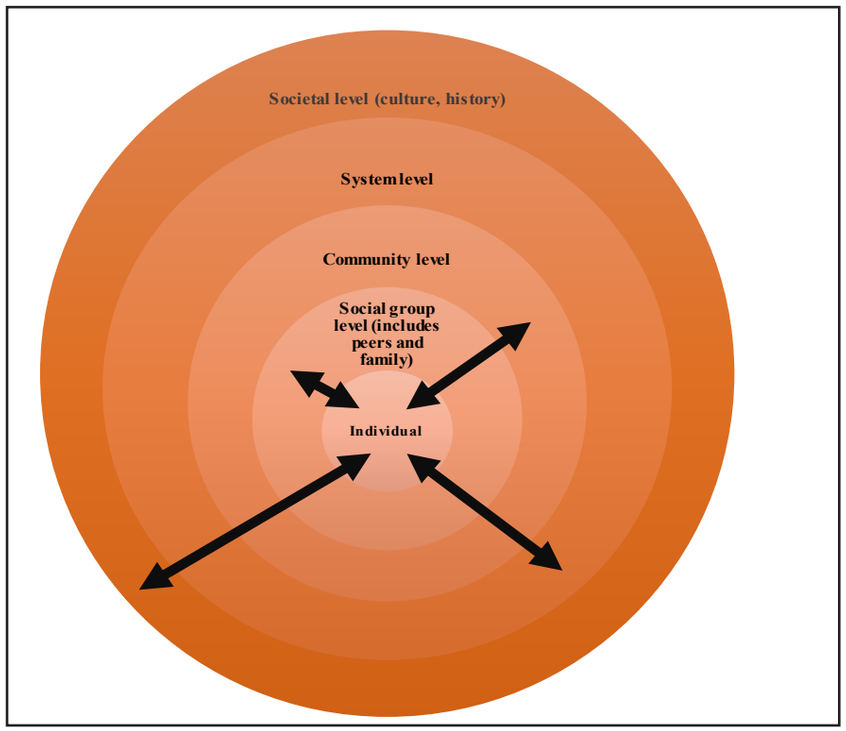
The formative research was oriented around a social-ecological approach (Bronfenbrenner, 1979; Knerr, Gardner, & Cluver, 2011; Stokols, 1992; 1996), in order to identify specific contributing factors at multiple levels that could be included in a communication strategy (Burton, 2012). It was understood during this process that aspects of broader contributing factors in South Africa could be implicated, including the impact of poverty, enduring impacts of apartheid, existing social and cultural norms and practices, the role of social institutions, legal and policy frameworks (and their implementation), and the allocation of resources (UBS Optimus Foundation & WHO, 2013).

The social-ecological framework we used employs two major dimensions: (1) *levels of influence*, moving from the individual out to broader societal factors; and (2) *pathways of influence*, linking factors at one level to those in another, both as a means of understanding causality and of guiding the change process advocated through the communication strategy. Thus, for example, system-level factors – e.g., the lack of capacity and training among child and family serving agencies to address violence victims – have an influence on individual decisions to report violence against children and to seek treatment. As described later in this article, one campaign focus (through a media advocacy component) could therefore be directed to improving these systems, with the assumption that doing so would contribute to changes in individual decisions. Or, if exposure to, and normalisation of violence is a factor that contributes to behavioral norms at the societal, community, family and peer levels, then the campaign should include multiple components at different levels seeking to break the pattern of normalisation.

Figure 1 (next page) illustrates this approach.

AJIC 20-21-Jan-18-22h19.indd 52-53 1/21/2018 10:43:10 PM

Figure 1: Social-ecological levels and pathways of influence



The overall research question guiding the effort was as follows: What kind of C4D strategy would be most effective in combatting violence against children in the South African context, and how would such a strategy be empirically and theoretically grounded?

2. Methods

The proposed communication strategy was developed through an intensive, collaborative research process that included the following steps:

- An extensive literature review that included use of general online search tools, consultation of significant research reports provided by UNICEF and key research institutions (e.g., the University of Cape Town Children's Institute), and specific database searches (e.g., LexisNexis, Google Scholar, PsychINFO, JSTOR, Web of Science, PubMed, Scopus, AnthroSource);
- Meetings and discussions with UNICEF South Africa topical experts;
- Semi-structured interviews with identified local key informants (referred to in this article as expert respondents) to elicit information that would help to understand and inform knowledge gaps in the literature and prioritise those

with respect to project relevance;

- Conduct of four focus group sessions (total n=33) with samples of parents, youth, teachers, and social service practitioners, to gain information on general attitudes, beliefs and experiences concerning the issue of violence against children in South Africa, and feedback on ideas for the communication strategy; and
- A stakeholder meeting in Pretoria, South Africa, that included representatives from media, non-governmental organisations (NGOs), service providers who work with victimised children, government ministries, and UNICEF.

Topical experts and key informants were drawn from the following domains/sectors: experts in child development from South African universities; treatment providers for children who are victims of violence; representatives from South African NGOs that conduct relevant communication efforts; broadcast media organisations; the Department of Social Development; and local NGOs advocating for child rights.

A partner organisation in South Africa specialising in qualitative research conducted the focus group discussions. Participants were recruited using a purposive sampling strategy (Bernard, 2011), working through existing contact networks from our research partner and UNICEF. Collected data were transcribed and then analysed for key themes using QSR International NVivo, qualitative data analysis software for researchers. (A listing of key informant interviews and focus groups is at the conclusion of the References section below.)

Research findings were compiled and used to inform the development of a sequenced communication strategy and its theoretical justification. Relevant stakeholders in South Africa reviewed the draft strategy prior to its finalisation.

3. Findings from the literature review and formative research

Context of child violence in South Africa

Data reviewed in this section are drawn from the literature reviewed and pertinent data collected from the qualitative research, including the key informant interviews and focus groups as a means of triangulation.

Violence against children should be viewed in the context of the broader environment of violence in South Africa. In 2015, based on 2010-2012 data, South Africa was said to have the second-highest rate of gun-related deaths in the world, at 9.4 per 100,000 (*BusinessTech*, 2015). South Africa also ranks high in rates of interpersonal violence and violence against women (DSD, DWCPD, & UNICEF, 2012). Reliable, comprehensive data specifically on violence against children are, however, difficult to come by, thereby hampering a full understanding of the extent of the problem (UNICEF, 2014). In general, violence involving adolescents (typically meaning

AJIC 20-21-Jan-18-22h19.indd 54-55 1/21/2018 10:43:10 PM

children between ages 10 to 19) is often connected to community violence and crime, whereas violence against younger children, age five and under, most typically occurs in the context of family (UCT, n.d.).

There is no one source of comprehensive data; however, multiple sources attest to the widespread nature of violence against children. By one report, 827 children were murdered in South Africa in 2012-13, and 21,575 children were assaulted (Gould, 2014). At the 52 Thuthuzela Care Centres that provide "one-stop" services to victims of sexual assault and rape, for fiscal year 2013-2014, a total of 30,706 matters were reported, of which 2,769 pertained to trafficking, domestic violence or matters governed by the Children's Act of 2005, and the overwhelming balance concerned sexual offences (Department of Justice and Constitutional Development, 2014). The South African Medical Research Council, in an examination of child homicide rates by age, found that the highest risk of death for girls was in the 0-4 age group with a rate of 8.3 per 100,000, while the highest risk of death for boys was in the adolescent 15-17 age group with an alarming rate of 21.7 per 100,000 (Mathews, Abrahams, Jewkes, Martin, & Lombard, 2012). In the 0-4 age group, there was only a 0.7 difference in the homicide rates for girls and boys; however, the overall male child homicide rate was almost double that of the female child homicide rate because of the substantial mortality rate of male adolescents (Mathews et al., 2012).

Child violence in South Africa occurs in multiple settings (Mathews, Jamieson, Lake & Smith, 2014, p. 43; Proudlock, 2014, p. 173). A pilot child death review conducted by the University of Cape Town found that of the children and babies who died in 2009, 44 % were killed in connection with violence (Nicolson, 2015). Corporal punishment appears to be relatively widespread in South Africa, even in schools where it is against the law (Van der Merwe, Dawes, & Ward, 2012). Some sources have indicated that corporal punishment is more prevalent in rural and poorer provinces or areas, with a high degree of continued use found in KwaZulu-Natal Province (Burton & Leoschut, 2013). Traditional practices involving violence against children, such as virginity testing, also appear to be more prevalent in rural than urban areas (Curran & Bonthuys, 2004; UCT, n.d.). Additionally, the World Bank and other sources have identified bullying and cyber-bullying as problems among South African children (Burton, 2012). Supporting the latter assessment, youth in one of the focus group discussions for our research expressed a considerable amount of concern over cyber-bullying, including harassment via the social media platform Instagram. There is also violence directed to specific categories of children, including the disabled, children from immigrant families, street children, and those with HIV/AIDS, as well as evidence of discrimination and violence, in Southern and East Africa, against children with albinism (The African Child Policy Forum, 2014).

Children are victimised not only by adults but also by their peers. One expert respondent from a treatment setting, interviewed during our research, estimated that

as many as 40% of her clients were affected by peer violence. Children as young as age 5, she said, are perpetrators as well as victims. Peer-on-peer violence, according to another NGO expert respondent, also includes sexual abuse. Data show that peer violence in schools ranges from threats of violence and assaults to sexual assaults and robbery (Burton, 2012). A study conducted by South Africa's Centre for the Study of Violence and Reconciliation concluded that peers are significant perpetrators of homicide and rape, with the 15-34 age group comprising 9 out of 12 (75%) of suspects for victims ages 14 and younger, and 42% of rapes committed against children under age 12 (Graham, Bruce, & Perold, 2010). Thus because child violence includes both perpetration and victimisation, against what appears to be a backdrop of normalised violence, a third expert NGO respondent said that there is a shift in thinking, from a conceptualisation of "violence against children" to the notion of "violence in childhood", which is seen as a more adequate description of the situation.

A social ecology of causal factors for violence against children in South Africa

Following the social-ecological approach outlined earlier, we understand violence against children in South Africa as the outcome of multiple, interacting factors. While we cannot detail all the formative evidence herein, the literature review and the qualitative formative research support a general understanding that, at the broader, distal levels, factors include gender norms and the continuing impacts of apartheid on violent behavioural patterns through, among other means, the cultural normalisation of violence (from high exposure), and socioeconomic inequity linked to family fragmentation (Edberg, Shaikh, Thurman, & Rimal, 2015).

At the more proximal levels, the data from the literature and formative research point to substance abuse; community-violence exposure and victimisation; difficult family circumstances and partner violence; school violence (including peer-to-peer violence, in-person or virtual); vulnerability of specific population subgroups including infants, HIV/AIDS orphans, and immigrants; traditional practices such as bride-stealing, virginity testing and circumcision; common cultural practices regarding discipline of children; a lack of capacity by social, health and police services to provide adequate prevention and intervention; and low levels of awareness and trust in these services (Edberg et al., 2015).

Normalisation at multiple levels

One expert respondent described the underlying atmosphere of normalised violence as follows: "People learn violence as a language; it's so ingrained that even before they learn to speak, they learn violence." A youth focus group participant underscored this description, saying that violence "is the only world we know." In a statement issued by the University of Cape Town, a development policy expert was quoted as saying:

> Due to the normalisation of violence in South Africa's past, there is now a widespread tolerance of it. So we need to work very hard to break this cycle. This requires an attitude that preventing violence is everyone's business:

AJIC 20-21-Jan-18-22h19.indd 56-57 1/21/2018 10:43:10 PM

> government, civil society, religious and traditional leaders, communities, caregivers, children, the media… all have a positive role to play in saying no to violence against children. (UCT, 2014, p. 3)

Youth respondents even talked about the normalisation of cyberbullying. The youth who are not bullied "are not taking it serious because it is like you are being desensitised of the whole thing because we [are] growing up watching bullies on TV and everything else so it becomes normal to you." Yet another youth said, "it starts social [social media] and goes to physical."

Causal links between social-ecological levels

Links can be drawn between the distal and proximal levels of causation. Respondents in focus group discussions with social workers and parents, for example, pointed to family breakdown and poverty, and their association with substance abuse and family violence, as a syndrome correlated with violence against children, particularly neglect and lack of protection. For instance, one respondent noted, "[Violence] is also linked to the social economic conditions in South Africa as a whole. Because socially the family structures are really destroyed in our country." This was echoed by another respondent stating, "Yes, [family structures are] almost non-existent." Economic factors also play a role, as a third respondent expressed, "[M]ost of the parents are not working. In the morning they go to drink. Sit in there drinking the whole day. They don't care about the children. And they [are] angry and frustrated and the first person that is suffering are the children when they get home." There also was a link made to a general breakdown in cultural values, including a change from collective to more individualistic relationships.

Moreover, at the family level, the normalisation of violence is embedded in traditional childrearing practices. In some contexts, parents and teachers do not see corporal punishment as constituting abuse. According to one service-provider focus group respondent, "Children need to be disciplined but because not all parent[s] know the difference between discipline and abuse[,] we should teach parents that there are other ways to discipline your children. You know, let them stand in a corner, you know. Withhold certain treats." Physical discipline is customary in certain South African contexts, and to move towards changing this practice, parent respondents suggested that allowing parents who practice corporal punishment to get more exposure to the practices of parents who do not use such punishment, along with exposure to positive messages, would be useful. Some parent respondents also cited the usefulness of support from other community members when, for example, there are many single-parent households in a community. At the same time, there were concerns expressed about the potential for loss of authority over children in the absence of the sanction of corporal punishment.

At the government level, there is a substantial body of law that protects and promotes child rights. Despite this strong legal foundation, there are multiple barriers through

lower social-ecological levels, including the community and family levels, with respect to implementation. Enforcement remains weak across national and provincial government departments, with respect to both prevention of violence against children and adequate response to incidents of such violence (Proudlock, 2014). Moreover, the social context is complex; child abuse cases may entail complicity by families, the police and other services (Richter & Dawes, 2008).

South African C4D efforts to address violence against children

South Africa has a rich media environment, and government, private and non-profit media organisations have been involved in initiatives to address interpersonal violence and raise public awareness of the negative impacts of violence, including violence against children. Government-sponsored efforts include the annual 16 Days of Activism for No Violence against Women and Children campaign; Child Protection Week, hosted by the Department of Social Development (DSD) since 1998; and participation in the UN's UNiTE to End Violence against Women campaign (DSD, DWCPD, & UNICEF, 2012). The South African Integrated National Programme of Action Addressing Violence against Women and Children (2013-2018) includes, as a key objective, a call to "prevent violence from occurring through a sustained strategy for transforming attitudes, practices and behaviours" (DSD, 2014, p. 25).

A number of NGOs in South Africa have implemented public communication campaigns to address violence against both children and women. Perhaps the most notable and widely recognised efforts are those conducted by the Soul City Institute for Social Justice (Soul City Institute), based in Johannesburg. Soul City employs an "edutainment" or "infotainment" approach, harnessing popular culture and communication via mass media in an effort to bring about social change through entertainment delivery modes. Soul City activities have included dramatic soap-opera style ("soapie") TV series, radio programmes, and accompanying print materials, including a series focusing on alcohol and violence (*Phuza Wise*); the *Kwanda* ("to grow") reality TV show focused on community mobilisation and improvement; and the *Soul Buddyz* television and multimedia series aimed at promoting health and well-being among children aged 8-12.

Resources Aimed at the Prevention of Child Abuse (RAPCAN) is a South African NGO engaged in activities to help address violence against children, including some communication interventions directed at parents, educators and communities, and some advocacy to end corporal punishment. Another South African NGO, Sonke Gender Justice, focuses on HIV/AIDS issues and sexual and reproductive health rights, and has implemented advocacy campaigns aimed at promoting child rights, including community mobilisation and media campaigns in partnership with Promundo to increase men's involvement in nonviolent parenting (Sonke Gender Justice, n.d.). The loveLife NGO primarily addresses HIV prevention among youth, and tis work intersects with child violence issues because of its focus on broader

AJIC 20-21-Jan-18-22h19.indd 58-59 1/21/2018 10:43:11 PM

social determinants of risk. Research shows, for example, that childhood sexual and physical abuse contributes to later, HIV-transmission-causing sexual risk behaviour and victimisation through early sexual initiation, unprotected sex, and use of alcohol and drugs during sexual activity (Richter et al., 2014). The loveLife programme's initiatives have included peer educator programmes, media campaigns, local community dialogues, and a Cyber Y programme for youth that combines computer literacy training with information about healthy sexuality and lifestyle choices.

There is not yet a sufficient body of evidence assessing the effectiveness of specific C4D initiatives in preventing and responding to violence against children in South Africa. For example, reports summarising two of the primary public awareness activities, DSD's Child Protection Week and the 16 Days of Activism for No Violence against Women and Children campaign, do not include any measurement or evaluation of effectiveness (Van Niekerk & Makoae, 2014). And according to the *South African Child Gauge 2014*, "statistics on reported violence against children have not reduced substantially in the past two decades" (Van Niekerk & Makoae, 2014, p. 38).

While not extensive, there have been some evaluations of the effectiveness of Soul City's C4D efforts, with evidence found of positive attitude change regarding the acceptability of violence (Soul City Institute, n.d., 2011). Soul City deploys a variety of measurement methods, including quantitative baseline and follow-up surveys, and some qualitative data (Soul City Institute, 2016). An evaluation of a Soul City intervention to address domestic violence found a 14 % increase in agreement with a statement that no woman deserves to be beaten, and the same percentage increase in awareness about a national helpline connecting Soul City audiences to assistance for domestic violence (Hillis et al., 2015; Usdin, Scheepers, Goldstein, & Japhet, 2005). The intervention also correlated with a shift in attitudes, showing a 10% increase in respondents disagreeing that domestic violence was a private affair (Usdin et al., 2005). Soul City evaluations assessing some of its multimedia programs that include youth as a target audience show increases in HIV/AIDS knowledge and condom use among youth (Soul City Institute, 2016). There is also some evidence of impact among youth of loveLife programmes (Peltzer & Chirinda, 2014). In addition, outside South Africa, there is evidence that communication programmes have decreased the acceptability of violence against intimate partners and children (Promundo, 2012).

It bears noting that some of Soul City's evaluation documents appear to be incomplete. For example, a 2007 evaluation report on a health promotion intervention involving multimedia components cited a nationally representative sample of approximately 1,500 people interviewed over three consecutive years; however, outcome measurement and reporting focused only on a one-year sample (Soul City Institute, 2007).

4. Social-ecological analysis underlying the communications strategy to address violence against children

Theoretical basis

The formative research identified both broad, distal contributing factors (e.g., behavioural legacy of apartheid), as well as more proximal factors at the levels of institutions, communities, families, and individuals, that contribute to violence against children in South Africa. The broader factors identified tend to be historically and societally embedded and thus likely slow to change, while some of the proximal factors would likely be conducive to shorter-term change. Accordingly, we, along with the rest of the research team, concluded that a communication effort would need to operate at multiple levels (i.e., follow a social-ecological approach), and be staged (i.e., progress through several stages and target population levels) to be effective and optimise the best combination of campaign components.

It should also be noted that the formative data suggested the need for stages even at the highly proximal, individual-factor level. For example, a parent might receive or hear information regarding the use of non-violent disciplinary practices. Yet if parents perceive these practices to be normative (in part due to cultural traditions, in part because of the general normalisation of violence as documented in the formative research), the information would likely need to be strengthened by follow-up (i.e., staged) components employing social support and modeling from other parents to translate the information into action.

Multiple social and behaviour change theories support a staged communication strategy. As an overall framework, we drew on the premise of the trans-theoretical model (Prochaska & DiClemente, 1983; Prochaska, Redding, & Evers, 2002) that behaviour change is a staged process, not a single event. Implied is the idea that addressing readiness to change must be included as part of in the behaviour change process, and that messages and strategies need to be tailored to a succession of change stages and their differing requirements. Second is diffusion of innovations theory (Rogers, 1995), which characterises the adoption of a new behaviour or technology as occurring through stages within a diffusion context that includes the social and cultural environment, and can be facilitated via change agents. Third is social cognitive theory (Bandura, 1986; 2001), focusing on the person-environment interaction as a mechanism for change, in which individual change is facilitated by behavioural models, skill-building, social support, and positive reinforcement from one's social environment, leading to greater behavioural self-efficacy. Linked to this is social support theory (House, 1981; Berkman & Glass, 2000), focusing on the importance of several types of social support to reinforce behaviour change.

Fifth is a set of communications-related theories, in particular social marketing/branding theory and media advocacy theory. Social marketing/branding theory

AJIC 20-21-Jan-18-22h19.indd 60-61 1/21/2018 10:43:11 PM

(Evans et al., 2011; Hecht & Lee, 2008; Kotler, Roberto & Lee, 2002) likens the adoption of behaviour to adoption or purchase of a product. The marketing task involves linking the behaviour to desirable attributes that would enhance its attractiveness, such that the behaviour represents those attributes, as in a "brand". Media advocacy theory (Dorfman & Krasnow, 2014; Wallack, 1994) focuses on the use of media techniques for agenda-setting and public policy change. Finally, we drew on cultural theory (summarised in Edberg, 2013, as it pertains to health), which emphasises the embedded nature of behaviour, such that a behaviour cannot be considered or addressed outside the socio-cultural context that gives it meaning and value, and that in turn contributes to constraints and facilitators concerning specific behavioural options.

Based on the data collection and analysis, we have outlined below a framework and approach for a staged communication strategy. Each phase of the strategy draws on descriptive and causal data based on the formative research, and is linked to one or more of the theoretical perspectives outlined herein, depending upon the message content and target audience(s) for that phase. For example, the broad media campaign provided in phase one is intended to introduce and frame a coherent message about violence against children. For this purpose, branding theory is pertinent, as the goal is to establish a unified identity for the campaign. In phase three, on the other hand, the goal is to provide social support and models to facilitate individual behaviour change; thus social support theory and social cognitive theory are relevant in structuring the communication activities in that phase. And, in keeping with a social-ecological approach, the communication strategy assumes that the environment for behaviour change – specifically in this case, the social, legal and health service infrastructure, as well as political commitment – must also evolve in order to facilitate successful actions by individuals and groups.

Objectives implemented through a staged process

It is our view that a communications campaign addressing violence against children for South Africa as a whole cannot effectively target, as its primary end, broad distal factors such as the legacy of apartheid and continuing economic inequality, because these factors underlie multiple phenomena and could therefore obscure the clarity of the intended behavioural change goal. This is not to say, however, that these factors are not significant, and it is part of the central problematic addressed in this communication strategy to target the normalisation of violence and the behavioural implications of that normalisation that are consequences of that legacy. This is a key theme underlying sample campaign activities at multiple levels described below. Beyond that, the strategy seeks to identify motivators of change, facilitators of change, as well as facilitators of sustainable change, and to integrate these into a coordinated programme of action.

The overall behavioural goal is to reduce the incidence of violence against children. A communication campaign, however, constitutes only part of the process of reaching that goal, and must be integrated with a comprehensive undertaking that includes the implementation of adequate policies and regulations, law enforcement, prevention programming, and treatment services. Thus, the overall goal is to influence knowledge, attitudes, practices, and the supportive environment so that violence against children is not viewed as normal, but as harmful and antithetical to personal aspirations in a changing South Africa progressing beyond the legacy of apartheid as a broad background motivation, and to motivate and persuade multiple audiences in a movement to change behaviour over time through a series of coordinated stages addressing more proximal factors.

Specific campaign objectives are based on promoting behaviour change as a staged process (per our theoretical framework), in which members of the target populations: (1) first become more aware of violence against children and its negative consequences, and understand personal efficacy in avoiding the proscribed behaviour; (2) then come to value and associate a reduction in violence against children with personal and South African progress (the brand); 3) are then motivated and socially supported by the linking of the behaviour change to a *social movement* that is a positive alternative from which they are more likely to experience valued outcomes; (4) are individually supported through instruction messages, modeling and positive reinforcement regarding how to change the risky behaviour; and (5) are then further supported in maintaining the positive behaviour over time by improvement in the service infrastructure.

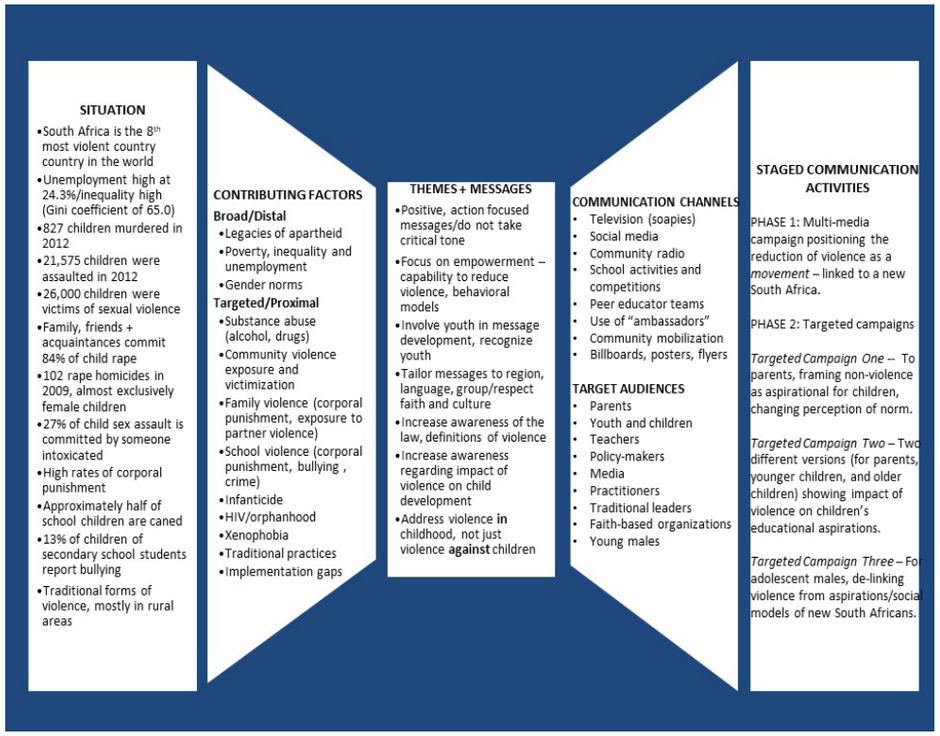
Our formative data were used to identify not only causal factors, but also communication channels, themes, messages and activity types were used to develop the strategy. Communication activities under the strategy would be conducted as needed in English, Afrikaans, Zulu, Sotho, and Xhosa, and – for community radio and community action teams – the language(s) appropriate to the specific audience.

5. Results of the analysis: A phased communication strategy to address violence against children at multiple social-ecological levels

Figure 2 (next page) illustrates the overall flow from causal factors to themes/ messages, communications channels, and target audiences, and then to campaign activities.

AJIC 20-21-Jan-18-22h19.indd 62-63 1/21/2018 10:43:11 PM

Figure 2: C4D strategies addressing violence against children: Continuum from causal factors to communication



Based on our analysis, the following represents an example of a hypothetical, staged C4D campaign that could be implemented via a collaborative engagement by UNICEF and the South African government, and at a community level, to empower NGOs, schools, and private businesses or organisations, and sustain campaign initiatives. The campaign description provided is an overview, with objectives, target audiences, key themes and messages, communications channels, activities, and potential evaluation approaches for each phase. Importantly, it is designed to address contributing factors at the multiple social-ecological levels described thus far, in a coordinated sequence.

Phase one: Establishing a campaign brand and addressing societal-level factors

The intent of a first campaign phase (estimated duration of one and a half years) is to address the normalisation of violence, a key causal factor in the social-ecological spectrum outlined thus far, and to introduce an agenda that reframes violence through a branding process. Moreover, normalisation of violence permeates multiple levels, and is broadly associated with South Africa's past. Thus a reframing effort through branding would seek to *link the reduction of violence against children to future aspirations*. As part of that objective, the first phase needs to increase awareness that violence against children is harmful and antithetical to individuals, families, schools and communities in a changing South Africa. Three aims follow from this objective: (1) clarify the definition of violence so that target populations understand what is at issue; (2) brand the *reduction of violence against children as aspirational*, empowering, and forward thinking; and (3) frame the reduction of violence against children as a social movement in order to facilitate collective action by multiple groups. Target audiences are the general population, including youth, parents, educators, and community leaders because the objective is to address a broad societal-level theme.

This phase includes an important definitional element that supports the ability of individuals, particularly in a family context, to recognise violent behavior. The definitional aspect of this phase could employ communication strategies that include the presentation of scenarios depicting violence against children with taglines such as "This is not love. This is violence." A tagline with this message would be an attempt to address, as documented in the formative research, the normalisation in South Africa of violent discipline and its consideration as a time-honored method to regulate children's behaviour. This family-level message should be linked to the broader social context, as a foundational theme tying a reduction of violence against children to a new South Africa, intended to impart a positive and aspirational "brand identity" to reducing violence, instead of a critical or negative tone (a point emphasised by stakeholders). Importantly, this theme would best be positioned as the goal of a "movement" – a social action form that is familiar and popular in South Africa, according to stakeholders who provided feedback on the proposed strategy – and as a goal that requires collective action. The theme would seek to position youth, parents, and community leaders as agents of change.

Because broader themes are involved that do not target a specific demographic or community, we concluded that the objectives of phase one would be best accomplished through a coordinated mass media campaign together with social mobilisation. As the kickoff and "agenda-setting" phase, we consider it important that this phase engage all possible communications channels, including: (1) major media, through public service announcements (PSAs) linked to highly popular television programming, including Soul City's "infotainment" initiatives and in collaboration with national media organisations; (2) social media, via platforms like Facebook, Twitter, Instagram, and Snapchat; (3) community radio in each province; (4) public events, specifically, the global 16 Days of Activism for No Violence against Women and Children campaign and National Child Protection Week, both led by the South African government; (5) youth action, through song competitions, creative arts, the formation of change agent teams or working with existing teams (e.g., loveLife peer educator teams), and social media; and (6) print materials, such as billboards, bumper stickers or posters with the theme/slogan, and textiles, such as t-shirts, hats, rubber bracelets and reusable bags.

AJIC 20-21-Jan-18-22h19.indd 64-65 1/21/2018 10:43:11 PM

Sample activities to implement this phase include: (1) coordinating the launch of the overall campaign with media and events, which could include a large launch day music concert with celebrity appearances; (2) incorporating this theme in the DSD-sponsored 16 Days of Activism and National Child Protection Week annual campaign; (3) developing radio segments or PSAs that can be adapted and translated by community radio stations; (4) holding a contest among high schools, technical schools, and colleges to develop a campaign logo; (5) holding a contest to develop theme music with the winner recording at a major studio with a known musical artist (e.g., Mafikizolo, Mi Casa, Miss Lira, Zahara); (6) with respect to community mobilisation, providing materials and training to new or existing teams or groups; and (7) launching a national, celebrity-driven social media campaign with designated hashtags. Recent successful examples include #62milliongirls and #ALSicebucketchallenge.

Phase two: Initiating individual change

While phase one focuses on awareness, motivation and ideational change regarding violence against children, phase two moves the change process forward by linking these changes to actions. Thus the overall phase two objective is to provide specific message instruction concerning alternatives to the use of violence, per the change mechanisms from social cognitive theory (Bandura, 2001, 1986) and diffusion of innovations (Rogers, 1995), and to address gaps in personal knowledge and self-efficacy identified through our conduct of formative research. Following the theoretical logic and formative input, the authors determined that phase two objectives would best be accomplished through a continuation of the mass media messages combined with targeted and culturally tailored media outputs (e.g., soapies, community radio, community theatre, print materials, and community action teams) that help people learn how to implement behaviour change in their real-world situations. Phase two activities are directed to parents, teachers, and youth.

Supported by social cognitive and diffusion of innovations theories, the focus of messages in this second phase is on social models, skills and confidence building. For parents, this part of the campaign includes models for how to encourage and maintain good behaviour in children without use of violence, and alternatives for handling family conflicts without violence. Similarly, teachers will see behavioural models of non-violent classroom control. For youth, the messages may be more complex. To mitigate bullying, youth will see models of how to intervene safely, as seen, for example, in programs like Breakthrough's *Bell Bajao!* (meaning "ring the bell" in Hindi) multimedia campaign in India (Silliman, n.d.). For youth, the strategy is to present examples of how to earn respect, and to have influence in their communities and schools without violence.

This phase would be implemented (over an estimated time of 18-months) through multiple channels, in collaboration with local NGOs, social services and health care providers, and high school or college theater/social justice programs, such as the Drama for Life programme at University of the Witwatersrand. Service providers such as the Teddy Bear Clinic may have existing parent training materials that could be employed to disseminate specific information on the prevention of violence against children. Sample activities in this phase could include: (1) developing and broadcasting content-appropriate soapies; (2) collaborating with national and community radio to participate in coordinated, tailored programming; (3) engaging youth through social media to promote and disseminate specific messages about how to reduce violence against children, and engaging performing arts and theater groups for the same purpose; (4) developing street theater productions to model solutions and raise awareness (e.g., City at Peace model in the United States); and (5) developing an action plan and materials with guidance on violence against children behaviour change for community action teams, and for distribution via social services and health care providers. The PSAs with the primary campaign theme would be maintained for continuing reinforcement.

Phase three: Engage social support systems

Phase two focused on the dissemination of models and guides for individual behaviour change supported by broad campaign themes. However, for individuals to actually make changes in behaviour, additional social facilitators are often necessary. Thus the objective of the third phase is to facilitate adoption of the behaviour change through the engagement of social support, using group and social mobilisation strategies. Following social support theory change mechanisms (House, 1981; Berkman & Glass, 2000), the authors, with stakeholder input, determined that this objective is most effectively accomplished through the use of community action teams, support from community leaders, youth peer action, teacher training, teacher support networks, and parent groups. Target audiences include parents, teachers, youth, traditional and faith leaders. Phase three is proposed to last one year, overlapping with the last six months of phase two.

The focus of messages in this phase is on social reinforcement for behaviour change. For example, parents' motivation to change would be strengthened by support from other parents and traditional or faith leaders, reinforcing the message that behaviour change garners approval, and that there are social support systems that can provide advice on how to implement and maintain change. In an interpersonal, concrete way, this also can help reinforce the reduction of violence as normative. Teachers will benefit from support as well, coming from other teachers and educational administrators. Behaviour change among youth is facilitated by support from adults in their social and family networks and from peers, though it has been well documented that social support has to be engaged carefully with adolescents (Reininger, Perez, Aguirre Flores, Chen, & Rahbar, 2012), as it can have both positive and negative effects.

AJIC 20-21-Jan-18-22h19.indd 66-67 1/21/2018 10:43:11 PM

Sample activities and communication channels to implement this phase include: (1) developing and broadcasting of new soapies focusing on social support themes, and radio programming (regional, community radio) that, for example, features a school that changes its approach to discipline, the way in which its teachers are supported by their colleagues and school administrators, and the positive outcomes that result; (2) organising community-based activities and support groups for parents hosted by faith organisations, civic organisations, and social services; (3) working with local and national journalists to foreground the issue on the national agenda, through special editions and op-ed features that highlight resources available for parents, youth, and others; (4) generating social media activities with the purpose of building social support for behaviour change; and (5) continued distribution of print materials (behaviour change guidance) through social services and health care providers as a means of reinforcement. For youth, the interpersonal activities could be organised through school clubs, civic organisations, and sports and arts activities. For teachers, such activities could be organised through teachers unions or at school or district levels. Again, PSAs with the primary campaign theme would be continued for ongoing reinforcement.

Phase four: Facilitate sustained change

The key objective of the fourth phase (estimated implementation of one year overlapping with the last six months of phase three) is to facilitate maintenance of the behaviour change by advocating for resources and services through, for example, law enforcement, social services, school-based services, and youth gang interventions. Maintenance is typically the last stage of change processes outlined, for example, in the trans-theoretical model (Prochaska & DiClemente, 1983; Prochaska, Redding, & Evers, 2002). The authors, with stakeholders' review in South Africa, concluded that the fourth objective is best accomplished through media advocacy (Dorfman & Krasnow, 2014; Wallack, 1994), youth action, and community-level engagement, and that it will require the long-term allocation of resources. Key target audiences are the media, policy leaders and decision-makers.

The focus of messages in this phase is advocacy for increased attention and resources allotted to the kinds of services that are necessary to support and sustain behaviour changes made by individuals. These services include child protection, family counseling, and law enforcement. The messages should center on the idea that movement forward cannot take place without everyone on board (a theme underscored in stakeholder input), and that policies are not enough without the capacity to carry them out.

Sample activities and channels to implement this phase include: (1) developing and publishing opinion pieces for broadcast and print media; (2) supporting radio programming that highlights capacity and resource needs; (3) engaging social media to create demand for better services and awareness of the service gaps; (4) mobilising community and youth groups to stage events and speak before policymaking bodies and individual stakeholders to advocate for and influence relevant policymaking; and (5) continuing television PSAs carrying the primary campaign theme, at selected intervals for reinforcement.

Campaign outcomes and impacts: Outline of monitoring and evaluation

In general, monitoring and evaluation would entail collaboration with a university or research institution (e.g., the University of Cape Town's Children's Institute) for the conduct of a baseline survey (national sample) prior to the campaign, in order to assess: (1) how violence against children is defined; (2) self-reported behaviour; (3) level of intent to change violence against children; (4) level of concern about violence against children; (5) awareness of or involvement with any community mobilisation activities; and (6) individual as well as collective efficacy with respect to changing cultural norms and perceptions that support violence against children. Once the campaign is initiated, follow-up surveys, with measures of campaign activity exposure, would be implemented at six months and one year, followed by two additional one-year follow-ups. The goal of follow-up data collection would be to evaluate change in these same dimensions, moderated by measures of campaign *reach* – the degree to which messages and activities were received by/involved participation of target audience members.

In each phase, monitoring would focus on assessment of reach; for example, the recording of activities implemented and programs aired, and tracking, by phase, the number of participants in activities as well as materials (e.g., posters, op-ed pieces) distributed or published. If possible, focus groups should be conducted with a sample of parents, youth, teachers, and practitioners to obtain more extensive information on adoption of the theme, attitude and behaviour change, and on barriers and facilitators of change.

6. Conclusions and practical implications

The proposed communication strategy is an attempt to develop a grounded and theory-based plan for engaging in a phased behaviour change promotion effort, using multiple communication channels tailored to a national and local context. It is also an attempt to develop a strategy with a social-ecological orientation, in which the factors influencing behaviour change are understood to occur, and interact, at multiple levels, from the individual out to the social environment.

Our research began with the premise that mediated communication campaigns aimed at addressing social/health problems, such as the societal problem of violence against children, are often not optimally tailored to the complex of factors facilitating violence in the local or regional setting, are not tied to a theory-informed model of change, and are not comprehensively evaluated. In the hypothetical strategy outlined above, we have made a concerted effort to develop a coherent approach that includes

AJIC 20-21-Jan-18-22h19.indd 68-69 1/21/2018 10:43:12 PM

these often-missing elements, while at the same time being mindful of resource constraints. It is our hope that the strategy provides a model that can help to fill gaps in existing practice with respect to reducing violence against children.

Implementation and replication

The strategy is oriented to a South African context. However, the basic framework, process, and at least some of the content, may have relevance for the development of campaigns in other countries. Key replicable elements of the strategy could include the staged process, the logic behind that process, and the theoretical justification. In terms of content, replicable elements could include the general strategy of branding a reduction of violence as a focus of national progress, the movement from awareness and motivation to specific social support mechanisms for effecting behaviour change, and the targeting of factors within the social environment (e.g., access to and quality of services, training, implementation of protective legal frameworks that may already be in place) that need to change in order to facilitate individual and institutional change.

Limitations and key features of the proposed strategy

It is a limitation of the work presented here that, because of the time and resources available to conduct the formative research and develop a strategy, we were not able to address all necessary issues. We collected data regarding normative definitions of violence, and we included in the communication strategy elements that are intended to promote change in the prevalence of attitudes accepting harsh physical discipline of children (at home and at school), as well as norms for masculinity in the South African context that foster violence. The strategy seeks to address awareness gaps about the negative outcomes that can occur by these attitudes and practices. Similarly, we sought to address prevalent attitudes and expectations about the "normality" of community violence to which children are exposed, as perpetrators and victims. The normalisation of violence was one of the themes that arose frequently in our formative research, often linked to disruptions in family structure and the legacy of apartheid.

In connecting the various campaign activities to the theme of a South Africa moving beyond that legacy, we also addressed, to some degree, normative definitions regarding a "good child" – the teleology of childrearing. The communication campaign outlined herein takes on that issue by disseminating, through campaign branding, new expectations and norms regarding the level of violence acceptable for children within a changing South Africa. For example, in a township historically plagued by community and family violence, we heard from respondents that violence was understood as the means to power and access to resources. Thus, raising a child who understands that role of violence and can function accordingly might have been viewed as maintaining a positive behavior. In this campaign, we aim to alter this by linking personal and societal progress to a change in that kind of belief and associated childrearing goals, so that an attitudinal or behavioral effect is achieved because such

change is perceived as a valued outcome.

However, because of resource and time constraints, we were not able to address some of the other aspects of violence against children specific to the South African context that did arise in the formative research. Our suggested campaign does not, for example, address violence against migrant children, against children who are victims of HIV/AIDS (directly, or as orphans), against disabled children, or against children with certain physical conditions such as albinism. We did also not include campaign components addressing certain gender-based violence practices, such as virginity testing. These issues could perhaps best be addressed by focused campaigns rather than the broader effort proposed in this article.

References

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology, 52*, 1-26. https://doi.org/10.1146/annurev.psych.52.1.1

Berkman, L. F., & Glass, T. (2000). Social integration, social networks, social support, and health. In L. F. Berkman, & I. Kawachi (Eds.), *Social epidemiology* (pp. 137–173). New York: Oxford University Press.

Bernard, H. R. (2011). *Research methods in anthropology: Qualitative and quantitative approaches* (5th ed.). Lanham, MD: Altamira Press.

Bott, S. (2013). *From research to action: Advancing prevention and response to violence against children: Report on the Global Violence against Children Meeting*. Retrieved from https://www.unicef.org/protection/files/Swaziland_Global_VAC_Meeting_Report.pdf

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design*. Cambridge, MA: Harvard University Press.

Burton, P. (2012). *Country assessment on youth violence, policy and programmes in South Africa.* Washington, DC: Social Development Department, World Bank. Retrieved from http://documents.worldbank.org/curated/en/2012/06/16461732/country-assessment-youth-violence-policy-programmes-south-africa

Burton, P., & Leoschut, L. (2013). *School violence in South Africa: Results of the 2012 national school violence study.* Cape Town: Centre for Justice and Crime Prevention. Retrieved from http://www.cjcp.org.za/uploads/2/7/8/4/27845461/monograph12-school-violence-in-south_africa.pdf

BusinessTech. (2015, June 22). South Africa is the second worst country in the world for gun deaths. Retrieved from http://businesstech.co.za/news/government/91284/south-africa-is-the-second-worstcountry-for-gun-deaths-in-the-world/

Chan, M. (2013). Linking child survival and child development for health, equity, and sustainable development. *The Lancet, 381*(9877), 1514-1515. https://doi.org/10.1016/s0140-6736(13)60944-7

Curran, E., & Bonthuys, E. (2004). *Customary law and domestic violence in rural South African communities.* Johannesburg: Centre for the Study of Violence and Reconciliation. Retrieved from http://www.csvr.org.za/wits/papers/papclaw.htm

AJIC 20-21-Jan-18-22h19.indd 70-71 1/21/2018 10:43:12 PM

Department of Justice and Constitutional Development. (2014, December 8). Keynote address by the Deputy Minister of Justice and Constitutional Development, the Hon. John Jeffery, MP, at 4th African Conference on Sexual and Gender Based Violence. Retrieved from http://www.justice.gov.za/m_speeches/2014/20141208_GenderSummit.html#sthash.c4ClyFl8.dpuf

Department of Social Development (DSD). (2014). *South African integrated programme of action addressing violence against women and children (2013-2018)*. Pretoria. Retrieved from http://www.dsd.gov.za

DSD, Department of Women, Children and People with Disabilities (DWCPD), & UNICEF. (2012). *Violence against children in South Africa.* Pretoria. Retrieved from http://www.cjcp.org.za/uploads/2/7/8/4/27845461/vac_final_summary_low_res.pdf

Dorfman, L., & Krasnow, I. D. (2014). Public health and media advocacy. *Annual Review of Public Health, 35*, 293-306. https://doi.org/10.1146/annurev-publhealth-032013-182503

Edberg, M., Shaikh, H., Thurman, S., & Rimal, R. (2015). *Background literature on violence against children in South Africa: Foundation for a phased communications for development (C4D) strategy.* Washington, DC: Center for Social Well-Being and Development, for UNICEF South Africa.

Edberg, M. (2013). *Essentials of health, culture and diversity: Understanding people, reducing disparities.* Burlington, MA: Jones & Bartlett Learning.

Edberg, M., Chambers, C., & Shaw, D. (2011). *The situation analysis of children and women in Belize 2011: An ecological review.* Government of Belize and UNICEF Belize. Retrieved from http://www.unicef.org/sitan/files/SitAn_Belize_July_2011.pdf

Evans, W. D., Longfield, K., Shekhar, N., Rabemanatsoa, A., Snider, J., & Reerink, I. (2011). Social marketing and condom promotion in Madagascar: A case study in brand equity research. In R. Obregon, & S. Waisboard (Eds.), *The handbook of global health communication* (pp. 330-347). New York: Wiley.

Fegert, J., & Stötzel, M. (2016). Child protection: A universal concern and a permanent challenge in the field of child and adolescent mental health. *Child and Adolescent Psychiatry and Mental Health, 10*, 18. https://doi.org/10.1186/s13034-016-0106-7

Fehling, M., Nelson, B. D., & Venkatapuram, S. (2013). Limitations of the Millennium Development Goals: A literature review. *Global Public Health, 8*(10), 1109-1122. https://doi.org /10.1080/17441692.2013.845676

Fulu, E., Kerr-Wilson, A., & Lang, J. (2014). *What works to prevent violence against women and girls? Evidence review of interventions to prevent violence against women and girls*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/337615/evidence-review-interventions-F.pdf

Gould, C. (2014, September 17). Comment: Why is crime and violence so high in South Africa? Retrieved from https://africacheck.org/2014/09/17/comment-why-is-crime-and-violence-so-high-in-south-africa-2/

Graham, L., Bruce, D., & Perold, H. (2010). *Ending the age of marginal majority – an exploration of strategies to overcome youth exclusion, vulnerability and violence in Southern Africa*. Retrieved from http://www.southernafricatrust.org/docs/Youth_violence_civic_engagement_SADC_2010-Full.pdf

Hecht, M. L., & Lee, J. K. (2008). Branding through cultural grounding: The Keepin' it REAL curriculum. In W.D. Evans, & G. Hastings (Eds.), *Public health branding: Applying marketing for social change* (pp. 161-179). Oxford: Oxford University Press.

Hillis, S. D., Mercy, J. A., Saul, J., Gleckel, J., Abad, N., & Kress, H. (2015). *THRIVES: A global technical package to prevent violence against children*. Atlanta: US Centers for Disease Control and Prevention.

House, J. S. (1981). *Work stress and social support*. Reading, MA: Addison-Wesley.

Knerr, W., Gardner, F., & Cluver, L. (2011). *Parenting and the prevention of child maltreatment in low- and middle-income countries: A systematic review of interventions and a discussion of prevention of the risks of future violent behaviour among boys*. Pretoria: Sexual Violence Research Initiative, Medical Research Council. Retrieved from http://www.svri.org/sites/default/files/attachments/2016-04-13/parenting.pdf

Kotler, P., Roberto, N., & Lee, N. (2002). *Social marketing: Improving the quality of life* (2nd ed.). Thousand Oaks, CA: Sage.

Landers, C. (2013). *Preventing and responding to violence, abuse, and neglect in early childhood – a technical background document*. Retrieved from http://www.unicef.org/protection/files/Report_on_preventing_and_responding_to_violence_in_early_childhood_2013_Cassie_Landers.pdf

Landis, D., Williamson, K., Fry, D., & Stark, L. (2013). *Measuring violence against children in humanitarian settings: A scoping exercise of methods and tools.* New York and London: Child Protection in Crisis (CPC) Network and Save the Children UK.

Mathews, S., Abrahams, N., Jewkes, R., Martin, L. J., & Lombard, C. (2012). *Child homicide patterns in South Africa: Is there a link to child abuse?* South African Medical Research Council Research Brief. Retrieved from http://www.mrc.ac.za/policybriefs/childhomicide.pdf

Mathews, S., Jamieson, L., Lake, L. & Smith, C. (Eds.). (2014). *South African child gauge 2014*. Children's Institute, University of Cape Town. Retrieved from http://www.ci.org.za/depts/ci/pubs/pdf/general/gauge2014/ChildGauge2014.pdf

Nicolson, G. (2015, July 13). Analysis: The gruesome truth about child deaths in South Africa. *Daily Maverick*. Retrieved from http://www.dailymaverick.co.za/article/2015-07-13-analysis-the-gruesome-truth-about-child-deaths-in-south-africa/#.Vawx9mC3nar

Peltzer, K., & Chirinda, W. (2014). Access to opportunities and the Lovelife programme among youth in South Africa. *Journal of Psychology in Africa 23*(1), 77-84. https://doi.org/10.1080/14330237.2013.10820596

Pinheiro, P. S. (2006). *World report on violence against children*. Geneva: UNICEF. Retrieved from http://www.unicef.org/lac/full_tex%283%29.pdf

Prochaska, J. O., & DiClemente, C. C. (1983). Stages and processes of self-change of smoking: toward an integrative model of change. *Journal of Consulting and Clinical Psychology, 51*, 390-395. https://doi.org/10.1037//0022-006X.51.3.390

Prochaska, J. O., Redding, C. A., & Evers, K. E. (2002). The transtheoretical model and stages of change. In K. Glanz, B. K. Rimer, & F. M. Lewis (Eds.), *Health behavior and health education* (3rd ed.). San Francisco: John Wiley & Sons.

Promundo. (2012). *Engaging men to prevent gender-based violence: A multi-country intervention and impact evaluation study.* Washington, DC. Retrieved from http://promundoglobal.org/resources/engaging-men-to-prevent-gender-based- violence-a-multi-country-intervention-and-impact-evaluation-study/

AJIC 20-21-Jan-18-22h19.indd 72-73 1/21/2018 10:43:12 PM

Proudlock, P. (Ed.) (2014). *South Africa's progress in realising children's rights: A law review*. Cape Town: Children's Institute, University of Cape Town, and Save the Children South Africa. Retrieved from http://ci.org.za/depts/ci/pubs/pdf/researchreports/2014/Realising_childrens_rights_law_review_2014.pdf

Reininger, B. M., Perez, A., Aguirre Flores, M. I., Chen, Z., & Rahbar, M. H. (2012). Perceptions of social support, empowerment, and youth risk behaviors. *Journal of Primary Prevention*, *33*(1): 33–46. https://doi.org/10.1007/s10935-012-0260-5

Richter, L. M., & Dawes, A. R. L. (2008). Child abuse in South Africa: Rights and wrongs. *Child Abuse Review, 17*, 79-93. https://doi.org/10.1002/car.1004

Richter, L., Komárek, A., Desmond, C., Celentano, D., Morin, S., Sweat, M., … Coates, T. (2014). Reported physical and sexual abuse in childhood and adult HIV risk behaviour in three African countries: Findings from Project Accept (HPTN-043). *AIDS and Behavior*, *18*(2), 381–389. https://doi.org/10.1007/s10461-013-0439-7

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York: Free Press.

Silliman, J. (n.d.). *Breakthrough's Bell Bajao! A campaign to bring domestic violence to a halt*. Retrieved from http://www.breakthrough.tv

Sonke Gender Justice. (n.d.). *Children's rights and positive parenting (CRPP) portfolio*. Retrieved from http://www.genderjustice.org.za

Sood, S. (2015). *Violence against children (VAC) – a systematic review of C4D approaches*. Retrieved from https://www.nationalacademies.org

Soul City Institute. (n.d.). *Soul Buddyz* series. Retrieved from http://www.soulcity.org.za/research/evaluations/series/soul-buddyz-series

Soul City Institute. (2007). *A summary report of the research by Markdata October 2007 - HIV/AIDS impacts of Soul City Series 7*. Retrieved from http://www.soulcity.org.za/research/evaluations/series/soul-city/soul-city-its-real-evaluation-report-2007/evaluation-report-2007

Soul City Institute. (2011). *Kwanda report 2011*. Retrieved from http://www.soulcity.org.za/research/evaluations/kwanda/Kwanda%20Report.pdf/view

Soul City Institute. (2016). *Evaluations of the different Soul City programmes*. Retrieved from http://www.soulcity.org.za/research/evaluations

Stokols, D. (1992). Establishing and maintaining healthy environments – toward a social ecology of health promotion. *American Psychologist, 47*(1), 6-22. https://doi.org/doi/10.1037/0003-066X.47.1.6

Stokols, D. (1996). Translating social ecological theory into guidelines for community health promotion. *American Journal of Health Promotion, 10*, 282-298. https://doi.org/10.4278/0890-1171-10.4.282

The African Child Policy Forum. (2014). *The African report on violence against children*. Addis Ababa. Retrieved from http://srsg.violenceagainstchildren.org/sites/default/files/publications_final/african_report_on_vac/african_report_on_violence_against_children_2014.pdf

UBS Optimus Foundation & World Health Organisation (WHO). (2013). *ECD+ workshop preceding the WHO's 6th milestones in the global campaign for violence prevention meeting*. Retrieved from http://www.who.int

UNICEF. (n.d.). MODULE 1: Understanding the social ecological model (SEM) and communication for development (C4D). Retrieved from https://www.unicef.org

UNICEF. (2014). *Hidden in plain sight: A statistical analysis of violence against children* Retrieved from http://www.unicef.org/publications/index_74865.html

UNICEF. (2015). *A post-2015 world fit for children*. Retrieved from http://www.unicef.org/agenda2030/files/P2015_issue_brief_set.pdf

University of Cape Town (UCT). (n.d.). *Towards a more comprehensive understanding of the direct and indirect determinants of violence against children in South Africa with a view to enhancing violence prevention: Critical literature review.* Unpublished manuscript. Cape Town: University of Cape Town.

UCT. (2014). Preventing violence against children: Break the intergenerational cycle. Press release. Retrieved from https://www.uct.ac.za/usr/press/2014/Preventing%20violence%20against%20children.pdf

UN. (2014). *The road to dignity by 2030: Ending poverty, transforming all lives and protecting the planet*. Retrieved from http://www.un.org/disabilities/documents/reports/SG_Synthesis_Report_Road_to_Dignity_by_2030.pdf

UN Development Programme (UNDP). (2011). Communication for development – strengthening the effectiveness of the United Nations. Retrieved from http://www.undp.org/content/undp/en/home/librarypage/democratic-governance/civic_engagement/c4d-effectivenessofun.html

UN Economic and Social Council (UN ECOSOC). (2008). *UNICEF child protection strategy*. E/ICEF/2008/5/Rev.1. Retrieved from http://www.unicef.org/protection/CP_Strategy_English(1).pdf

US Centers for Disease Control and Prevention (USCDC). (n.d.). The social-ecological model: A framework for prevention. Retrieved from https://www.cdc.gov/violenceprevention/overview/social-ecologicalmodel.html

Usdin, S., Scheepers, E., Goldstein, S., & Japhet, G. (2005). Achieving social change on gender-based violence: A report on the impact evaluation of Soul City's fourth series. *Social Science & Medicine*, *61*(11), 2434-2445. https://doi.org/10.1016/j.socscimed.2005.04.035

Van der Merwe, A., Dawes, A., & Ward, C. (2012). The development of youth violence: An ecological understanding. In C. Ward, A. Van der Merwe, & A. Dawes (Eds.), *Youth violence: Sources and solutions in South Africa.* Cape Town: University of Cape Town Press.

Van Niekerk, J. M., & Makoae, M. (2014). The prevention of violence against children: Creating a common understanding. In S. Mathews, L. Jamieson, L. Lake, & C. Smith, (Eds.). *South African child gauge 2014* (pp. 35-42). Cape Town: Children's Institute, University of Cape Town. Retrieved from https://www.researchgate.net/publication/282769760_The_prevention_of_violence_against_children

Wallack, L. (1994). Media advocacy: A strategy for empowering people and communities. *Journal of Public Health, 15*(4), 420-436. https://doi.org/10.1177/109019819602300303

World Health Organisation (WHO). (2002). *World report on violence and health: Summary*. Geneva. Retrieved from http://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf

WHO. (2012). *Sexual violence – understanding and addressing violence against women*. Information Sheet WHO/RHR/12.37. Retrieved from http://www.who.int/reproductivehealth/publications/violence/rhr12_37/en

WHO. (2013). *European report on preventing child maltreatment*. Retrieved from http://www.euro.who.int/__data/assets/pdf_file/0019/217018/European-Report-on-Preventing-Child-Maltreatment.pdf?ua=1

AJIC 20-21-Jan-18-22h19.indd 74-75 1/21/2018 10:43:12 PM

Key informant interviews (conducted via Skype or telephone)

Centre for Justice and Crime Prevention interviewee, Cape Town, 20 August 2015

Childline South Africa interviewee, Durban, 26 August 2015

Child Rights and Positive Parenting Portfolio and MenCare Global Fatherhood Campaign interviewee, Sonke Gender Justice, Johannesburg, 24 August 2015

Children's Radio Foundation interviewee, Cape Town, 31 July 2015

Directorate of Social Cohesion and Gender Equity in Education interviewee, Department of Basic Education, Pretoria, 13 August 2015

Psychology Department interviewee, University of Cape Town, 27 August 2015

Radio 2000 interviewee, Johannesburg, 4 August 2015

Soul City Institute for Health and Development Communication interviewee, Johannesburg, 17 August 2015

Teddy Bear Clinic for Abused Children interviewee, Johannesburg, 5 August 2015

Focus group discussions (recruited via convenience sampling). All focus groups conducted at the facilities of JDI Research in Johannesburg

Parents focus group, 31 August 2015

Practitioners focus group (e.g., police officers, social workers, NGO personnel), 1 September 2015

Teachers focus group, 31 August 2015

Youth focus group, 1 September 2015

FOCUS SECTION ON CYBERSECURITY

AJIC 20-21-Jan-18-22h19.indd 76-77 1/21/2018 10:43:13 PM

Guest Editor's Introduction: *AJIC* Focus Section on Cybersecurity

Kiru Pillay
Visiting Researcher, LINK Centre, University of the Witwatersrand (Wits), Johannesburg; and Chief Director, Cybersecurity Operations, Department of Telecommunications and Postal Services, Pretoria

Abstract
This introduction to the *AJIC* Focus Section on Cybersecurity provides the context for the section, introduces the three articles, and establishes the importance of ongoing emperical research in support of policy and strategy in the cybersecurity domain.

Keywords
cybersecurity, cybersecurity policy, cyber-threats, cybersecurity awareness (CSA), cybersecurity research, developing world, Africa, South Africa

DOI: https://doi.org/10.23962/10539/23575

Recommended citation
Pillay, K. (2017). Guest editor's introduction: *AJIC* focus section on cybersecurity. *The African Journal of Information and Communication (AJIC)*, *20*, 79-82. https://doi.org/10.23962/10539/23575

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

AJIC 20-21-Jan-18-22h19.indd 78-79 1/21/2018 10:43:13 PM

1. The widening range of cyber-threats

The imperative for developing countries to deploy information and communication technologies (ICTs) and the Internet as effective tools to redress historical challenges and inequalities is well understood by governments, nowhere more so than in Africa. ICTs and the Internet are seen as the essential channels to deliver a wide range of basic services and applications. This adoption of ICTs and the Internet into all aspects of everyday life has engendered emergence of what we refer to, in a favourable light, as information societies and knowledge economies.

However, the growth of such societies and economies is accompanied by new and serious threats. While technological advancement introduces greater variety and convenience into our lives, it also opens more and more avenues for people to be targeted by threat actors, who increasingly view public- and private-sector organisations – and individual citizens – as attractive targets for a range of cyber-threats.

Attacks against information infrastructure and Internet services are now commonplace, and 2017, in particular, has seen a large number of global incidents and data breaches. These attacks have placed the spotlight firmly on how governments are taking up the challenge of securing information systems, critical infrastructure and citizen's information, while at the same time building confidence in the ability to use the Internet to access services and transact safely. Numerous large-scale data breaches have released citizens' personal and financial information into the public domain and have, to a large extent, eroded confidence in the public and private sectors' abilities to defend against, and recover from, these attacks. These attacks have also increased the public's knowledge around issues like ransomware, with this word having now entered into daily usage. The scale and sophistication of the attacks are themselves increasing at a rate not seen previously, with cybercrime now emerging as a well-paid, outsourced model.

2. African cybersecurity responses

The issue of cybersecurity looms large in the strategies of many governments in Africa. Governments on the continent are increasingly mindful of the shared public-private responsibility for cybersecurity, and are aware of the need to mobilise both public and private organisations within a multistakeholder model. This is reflected in the growing number of African countries who have established, or are in the process of establishing, enabling policy and legislative frameworks for cybersecurity, including Botswana, Swaziland, Namibia and Zambia. Southern African Development Community (SADC) countries have been aided in the legislative drafting process by the development of SADC Computer Crime and Cyber Crime Model Laws, which are part of the Harmonisation of ICT Policies in Sub-Saharan Africa (HIIPSA) project. Continental instruments such as the African Union Convention on Cyber Security and Personal Data Protection have also being mooted, and the ratification of this AU Convention is being actively pursued.

The key South Africa government response to the issue of cybersecurity has been passage of the National Cybersecurity Policy Framework (NCPF) in 2012, which is aimed at a "coherent and integrated Cybersecurity approach to address Cybersecurity threats", and at promotion of a cybersecurity culture and to building of confidence and trust in the secure use of ICTs (SSA, 2015). The NCPF has also given rise to the Cybercrimes and Cybersecurity Bill, which is currently before Parliament, and which will bring South Africa in line with international laws dealing with cybercrime (Minister of Justice, 2017).

The importance of cybersecurity is also reflected in the increasing number of countries that are establishing an operational capability in the form of national Computer Security Incident Response Teams (CSIRTs). These CSIRTs have a national mandate and currently exist in at least 16 African countries, with others either in the process of being established, or being planned. Apart from their domestic capabilities, national CSIRTs seek to address the transnational nature of cybersecurity incidents by developing cooperation frameworks between countries.

3. Contributions in this *AJIC* Focus Section

The three cybersecurity articles that follow in this *AJIC* Focus Section on Cybersecurity cover a broad spectrum of topics within the cybersecurity domain. The articles represent what is almost a hierarchy of issues and understandings that governments must have in order to create an enabling environment for cybersecurity. The first of these, covered in Sutherland's contribution, is the issue of governance and enabling policy and legislative frameworks. The article dissects the South African cybersecurity legislative ecosystem, and also delves into the issues of privacy and the operational capacity mandated by the legislative framework under the guise of national and sector CSIRTs.

The second article, by Van Niekerk, on cyber-incidents, provides a segue from the discussion of governance in encapsulating the range and scale of incidents faced by both the public and private sectors, and in describing the threat actors and the nature of the victims. The article illustrates why cybercrime is particularly difficult to combat, due to a range of factors including the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

The third article, by Chandarman and Van Niekerk focuses on the issue of cybersecurity awareness (CSA). With humans now often cited as being the weakest

AJIC 20-21-Jan-18-22h19.indd 80-81 1/21/2018 10:43:13 PM

link in the cybersecurity value chain, the issue of CSA is high in the strategic plans of governments and private organisations. Awareness programmes are geared towards educating citizens around threats and vulnerabilities that exist in cyberspace and, in so doing, instilling in citizens a sense of confidence in their ability to transact and interact in cyberspace. But as this article demonstrates, there are elements of "cognitive dissonance" at play among users, making achievement of true CSA an extremely complex task.

4. Cybersecurity research

The need for research into the various aspects of cybersecurity is increasing and the current dearth of empirical data to inform policy and strategic interventions must be urgently addressed. Policy and strategic issues in the merging digital world are increasingly being conflated. Ownership of critical infrastructure by the private sector, and the threats posed to nation-states by any attack on this critical infrastructure, mean that multistakeholder approaches are imperative.

The sheer number of threat actors, and the principle that a threat actor need only be successful once, mean that the scale of the problem facing governments will only increase. The transnational nature of the incidents, and the increasing sophistication and technical capabilities of the threat actors facing government, mean that strategies and operational plans need to be as sophisticated and comprehensive as possible. Much more research will thus be required to inform these strategies and plans if they are to ensure that cyberspace is a predominantly safe place for interactions by individuals and institutions.

References

Minister of Justice (2017). *Cybercrimes and Cybersecurity Bill*. Minister of Justice and Correctional Services. Pretoria. Retrieved from http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

State Security Agency (SSA). (2015). *The National Cybersecurity Policy Framework (NCPF)*. Pretoria. Retrieved from https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Governance of Cybersecurity – The Case of South Africa

Ewan Sutherland
Visiting Adjunct Professor, LINK Centre, University of the Witwatersrand (Wits), Johannesburg

Abstract

Cybersecurity is a growing concern for governments, with the push for universal access to the Internet, the increasing ubiquity of social networks and the growing reliance on digital government service, and given a growing range of threats from foreign powers, terrorists and criminals. These complex issues span all government ministries, their agencies and contractors, plus provincial and municipal government, and require the state to create legal frameworks and agencies to protect data and offer advice to businesses and citizens, plus ensuring a sufficient supply of skilled technicians and engineers. In the case of South Africa, its government responded in 2015 with a National Cybersecurity Policy Framework (NCPF), with implementation led by the Ministry of State Security. The Protection of Personal Information (POPI) Act of 2013 created the Information Regulator to ensure data privacy. The POPI regime is only being implemented slowly and has overly wide exemptions for national security. South Africa lags behind advanced economies in cybersecurity legislation, in government coordination, in engagement with business and citizens, and in the supply of skilled labour. Delays have meant it lacks the experiences obtained in faster moving countries, and the improvements they have made to their policies and, especially, implementation. Parliament has neither pressed the government for faster action nor explored areas where powers might have been taken that infringe human rights.

Keywords

cybercrime, cybersecurity, data protection, privacy, governance, South Africa

DOI: https://doi.org/10.23962/10539/23574

Recommended citation

Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 83-112. https://doi.org/10.23962/10539/23574

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

AJIC 20-21-Jan-18-22h19.indd 82-83 1/21/2018 10:43:13 PM

1. Introduction

National governments are adopting cybersecurity strategies to address a wide range of threats (OECD, 2012), including foreign governments attacking critical national infrastructure (CNI) (e.g., the electricity grid in Ukraine (Zetter, 2016)), criminals locking then ransoming computer systems (e.g., a hospital in England (Palmer, 2017)), hacktivists protesting against the activities of firms (e.g., Armscor (Moyo, 2016a; 2016b)) and the bulk theft of identities (Romanosky, Telang, & Acquisti, 2011). Such threats are of growing significance, given the pursuit by governments of universal Internet access and the rising use of and reliance on online government and commercial services, plus the ubiquity of social networks, and the emergence of an Internet of Things (IoT) that raises questions over the cybersecurity of objects as mundane as fridges and toys.[1] The governance challenges that follow from this include coordinating cybersecurity activities and data protection across the whole of government, including sub-national levels (e.g., municipalities), independent agencies (e.g., regulators), and contractors (e.g., outsourced services) (Chertoff, 2008). Governments must also influence the practices of businesses, especially CNI providers, as well as voluntary organisations, households, and individuals. Despite some national cybersecurity strategies having been reviewed and revised, there remain considerable challenges in ensuring these are well-constructed, cost-effective, and subject to appropriate governance (OECD, 2015; Dean, 2016). This article considers the governance of cybersecurity in South Africa, a complex federal state with a relatively sophisticated economy (OECD, 2017), though with many impoverished citizens (StatsSA, 2017), who often have limited digital literacy (RIA, 2016; Siemens, 2016), creating significant challenges for its government in assessing the risks from and of devising responses to:

- cybercrime;
- cyberespionage;
- cyberterrorism; and
- cyberwarfare.

In 2012, the South African Cabinet adopted a National Cybersecurity Policy Framework (NCPF, setting out measures and mechanisms for coordination across government (SSA, 2015). At the time of writing, the Information Regulator (i.e., the data protection authority) was not fully operational and the Cyber Warfare Strategy had yet to be finalised. The proposed coordination mechanisms were complex, making their management difficult, especially given the poor track record of inter-ministerial coordination and the difficulties in overcoming rivalries. Moreover, there are only limited oversight and review mechanisms, with many activities clouded in, possibly unnecessary and counterproductive, secrecy.

1 There has been one major distributed denial of service (DDoS) attack using hacked closed-circuit television (CCTV) cameras (Goodin, 2017), while one government has issued a warning against use of particular toys (Conradis, 2017), and in one country, an adult toy manufacturer settled litigation over violations of the privacy of its customers (Roberts, 2017).

There are significant challenges in assessing possible threats and in keeping such assessments accurate, given advances in technologies and in their uses, such as the evolving "dark net" (Fachkha & Debbabi, 2016; Lacson & Jones, 2016), and the growing offensive capabilities of a few countries and of groups of individuals, including terrorists (Liff, 2012; Lindsay, 2015), plus a great many everyday cybercriminals (Akamai, 2016; 2017; Cisco, 2017). South Africa has been the country most often attacked in Africa (Wolfpack, 2013; TMG Digital, 2016; Van Heerden, Von Soms, & Mooi, 2016), with an estimated cost in 2014 of ZAR5.8 billion (Fripp, 2014). While one in 10 businesses reported a cyberattack during 2015, this is expected to rise significantly from 2018, when reporting is, finally, made mandatory, triggering much greater attention to prevention and security, especially because firms can then be held legally liable (Jonker, 2015). Cybercrimes are likely to be underreported by citizens, given their uncertainty about the capability of the South African Police Service (SAPS) in matters of technology. There are dangers in the lobbying and salesmanship from those making cybersecurity systems, who may overstate the risks and the effectiveness of their products, in order to increase their profits. Equally, the intelligence services may seek greater budgets to buy such systems, an extension of the military-industrial complex described by Eisenhower (Brito & Watkins, 2011).

The African National Congress (ANC) has been in government since 1994, following the first elections under universal franchise (Southall, 1994). However, it has been losing its attractiveness to the electorate, as a result of internal rifts and its failures on service delivery, with President Zuma having emphasised loyalty to himself (Booysen, 2015; Southall, 2015; Paret, 2016). There is an independent and powerful Constitutional Court, one that has shown it will hold anyone and everyone to account (Gibson, 2016; Roux, 2016). Whereas Parliament has often struggled to scrutinise complex legislation and exercises only limited oversight of budgets, ministers and policies (Hawker, 2003; 2007). This fits broadly within the framework of weak institutional endowments (North, 1990), explaining the limits to the ability of governments to create mechanisms and structures to deal with complex issues. If government is to persuade firms and individuals to adopt measures to improve their cybersecurity, then it needs to ensure its own activities are highly secure or, initially, not embarrassingly insecure, and to acknowledge the limitations of its influence, in order to maximise its credibility.

After 1994, governance of the intelligence community and of the wider security sector was never going to be easy, given the histories of the state and of the ANC, neither of which had shown much regard for accountability or transparency in intelligence and security matters. Nonetheless, section 198 of the 1996 Constitution, on the governance of the intelligence services, expressly controls what is now the State Security Agency (SSA), requiring it to observe the rights of citizens (Klaaren, 2015). Whether those rights are protected and the extent to which the SSA prefers to practice its own exceptionalism, believing that it is above rather than under the

AJIC 20-21-Jan-18-22h19.indd 84-85 1/21/2018 10:43:13 PM

Constitution, are matters of contention (Nathan, 2010; Van der Westhuizen, 2013). The only authoritative inquiry found that officials drafting and vetting operational policies lacked an adequate understanding of the Constitution and its protections for citizens (Matthews, Ginwala, & Nathan, 2008). A major concern has been that the SSA has become an instrument of senior members of the ANC, concerned more with its internal personal and political battles than with assessing and countering external and terrorist threats (Solomon, 2012; McKinley, 2013).[2] This has been further complicated by the fusion of the ANC with the state, the party having been in office for over two decades, deploying its own members into all levels of the administration, and emphasised by President Zuma having formerly been a head of the ANC intelligence service.

Assessing the relative performance of South Africa is limited by the lack of comparative data. Following its development of other compound indicators, the International Telecommunication Union produced the Global Cybersecurity Index (GCI) (ITU, 2017), with a view to raising awareness of the challenges.[3] The title is disingenuous, since the GCI measures not cybersecurity, but legislative measures and policies on paper, which do not determine and cannot predict levels of cybersecurity in practice. To measure cybersecurity it would be necessary to capture the efforts of governments and their agencies to implement and enforce the policies, for example, to identify budgets, campaigns, and skills development. Unsurprisingly, the "leading" nations in the GCI are OECD countries with good governance, plus a couple of the faster moving autocracies, while South Africa is considered "maturing", along with a mixed bag of countries. Commercial reports on cybersecurity point to realities as experienced by citizens and firms, but offer little specific information about South Africa (Akamai, 2016; 2017; Cisco, 2017; Microsoft, 2017; Norton, 2016; Symantec, 2017).

The challenges for businesses include legal liability for the loss of customer data and the consequential falls in share prices, loss of brand value and of customer loyalty (e.g., the Equifax data breach (Volz & Shepardson, 2017), and the release of 30 million South African IDs (Lotz, 2017)). Firms are often reluctant to admit to data breaches because of potential financial losses, despite such reporting being included in corporate social responsibility (CSR) and in some countries being a legal obligation under data protection laws, notably in South Africa from 2018. The King Committee (2016) called for the governing bodies of South African firms to be proactive in monitoring and responding to cyberattacks, though there has been no assessment of the effectiveness of corporate cybersecurity governance.

2 Cyril Ramaphosa, despite being Deputy President, was apparently spied on because of his candidacy for the ANC Presidency (Letsoalo, 2017).

3 One of its partners in this venture is the Egyptian regulatory authority that runs a deep packet inspection system for the repressive regime of Marshal Al Sisi.

The next section examines the National Cybersecurity Policy Framework. This is followed by analyses of privacy and data protection. Surveillance is then examined, insofar as information is made public, followed by an analysis of cybersecurity skills. Finally, conclusions are drawn and issues identified for further research.

2. The National Cybersecurity Policy Framework (NCPF)

Like many other laws and policies, the National Cybersecurity Policy Framework was partly the result of diffusion (Meseguer, 2005; Gilardi, 2010), drawing on sources such as the EU, the North Atlantic Treaty Organisation (NATO) and the US, which are more advanced users of technology and have faster-moving policy formulation (Grobler, Van Vuuren, & Leenen, 2012; Van Vuuren, Phahlamohlaka, & Leenen, 2012; 2014). The South African government used some foreign experiences and texts, raising questions about the effectiveness of its adaptation to the legal and political systems and cultures, and the degree to which it has designed something it had the administrative and technological skills to deliver.

The development of the NCPF was slow, not helped by President Zuma moving responsibility between Cabinet "clusters" and between departments, nor by his rapid turnover of ministers. The Minister of Communications published a detailed cybersecurity policy draft (Nyanda, 2010), which took two years to be approved by Cabinet and a further three years to be published, and only in Afrikaans and English.[4] By then, it was the Minister of State Security who was in charge (SSA, 2015), with the State Security Agency (SSA) responsible for implementing the policy, roadmap and strategy. Nonetheless, the Department for Telecommunications and Postal Services (DTPS), inheritor of part of the work of the Department of Communications (DoC), retained significant responsibilities.

Implementation of the NCPF requires extensive coordination across government (see Table 1), with the lead assigned to the Justice, Crime Prevention and Security Cluster of ministers (JCPS, n.d.). A Cybersecurity Response Committee, chaired by the Director-General of State Security, with the heads of the relevant departments and agencies, was charged with strategy and decision-making, and required to identify and prioritise areas for intervention, based on assessments of possible threats.[5] The closeness to state security means there is only limited transparency or oversight, though DTPS (2017a) did give an initial briefing to its Parliamentary Portfolio Committee. One weakness was that the national e-government strategy had not been updated for many years (DPSA, 2001), until the recent addition of a complementary strategy, strangely this came from DTPS, based on the ECT Act (DTPS, 2017b; 2017d). It admitted significant failures in implementing the 2001 policy and added some limited security measures, notably a Security Sub-Committee

4 There are nine other official languages.

5 The Cybersecurity Response Committee is supported by the SSA Cybersecurity Centre.

AJIC 20-21-Jan-18-22h19.indd 86-87 1/21/2018 10:43:14 PM

of the National e-government Steering Committee, though it failed to mention the NCPF.[6]

Table 1: Departments directly engaged in cybersecurity (RSA, 2016)

Cluster	*Department*	*Legislation or policy*	*Agencies and centres*
Justice, Crime Prevention and Security Cluster Cybersecurity Response Committee	State Security	National Cybersecurity Policy Framework (NCPF) Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) Protection of State Information Bill	State Security Agency (SSA) SSA Cybersecurity Centre Electronic Communications Security Computer Security Incident Response Team (ECS-CSIRT, n.d.)
	Justice and Constitutional Development	Cybercrimes and Cybersecurity Bill	National Prosecuting Authority (NPA) South African Police Service (SAPS)
	Defence	Cyber Warfare Strategy	Cyberwarfare Command Centre HQ COMSEC Ltd
	Telecommunications and Postal Services	Electronic Communications and Transactions (ECT) Act Cryptography Regulations (RSA, 2006) e-government Strategy and Roadmap (DTPS, 2017d)	National Cybersecurity Advisory Council (NCAC) National Cybersecurity Hub Cyber Inspectorate
Economic Sectors, Employment and Infrastructure Development Cluster	Trade and Industry	Companies Act	-
	Public Service and Administration	Promotion of Access to Information Act (PAI) Governance of Corporate IT Framework (DPSA, 2012) e-government strategy*	State Information Technology Agency (SITA)
Governance and Administration	Public Service and Administration	-	-
	Justice and Constitutional Development	-	-

* Additionally, the various provinces have adopted their own e-government strategies.

6 It maintained the 1996 Minimum Information Security Standards (MISS) ensuring "the national interests of the Republic are protected".

The overarching objective of government is (RSA, 2010a):

> Outcome 3: All people in South Africa are and feel safe.

Based on this, there was a "delivery agreement" between the Presidency and the Justice Ministerial Cluster (RSA, 2010b), calling for:

> Development of a Cybersecurity Policy and the implementation thereof.
> Development of capacity to combat and investigate cyber crime.

Nonetheless, the ability to combat and investigate breaches of cybersecurity seems to lie much further in the future, as does the prosecution of individuals, given the need to implement the Cybercrimes and Cybersecurity Bill and to train police, prosecutors and judges.

Formerly, the Department of Communications (DoC) sat in the Economic Sectors Ministerial Cluster, responsible for the communications regulatory authority and for broadcasting, posts and telecommunications markets. In 2014, the DoC was split, with the creation of the new Department of Telecommunications and Postal Services (DTPS), under a former security minister, taking over its work on cybersecurity. A National Cybersecurity Advisory Council (NCAC) had been created to aid the DoC on policy and technical issues (see Table 2), but is reported as having done very little (IT News Africa, 2013).[1] Nonetheless, in 2017 applications were invited to serve on a new NCAC (DTPS, 2017c).

Table 2: National Cybersecurity Advisory Council (Oxford, 2013)

Name	*Affiliation*
Barend Taute (Chairman)	Council for Scientific and Industrial Research (CSIR)
Ritasha Jethva (Vice-chairman)	Accenture
Dr Khomotso Kganyago	Chief Security Advisor, Microsoft South Africa (deceased 2014)
Prof Tana Pistorius	Department of Mercantile Law, University of South Africa (UNISA)
Mark Heyink	Attorney
Sizwe Snail	Attorney
Collen Weapond	Fraud and corruption specialist Advocate

AJIC 20-21-Jan-18-22h19.indd 88-89 1/21/2018 10:43:14 PM

Chapter XII of the Electronic Communications and Transactions (ECT) Act of 2002 provides for the establishment of a Cyber Inspectorate, with power to inspect, search, and seize content, in pursuit of the unacceptable. It was intended to assist law enforcement agencies, and to provide services directly to the public and businesses. No implementing regulations were ever promulgated, no Cyber Inspectors were appointed, and no offences created by Chapter XIII were ever prosecuted.

In the US, one organisational solution to widespread cyberattacks was the creation by government and by the private sector of Computer Security Incident Response Teams (CSIRTs) (Wiik, Gonzalez, & Kossakowski, 2006; Bronk, Thorbruegge, & Hakkaja, 2006; Grobler & Bryk, 2010). This followed the isolated and uncoordinated responses to the "Morris worm" or "Internet worm" in 1988, which was seen as having been poorly handled, with duplicated efforts and conflicting solutions. The US Defense Advanced Research Projects Agency (DARPA) established the Computer Emergency Response Team (CERT*) Coordination Center, setting a pattern replicated by many organisations and governments. The various CSIRTs soon began ad hoc exchanges of information, formalised from 1990 through the Forum for Incident Response and Security Teams (FIRST, n.d.; Gonzalez, 2005; Wiik & Kossakowski, 2005), including significant numbers of face-to-face meetings. Three South African CSIRTs participate in FIRST:

- First National Bank;
- government (ECS-CSIRT); and
- Standard Bank Group.

In 2015, DTPS launched the National Cybersecurity Hub (NCH, n.d.)), aimed at informing business, voluntary organisations and the public, and to serve as the national CSIRT, a contact point for both domestic and foreign CSIRTs (Cwele, 2015).

Like other countries, South Africa adopted a variety of approaches to e-government at national, provincial and municipal levels, purportedly all under the Department of Public Service and Administration (Trusler, 2003; Mutula & Mostert, 2010; Cloete, 2012; DPSA, n.d.; Mawela, 2017), though most recently from DTPS (2017b). Beginning in 1997, there was a slow process of consultation and adoption, aimed at increasing productivity and efficiency for government and improving convenience for citizens. Implementation often failed to achieve the planned goals, due to the limited capacity and the lack of willingness of ministers and officials to engage with the challenges. Little attention was given to cybersecurity, despite risks to human rights from the misuse of the large volumes of personal data held by government, or its theft by cybercriminals.

The 2010 draft NCPF acknowledged the lack of coordination within government and the insufficiency of existing legal measures needed to counter and prosecute

cybercrime. It aimed to:

- facilitate the establishment of relevant structures in support of cybersecurity;
- ensure the reduction of cybersecurity threats and vulnerabilities;
- foster cooperation and coordination between government and private sector;
- promote and strengthen international cooperation;
- build capacity and promoting a culture of cybersecurity; and
- promote compliance with appropriate technical and operational cybersecurity standards.

Organisational deficiencies were to be reduced by creating NCAC (see Table 2), with officials drawn from a range of ministries and agencies, and with five independent members, to coordinate implementation of policies. It was to work with the government CSIRT, responding to breaches, incidents, and threats though there is very little evidence it has yet done anything.

A central challenge for government is the promotion of cybersecurity measures amongst:

- government (at national, provincial and municipal levels);
- general public;
- private sector (both domestic and foreign firms);
- civil society; and
- special interest groups.

The Minister of Justice and Correctional Services (2015) published a draft Cybercrimes and Cybersecurity Bill in 2015, inviting comments, and later announced that a revised version was to be laid before Parliament (Minister of Justice, 2017b). However, it failed to publish either the comments received or an analysis of their content, making it impossible to know the extent to which the Department had responded to concerns, criticisms and proposals from experts and the general public. At the time of writing, the Bill is being scrutinised by the Portfolio Committee on Justice and Correctional Services (2017), which invited public comments and held two days of public hearings.[7] The Bill will formally create the Cyber Response Committee to coordinate work across government.

Internationally, South Africa has supported a series of resolutions of the UN General Assembly (2010) concerning CSIRTs, protection of CNIs and, more generally, the work of the UN Office on Drugs and Crime (UNODC, 2017).[8] It has also supported the International Multilateral Partnership Against Cyber-Terrorism (IMPACT, n.d.), created by a UN official, but now seemingly defunct. At the 2017 ITU World Telecommunications Development Conference, attempts to amend Resolution 45

7 To date these have not been published, though the Department responded to them.
8 UNODC has built up a repository of national laws and policies for cybersecurity.

AJIC 20-21-Jan-18-22h19.indd 90-91 1/21/2018 10:43:14 PM

(Rev. 2014) on cybersecurity failed, due to wildly differing aims amongst countries. South Africa signed the Budapest Convention on Cybercrime (Council of Europe, 2001), but never ratified it. It has also signed, but not ratified, the African Union Convention on Cyber Security and Personal Data Protection (AU, 2014); indeed so few countries have ratified it that it is unlikely to come into force.

As a signatory to the International Covenant on Civil and Political Rights (ICCPR),[9] South Africa is subject to periodic review, though it was 14 years late in submitting its most recent report. Amongst many suggestions to South Africa from the UN Human Rights Committee (2016):

> The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act. It is also concerned about the wide scope of the data retention regime under the Act. The Committee is further concerned at reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre, and at delays in fully operationalizing the Protection of Personal Information Act, 2013, due in particular to delays in the establishment of an information regulator (arts. 17 and 21).

A major part of any cybersecurity strategy concerns the military and its ability both to remain fully operational while under cyberattack and its capability to launch conventional and cyberattacks. The NCPF sets out the following tasks for the Department of Defence:

- address national security threats in cyberspace;
- combat cyberwarfare, cybercrime and other cyber ills;
- develop, review and update existing substantive and procedural laws to ensure alignment; and
- build confidence and trust in the secure use of information and communication technologies.

The preferred military terminology is information warfare, covering a broad range of operations in what it terms the "InfoSphere".

A Cyber Warfare Strategy is said to be at an advanced stage of development, having been submitted to the Chief of the South African National Defence Force (Department of Defence, 2016; 2017; Mapisa-Nqakula, 2016). In financial year 2016/17, there was to be a Cyberwarfare Implementation Plan and in 2017/18 a

9 https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

Cyberwarfare Command Centre Headquarters, the latter delayed because of financial constraints:

> South Africa requires the protection of its cyber-domain, through (inter alia) a comprehensive information warfare capability, integrated into its intelligence-related information systems at the international, national and defence levels. Both defence and wider-government capabilities must be enhanced to secure vital networks. (Department of Defence, 2015a, p. vi)

The Department of Defence (2015b) offers very little indication of possible threats or of their likely origins. It seems unlikely that any country would attempt to conquer South Africa or to seek to carve off part, but some states might wish to destabilise its government (e.g., in retaliation for its involvement in other African states) or to attack its ruling political party. Some individuals and commercial groups might consider attacks that would affect the supply of minerals to the global market and thus their prices. However, the most obvious attacks appear likely to come from domestic opponents of the regime or well-financed groups engaged in corruption.[10]

A somewhat unusual twist in the organisational arrangements is that protection of state information against a cyberthreat is the primary responsibility of the State Security Agency through a private company, Electronic Communications Security (Pty) Ltd (COMSEC Pty Ltd). This company was established in 2002, with the primary purpose of ensuring that critical electronic communications are secure and protected.

Defence networks are targets for attacks because they run command and control, administration, personnel, logistics and finance information systems. These networks thus require protection, including the use of technologies not available on the open market:

> The department will focus on cyber security over the medium-term through the approval of a DOD Cyber Warfare Strategy in the FY2015/16 and establishing a Cyber Command Centre Headquarters by the FY2018/19. The latter will be executed in the Defence Intelligence budget programme at a projected cost of R511 million over the medium-term. (Department of Defence, 2015b, p. 56)

There are significant path dependencies from past decisions that limit the ability of government to craft its strategies and plans, and little evidence of international cooperation or peer review. The division of responsibilities between several government departments, whose ministers have changed relatively frequently, creates problems, noticeably in delays and in redundant or vestigial bodies. Rapid turnover

10 For example, the Gupta family, through Oakbay, engaged an expensive public relations firm from the UK, spending sums that, had they been used for cyberattacks, could have been extremely damaging.

AJIC 20-21-Jan-18-22h19.indd 92-93 1/21/2018 10:43:14 PM

in ministers, reconfigurations of departments and complex coordination make it unnecessarily difficult for government to develop expertise and to deliver results, similar problems of turnover in committees make parliamentary oversight much more difficult.

3. Privacy and data protection

Unusually for Africa, South Africa has a common law right of privacy that dates from the 1950s (Burchell, 2009; Roos, 2016). A radio broadcaster consented to the publication of her photograph in a newspaper article, but the photograph was subsequently used in advertising without her consent, which was held to violate her right to privacy (O'Keeffe v Argus Printing, 1954).[11] The courts have also recognised unreasonable intrusions to include bugging a room, intercepting a telephone call, reading private documents, and unauthorised testing of blood. Some violations of privacy have been treated as criminal invasions of privacy (i.e., *crimen injuria*).

The Constitution of 1996 protects privacy in section 14:

> Everyone has the right to privacy, which includes the right not to have—
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications infringed.

Additionally, section 10 created the right to human dignity that must also be respected and protected.

The Constitutional Court has concentrated on forced legislative disclosure of information, providing general guidelines for data protection (SALRC, 2005):

- was the information obtained in an intrusive manner?
- was the information about intimate aspects of the subject's personal life?
- was it provided for one purpose but used for another?
- was it disseminated to the press or general public from whom the subject "could reasonably expect such information would be withheld"?

Debates on security have heavy historical baggage, especially in respect of the long rule of the National Party, which imposed the pass laws that still colour any consideration of identity documents (Breckenridge, 2005; Donovan, 2015).[12] A proxy for a national identity database was created by the mandatory registration of all SIM cards, which now encompasses most citizens and residents and large numbers of visitors. Such databases are especially attractive to hackers seeking financial rewards

11 The arguments echoed *Tolley v JS Fry & Sons Ltd* [1931] UKHL 1 (23 March 1931), http://www.bailii.org/uk/cases/UKHL/1931/1.html

12 The US government has incorporated biometric identities into passports for its own citizens, and requires visitors to have either a biometric passport or a biometric visa (including fingerprints).

from stealing large and inclusive sets of personal details. There are serious doubts about the security of such databases, notably the loss of Terabytes of data from the US National Security Agency (NSA) (Reuters, 2017).[13]

South Africa has prepared data protection legislation, though on a peculiarly tortuous path (Roos, 2016):

- South African Law Reform Commission (SALRC)
  - included in work programme in 2000
  - published a paper on privacy and data protection (SALRC, 2003)
  - published a paper on data protection (SALRC, 2005)
- Protection of Personal Information Bill in 2009
- Protection of Personal Information (POPI) Act of 2013
  - signed by President (2013)
  - appointment of board member of the Information Regulator (Gallens, 2016).

At the time of writing, the POPI Act is not fully implemented and may not be until late 2018. It will enable citizens, as data subjects, to bring civil actions against firms for data breaches. The Electronic Communications and Transactions (ECT) Act of 2002 sets out principles for information protection and created offences of unauthorised access to, interception of and interference with data. However, it appears to have had little practical effect.

The POPI Act broadly matches the European Union legislation (EU, 1995; 2016), with a view to attracting outsourcing and call centre business, since data cannot be transferred from the EU except to countries with comparable data protection provisions. This reflects efforts over a number of years to attract back office processing and call centre activities to major urban centres (Deloitte, 2015; Nelson Hall, 2015; BPESA, n.d.).

A central question concerning data protection emerges from section 6(1)(c) of POPI, which excludes processing by or on behalf of a public body involving national security, defence or public safety. This appears to give the intelligence services an entirely free hand in the processing of data, except that they must comply with Section 198 of the Constitution that, inter alia, enforces human rights. While those rights can be limited by statute, it is only insofar as is compatible with a democratic society. The subsequent section 6(1)(d) of POPI additionally exempts processing for Cabinet, an obscure provision, since it is in addition to national security purposes, without any indication of what processing the Cabinet might require. Eventually cases must be brought before the Constitutional Court to test the limits of the state to violate the right to privacy.

13 This included hacking tools.

AJIC 20-21-Jan-18-22h19.indd 94-95 1/21/2018 10:43:14 PM

In time South Africa should have a strong data protection law protecting privacy, combined with common law and the constitutional protections of privacy, though this might take a number of years. For the present, the intelligence services appear exempt, unless and until litigation is brought to limit their actions.

4. Surveillance

The interception of telephone calls has featured prominently in the South African popular press, because of the "spy tapes" concerning the then Deputy President Jacob Zuma and corruption allegations in the arms deal scandal (Wolf, 2011; 2015; *Zuma v DA*, 2017). The interception of postal articles and telephone calls was originally authorised by a minister, then from 1992 by a judge (Cohen, 2001), and since 1996, has been subject to the Constitution and its protection of human rights (see Table 3). The last are limited by national security, defined in the General Intelligence Law Amendment Act of 2013 (GILAA), to include the protection of the people and the territorial integrity of the Republic against the threat of or use of force, as well as espionage, sabotage and terrorism.

Table 3: Interception laws in South Africa

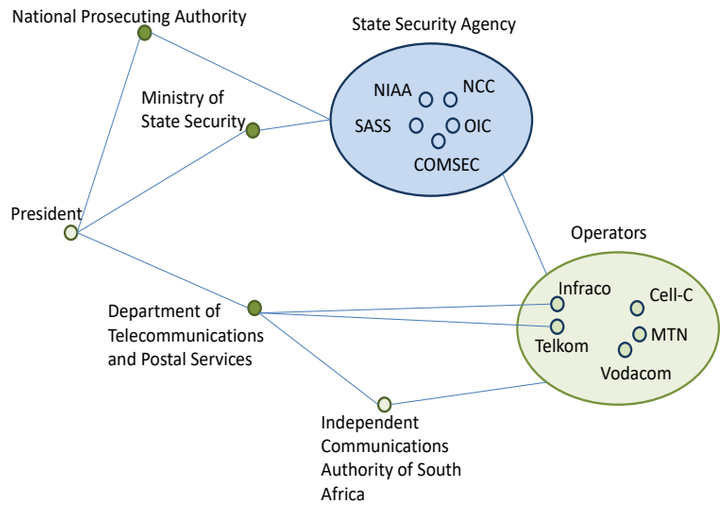
Statute	*Year*	*Section(s)*	*Authorisation*
Post Office Act	1958	118A	Minister
Interception and Monitoring Prohibition Act	1992	1	A discharged judge designated by the Minister of Justice
Interception and Monitoring Prohibition Amendment Act	1995	1	Redefines a judge to include currently serving, discharged and retired judges of the Supreme Court
Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA)	2002	7 & 8	A judge designated by Minister of Justice

All state intelligence activities are governed by the National Strategic Intelligence Act of 1994, Intelligence Services Oversight Act of 1994, Intelligence Services Act of 2002, and GILAA of 2013, stipulating that covert intelligence-gathering may only legally be conducted by these agencies. The Safety Matters Rationalisation Act of 1996 repealed 34 controversial apartheid-era laws dealing with security legislation, though it left significant security laws untouched.

The Intelligence Services Oversight Act of 1994 created the parliamentary Joint Standing Committee on Intelligence (JSCI, n.d.; Minister of Justice, 2017) and an

Inspector-General for Intelligence to investigate complaints, based on a framework set out in a white paper (RSA, 1994).[14] The JSCI comprises members of the six largest political parties in Parliament, charged with scrutinising and reporting on the finances and operations of the SSA (Ahmed, 1999). There are two routes for a citizen to complain about surveillance: to the JSCI or the Inspector-General. Nonetheless, there is considerable secrecy about surveillance practices, with sporadic attention from investigative journalists, non-governmental organisations (NGOs) and university researchers. There have also been a critical report by Privacy International (2016) and the suggestions by the UN Human Rights Committee (see above).

Figure 1: Surveillance system in South Africa



The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) of 2002 created:

- the Office for Interception Centres (OIC); and
- the National Communications Centre (NCC).

The former is domestic, while the latter provides bulk monitoring and the interception of signals outside the country or passing through or entering South Africa (see Figure 1) (Watney, 2015; McKinley, 2016). RICA requires owners of mobile phones to register their SIM cards with their service providers, which have to obtain certain customer details and pass these on to the OIC. The OIC and NCC provide call data records (CDRs) and interception for the intelligence services, the National Prosecuting Authority (NPA) and Financial Intelligence Centre (FIC).

14 The 1996 report of the JSCI covered the first wire-tapping scandal: the NIA tapping of the SAPS.

AJIC 20-21-Jan-18-22h19.indd 96-97 1/21/2018 10:43:15 PM

Related to the global adoption by businesses of CSR reporting, some service providers and network operators have published transparency reports on government collection of data and requirements to remove content from the Internet (GNI, n.d.)). The first transparency report by the Vodafone Group (2014) stated it was forbidden from publishing the scale of lawful interception on its network in South Africa.

Judge Yvonne Mokgoro was designated to approve and oversee applications from authorities seeking to intercept calls, on which she is required to publish annual reports (Mokgoro, 2014).[15] These have been intermittent, with the most recent report, covering 2014-15 (see Table 4), omitting any mention of IMSI-grabbers and limited to conventional interception. Her reports are sent to the parliamentary JSCI, which publishes them and considers their contents, though in closed meetings without publishing any minutes (JSCI, 2017; Minister of Justice and Corrctional Services, 2017). The only available JSCI report is minimalist, with no reference to cybersecurity (JSCI, 2015).

According to the Review Commission (Matthews, Ginwala, & Nathan, 2008), and subsequent investigative journalism, the NCC has mass surveillance capabilities unregulated by law, which would necessarily be unconstitutional. Twice the Ministry has introduced legislation that sought to recognise the NCC in law; in the first instance the National Strategic Intelligence Amendment Bill was withdrawn, in the second instance the relevant provisions were removed during parliamentary deliberations.

A further concern is the unregulated use by FIC, the SSA, and the South African Police Service (SAPS) of IMSI-grabbers,[16] devices that appear to be base stations belonging to mobile operators but which collect handset and SIM card details at a distance, with some allegedly able to perform man-in-the-middle attacks in order to intercept calls and data. One of these was used to jam mobile signals in Parliament (*Primedia Broadcasting v Speaker*, 2016), and another was found in a shopping mall in most peculiar circumstances.

While there are constitutional and legal frameworks for surveillance, these appear to be more honoured in the breach than in the observance, with the policies and practices for use of IMSI-grabbers protected from disclosure under the Promotion of Access to Information (PAI) Act,[17] and reporting by operators of requests for customer data prohibited by statute. The interceptions that are reported appear to be remarkably few in number (see Table 4), given the high level of crime (Kynoch, 2005); in particular, there is a long and dishonourable tradition in South Africa of political assassinations and financially-motivated killings, some apparently based on the locations of mobile phones (Shaw & Thomas, 2016; Shaw, 2017; Johnson, 2017).[18] Consequently, there is very little evidence that oversight and scrutiny are effective.

Table 4: Applications for directions to intercept under RICA (Mokgoro, 2014, p. 15)

	State Security Agency	*South African Secret Service*	*South Africa Police Service*	*Financial Intelligence Centre*	*South African National Defence Force*	*Total*
Applications (new)	28	2	150	3	3	185
Re-applications	30	-	2	-	-	54
Amendments	34	-	8	-	1	5
Extensions	31	-	4	-	-	35
Amendments and extensions	13	-	18	-	-	31
Entry warrants	4	-	-	-	-	4
Section 11	66	-	-	-	-	66
Oral intercepts	2	-	-	-	-	2
Refused	5 *	-	-	-	-	5
Total	**215**	**2**	**202**	**3**	**4**	**387**

* No RICA confirmation

5. Skills

South Africa has had a shortage of ICT skills for many years, despite high levels of unemployment and the presence of many colleges and universities. One cause is the lack of a national ICT planning process that could engage with industry, educational institutions and providers of continuing professional development (CPD). A particular problem is the very large number of small- and medium-sized enterprises (SMEs), which have limited budgets and capacity to develop ICT skills, thus requiring support from government. A major underlying concern is that too many schools lack the equipment and teachers trained in computer science and ICTs, aggravated by pupils not having computers and broadband access at home. While university graduations in ICTs have grown, it is by much less than other courses, in part because ICT students are dropping out (Kirlidog, Van der Vyver, Zeeman, & Coetzee, 2016).

In recent annual surveys, the Joburg Centre for Software Engineering (JCSE)

15 Judge Mokgoro noted the need to update the terminology in RICA.
16 Also known as IMSI-catchers and stingrays.
17 See, for example, Peekhaus (2014).
18 It was alleged that the then-Minister of Communications sought a contract killer to eliminate the Chairman of the Parliamentary committee investigating her for corruption (ENCA, 2013).

AJIC 20-21-Jan-18-22h19.indd 98-99 1/21/2018 10:43:15 PM

reported an acute shortage of skilled ICT workers in South Africa, with information security a leading issue for employers (Schofield, 2016). It concluded that the ICT industry could not wait for local, provincial and national governments to provide solutions, while tertiary education institutions did not possess the necessary responsiveness. Consequently, the ICT profession and sector would have to solve the "crisis" through their own initiatives.

Cybersecurity presents particular problems, with the need for skilled individuals in the defence and security sectors, in critical national infrastructure, and in banking and finance. The implementation of the POPI Act will require all firms to bolster their cybersecurity efforts, with additional staff and significant CPD, up to board level. Without a substantial increase in supply, the shortage of skills will persist, with skilled individuals likely to be attracted to organisations able to pay the most.

At a more general level, the public needs to be taught about dangerous and unsafe behaviours on the Internet (e.g., passwords and phishing). The failure to teach schoolchildren about online safety has already been acknowledged (Kritzinger, 2014).

The NCPF recognised that South Africa would lag behind and be increasingly vulnerable unless it developed the necessary skills, for which it relied on colleges and universities (SSA, 2015, p. 13). However, the support for research and training has been limited. The South African Cyber Security Academic Alliance (SACSAA, n.d.) comprises three groups:

- Nelson Mandela University (NMU):
    - Centre for Research in Information and Cyber Security (CRICS, n.d.);
- University of Johannesburg (UJ):
    - Centre for Cyber Security (CSI, n.d.);
- University of South Africa (UNISA):
    - Cyber Security Awareness (CSA, n.d.).

In 2015, SACSAA ran an awareness campaigns, warning of the dangers of cyberbullying, and a poster competition. Recently it has been silent and appears to be moribund. There are some commercial initiatives, notably a Deloitte Cyber Intelligence Center (CIC), part of its global network of such centres (Mbelli & Dwolatzky, 2016). The South African Banking Risk Information Centre (SABRIC, n.d.) is a collective effort by the banking sector, leveraging public and private partners.

While the vast majority of surveillance technology firms are based in China, Europe, the US and, especially, Israel, there appear to be two in South Africa (see Table 5), VASTech and iSolv Technologies, with VASTech having received funding from the South African government (PI, 2014). Additionally, Lightning Bird Logistics in Stellenbosch acts as an agent for the sale of IMSI-grabbers from the US firm Verint.

Exports of surveillance and wiretapping technologies to other African countries should be subject to controls through the South African National Conventional Arms Control Committee (NCACC), implementing the National Conventional Arms Control Act of 2000 and the international Wassenaar Arrangement (2017).

Table 5: Firms in South Africa engaged in surveillance technologies

Firm	*Location*	*Description*
VASTech (n.d.)	Technopark, Stellenbosch	An independent firm, established in 1999, selling hardware and software to government to be used in fighting cross-border and international crime.
iSolv Technologies(n.d.)	Parktown North, Johannesburg	A privately-owned company focused on the development and production of state-of-the-art ICT security solutions. Specialising in communications monitoring and cybersecurity.

As is the case more widely in ICTs, South Africa lacks sufficient skills for effective cybersecurity, with shortages affecting government recruitment and retention of staff. To date, efforts to engage the wider population for basic cybersecurity have received limited attention and resources.

6. Conclusions

A major complaint about the South African government has been its failure in service delivery, of which cybersecurity is an example, even if not widely appreciated. It has been the result of delays, of inadequate assessments of the risks, of insufficient transparency, and of difficulties in coordination across government, business and society. While the government has, somewhat tardily, adopted a National Cybersecurity Policy Framework, it is of considerable complexity and is being implemented only slowly, with very limited reporting and Parliamentary oversight. The various organisational structures and their links into yet more structures suggest that implementation will continue to prove difficult, with coordination essential between many rivalrous ministers, many of whom may soon move on. The lack of priority placed on cybersecurity is reflected in the policy taking two years to go from draft to adoption, the Cybercrimes Bill also taking two years, and similar delays with the Cyber Warfare Strategy. It will ultimately have taken two decades to deliver a data protection authority, depriving South Africa of the lessons that could have been learned in that time.

Parliamentary oversight is very difficult given the technical complexity of the material and the inter-ministerial spaghetti, aggravated by unnecessary turnover in

AJIC 20-21-Jan-18-22h19.indd 100-101 1/21/2018 10:43:15 PM

committee membership, limiting the development of expertise. Surprisingly, there were no parliamentary inquiries into the failure of the cybercrime inspectorate provisions of the ECT Act, the cleaving of DTPS from DoC, or the misuse of IMSI-grabbers, unlike comparable inquiries in the EU, UK and US (PAC, 2017; GAO, 2017; Oversight Committee, 2016; Schwab, 2016). Given the importance of cybersecurity to human rights and to growth of the digital economy, Parliament needs to develop methods to address its cross-governmental and technical nature, for example, by creating a forum or panel of expert advisers, together with a mechanism for coordination between Parliamentary Portfolio Committees.

The NCPF appears to have been written without much consideration of implementation, echoing the confused complexity of the ICT White Paper (DTPS, 2016; Freedman, 2016; McLeod, 2017). While there has been diffusion of policy elements and ideas from Europe and the US, there is little evidence of these having been adapted to South African national circumstances, especially the absence of any public assessment of the risks or of the potential impact of the proposed measures, or consideration of the ability to implement. The government failed to publish its analyses of the responses to its drafts of law and policy, raising questions about how effectively it makes use of such material and pointing to a serious weakness in governance.

That the intelligence and police services have wiretapping capabilities is very clear, though there is little evidence this reduces crime rates or secures South Africa against terrorism. It is observed more from leaks and the illicit sale and use of data, than from an increased number of prosecutions or greater success in the courts. Indeed, petty corruption in the interception of calls and in access to databases appears to be a significant problem, though the individuals are seldom prosecuted. The use of IMSI-grabbers is even more opaque, apparently without a policy or legal basis, used for blocking mobile signals in the vicinity of the President and possibly deployed more widely and much more intrusively. Yet more disturbing is the use of surveillance malware by the State Security Agency and Financial Intelligence Centre, which would certainly be unconstitutional. Ordinarily, those should have prompted Parliament to inquire into the use of such intrusive technologies, more commonly used by repressive regimes such as those in Ethiopia or Uganda. The likely outcome is for NGOs to go to the Constitutional Court for definitive rulings on the limits of the use of national security as a justification to withhold policy documents requested under the PAI Act, and then for them to seek to limit the use of IMSI-grabbers and surveillance software in order to uphold rights to dignity and privacy.

A major challenge is to persuade individual citizens and families to adopt good practice for cybersecurity, which requires a mixture of education and publicity. To date, relatively little has been done or to have been planned by government or industry, despite the rising levels of Internet adoption and global concern about

cyberthreats. A similar challenge lies in the persuasion of businesses, which must adopt appropriate measures to defend themselves, and the data they hold about their customers, from attacks, and to report all attacks that get through. This is an area in which the government needs to improve its credibility, by securing its own systems, by reporting its own breaches, and by helping and encouraging business to develop toolkits to defend themselves. These problems are aggravated by a longstanding shortage of ICT skills, which has hampered technology deployment and economic growth.

The diffusion and adaptation of cybersecurity policies requires further research, not least to determine the extent to which they are being matched to real threats and abilities, rather than being copied pro forma. It would also be useful to evaluate the effectiveness of coordination mechanisms within the South African Government, and with provincial and municipal administrations. An interesting phenomenon to monitor would be the spill-over of laws, policies and practices from South Africa into other SADC countries, and the ways in which they are adapted, rather than just being copied. The question of the availability of IMSI-grabbers is contentious and vexed, but requires work on their use by the Presidency, SSA, SAPS, criminals and, perhaps, foreign powers and terrorists. Equally, the use of surveillance malware requires further work, though this would be very difficult.

References

African Union (AU). (2014). Convention on Cyber Security and Personal Data Protection. Addis Ababa. Retrieved from https://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Ahmed, S. (1999). Being intelligent about intelligence: SA parliamentary oversight. *South African Journal of International Affairs, 6*(2), 191-198. https://doi.org/10.1080/10220469909545273

Akamai. (2016). *How the Mirai botnet is fuelling today's largest and most crippling DDOS attacks.* Cambridge, MA. Retrieved from https://www.akamai.com/uk/en/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf

Akamai. (2017). *State of the Internet/security Q4 2016 report.* Cambridge, MA. Retrieved from https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

Beresford, A. (2015). Power, patronage, and gatekeeper politics in South Africa. *African Affairs, 114*(455), 226-248. https://doi.org/10.1093/afraf/adu083

Booysen, S. (2015). *Dominance and decline: The ANC in the time of Zuma.* Johannesburg: Wits University Press.

Business Process Enabling South Africa (BPESA). (n.d.). Website. Retrieved from http://www.bpesa.org.za/

Breckenridge, K. (2005). The biometric state: the promise and peril of digital government in the new South Africa. *Journal of Southern African Studies, 31*(2), 267-282. https://doi.org/10.1080/03057070500109458

AJIC 20-21-Jan-18-22h19.indd 102-103 1/21/2018 10:43:15 PM

Brito, J., & Watkins, T. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *Harvard National Security Journal, 3*(1), 39-84. Retrieved from http://harvardnsj.org/2011/12/loving-the-cyber-bomb-the-dangers-of-threat-inflation-in-cybersecurity-policy/

Bronk, H., Thorbruegge, M., & Hakkaja, M. (2006). *A step-by-step approach on how to setup a CSIRT.* Heraklion: European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/csirt-setting-up-guide

Burchell, J. (2009). The legal protection of privacy in South Africa: A transplantable hybrid. *Electronic Journal of Comparative Law, 13*(1), 1-26. Retrieved from http://www.ejcl.org/131/art131-2.pdf

Chertoff, M. (2008). The cybersecurity challenge. *Regulation & Governance, 2*(4), 480-484. https://doi.org/10.1111/j.1748-5991.2008.00051.x

Cisco. (2017). *Annual cybersecurity report.* San Jose, CA. Retrieved from http://www.cisco.com/c/en/us/products/security/security-reports.html

Cloete, F. (2012). E-government lessons from South Africa 2001-2011: Institutions, state of progress and measurement. *The African Journal of Information and Communication (AJIC), 12,* 128-142. https://doi.org/10.23962/10539/19712

Cohen, T. (2001). "But for the nicety of knocking and requesting a right of entry": Surveillance law and privacy rights in South Africa. *South African Journal of Information and Communication (SAJIC), 1*, 1-18. https://doi.org/10.23962/10539/19841

Conradis, B. (2017, February 21). German regulator tells parents to destroy "spy" doll Cayla. *Deutsche Welle*. Retrieved from http://www.dw.com/en/german-regulator-tells-parents-to-destroy-spy-doll-cayla/a-37601577

Council of Europe. (2001). Convention on Cybercrime. *ETS No.185.* Strasbourg. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Centre for Research in Information and Cyber Security (CRICS). (n.d.). Website. Nelson Mandela University. Retrieved from http://crics.mandela.ac.za/

Cyber Security Awareness (CSA). (n.d.). Website. University of South Africa (UNISA). Retrieved from http://eagle.unisa.ac.za/elmarie/

Centre for Cyber Security (CSI). (n.d.).Website. Retrieved from http://adam.uj.ac.za/csi/

Corruption Watch (CW). (2016). *Annual report.* Johannesburg.

Cwele, S. C. (2015, October 30). Minister Siyabonga Cwele: Launch of Cybersecurity Hub. Text of speech. Retrieved from http://www.gov.za/speeches/minister-siyabonga-cwele-launch-cybersecurity-hub-30-oct-2015-0000

Dean, B. (2016). Natural and quasi-natural experiments to evaluate cybersecurity policies. *Journal of International Affairs, 70*(1), 139-160. Retrieved from https://jia.sipa.columbia.edu/natural-and-quasi-natural-experiments-evaluate-cybersecurity-policies

Deloitte. (2015). *Outsourcing is good for job creation in South Africa.* Johannesburg: Deloitte & Touche.

Department of Defence. (2015a). *South African defence review.* Pretoria. Retrieved from http://www.dod.mil.za/documents/defencereview/Defence%20Review%202015.pdf

Department of Defence. (2015b). *Department of Defence strategic plan for 2015 to 2020.* Pretoria. Retrieved from http://www.dod.mil.za/documents/annualreports/DoD%20Annual%20Performance%20Strat%20Plan%202403.pdf

Department of Defence. (2016). *Annual report 2015/16.* Pretoria. Retrieved from http://www.gov.za/sites/www.gov.za/files/DoD_Annual_Report_2015-2016%20RGB.pdf

Department of Defence. (2017). *Annual performance plan.* Pretoria. Retrieved from http://www.dod.mil.za/documents/app/2017/DoD%20APP%202017%20web%2010%20March.pdf

Department of Public Service and Administration (DPSA). (2001). *Electronic government: The digital future: A public service IT policy framework.* Pretoria.

DPSA (2012). *Public service corporate governance of information and communication technology policy framework.* Pretoria. Retrieved from http://www.gov.za/sites/www.gov.za/files/CGICTPolicyFramework.pdf

DPSA. (n.d.). Website. Retrieved from http://www.dpsa.gov.za/

Donovan, K. P. (2015). The biometric imaginary: Bureaucratic technopolitics in post-apartheid welfare. *Journal of Southern African Studies, 41*(4), 815-833. https://doi.org/10.1080/03057070.2015.1049485

Department of Telecommunications and Postal Services (DTPS). (2016). *National Integrated ICT Policy White Paper. Government Gazette, 176*(40325). Retrieved from http://www.gov.za/sites/www.gov.za/files/40325_gon1212.pdf

DTPS. (2017a). Cybersecurity: Department & SABRIC briefing, with Deputy Minister present. Retrieved from https://pmg.org.za/committee-meeting/24042/

DTPS. (2017b). *National e-government strategy and roadmap: Digitizing government services. Government Gazette, 622*(40772).

DTPS. (2017c). Invitation to nominate members of the National Cyber Security Advisory Council. Retrieved from https://www.dtps.gov.za/index.php?option=com_content&view=article&id=703:national-cybersecurity-advisory-council&catid=51:popular-topics&Itemid=298

DTPS. (2017d). *National e-Government Strategy and Roadmap. Government Gazette, 629*(41241).

EFF v Speaker of the National Assembly, ZACC 11 (Constitutional Court March 31, 2016).

Electronic Communications Security - Computer Security Incident Response Team (ECS-CSIRT). (n.d.). Website. Retrieved from http://www.ssa.gov.za/CSIRT.aspx

ENCA. (2013, August 12). Answers wanted in alleged Pule assassination plot. Retrieved from https://www.enca.com/south-africa/pule-linked-alleged-assassination-plot

EU. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Brussels. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

EU. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Brussels. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Fachkha, C., & Debbabi, M. (2016). Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization. *IEEE Communications Surveys & Tutorials, 18*(2), 1197-1227. https://doi.org/10.1109/COMST.2015.2497690

Feinstein, A. (2010, June 7). Rise of the tenderpreneurs, the fall of South Africa. *New Statesman*. Retrieved from http://www.newstatesman.com/africa/2010/06/south-world-anc-party-zuma

AJIC 20-21-Jan-18-22h19.indd 104-105 1/21/2018 10:43:16 PM

Forum for Incident Response and Security Teams (FIRST). (n.d.). Website. Retrieved from https://www.first.org/

Freedman, M. (2016, October 10). South Africa: ICT white paper under fire. *Extensia.* Retrieved from http://extensia-ltd.com/south-africa-ict-white-paper-fire/

Fripp, C. (2014, November 11). Cybercrime costs South Africa about R5.8 billion a year. *htxt.africa.* Retrieved from http://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/

Gallens, M. (2016, October 26). Pansy Tlakula appointed as new information regulator. *News24*. Retrieved from http://www.news24.com/SouthAfrica/News/pansy-tlakula-appointed-as-new-information-regulator-20161026

Gibson, J. L. (2016). Reassessing the institutional legitimacy of the South African Constitutional Court: New evidence, revised theory. *Politikon: South African Journal of Political Studies, 43*(1), 53-77. https://doi.org/10.1080/02589346.2016.1155135

Gilardi, F. (2010). Who learns from what in policy diffusion processes? *American Journal of Political Science, 54*(3), 650-666. https://doi.org/10.1111/j.1540-5907.2010.00452.x

Global Network Initiative (GNI). (n.d.). Website. Retrieved from http://www.globalnetworkinitiative.org/

Gonzalez, J. (2005). Computer safety, reliability, and security. In R. Winther, B. A. Gran, & G. Dahll (Eds.), *24th International Conference, SAFECOMP 2005.* Cham, Switzerland: Springer. https://doi.org/10.1007/11563228

Goodin, D. (2017, February 27). *Record-breaking DDoS reportedly delivered by 145,000+ hacked cameras*. Ars Technica. Retrieved from https://arstechnica.co.uk/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Government Accountability Office (GAO). (2017). *Cybersecurity – actions needed to strengthen U.S. capabilities. GAO-17-440T.* Washington, DC. Retrieved from http://gao.gov/products/GAO-17-440T

Grobler, M., & Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. In H. S. Venter, M. Coetzee, & M. Loock (Eds.), *Information security for South Africa (ISSA)* (pp. 1-6). New York: IEEE. https://doi.org/10.1109/ISSA.2010.5588307

Grobler, M., Van Vuuren, J. J., & Leenen, L. (2012). Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. In M. D. Hercheui, D. Whitehouse, W. McIver, & J. Phahlamohlaka (Eds.), *IFIP International Conference on Human Choice and Computers* (pp. 215-225). Berlin: Springer. https://doi.org/10.1007/978-3-642-33332-3_20

Hawker, G. (2003). Missing cadres? List voting and the ANC's management of its parliamentarians in the National Assembly, 1999-2003. *Journal of African Elections, 2*(1), 97-115. Retrieved from http://journals.co.za/content/eisa_jae/2/2/EJC32346

Hawker, G. (2007). Challenges for parliament in South Africa. *Australasian Parliamentary Review, 22*(1), 97-113.

International Multilateral Partnership Against Cyber-Terrorism (IMPACT). (n.d.). Website. Retrieved from http://www.impact-alliance.org/home/index.html

International Telecommunication Union (ITU). (2017). *Global cybersecurity index*. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

iSolv Technologies. (n.d.). Website. Retrieved from https://isolvtech.com/

IT News Africa. (2013, October 15). South Africa launches National Cyber Security Advisory Council. Retrieved from http://www.itnewsafrica.com/2013/10/south-africa-launches-national-cyber-security-advisory-council/

Johnson, R. W. (2017). *How long will South Africa survive? The crisis continues.* Johannesburg: Jonathan Ball.

Joint Standing Committee on Intelligence (JSCI). (n.d.). Website. Retrieved from http://www.parliament.gov.za/live/content.php?Item_ID=215&CommitteeID=132

JSCI. (2015). *Report of the Joint Standing Committee on Intelligence on activities of the Committee after 5 months of establishment.* Cape Town. Retrieved from https://pmg.org.za/tabledcommitteereport/

Jonker, M. (2015, November 2). One in ten SA businesses have experienced cyberattacks. Grant Thornton. Retrieved from https://www.grantthornton.co.za/insights/articles/one-in-ten-sa-businesses-have-experienced-cyber-attacks-in-the-past-year/

Justice, Crime Prevention and Security Cluster (JCPS). (n.d.). About. Retrieved from http://www.gov.za/about-government/justice-crime-prevention-and-security-cluster

King Committee. (2016). *King IV: Report on corporate governance.* Johannesburg: The Institute of Directors in Southern Africa.

Kirlidog, M., Van der Vyver, C., Zeeman, M., & Coetzee, W. (2016). Unfulfilled need: Reasons for insufficient ICT skills in South Africa. *Information Development*, 1-15. https://doi.org/10.1177/0266666916671984

Klaaren, J. (2015). The judicial role in defining national security and access to information in South Africa. *Democracy and Security, 11*(3), 275-297. https://doi.org/10.1080/17419166.2015.1067613

Koelble, T. (2017). One-party dominance and public sector corruption in South Africa: Consequences for democracy. In P. Harfst, I. Kubbe, & T. Poguntke (Eds.), *Parties, governments and elites* (pp. 281-300). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-17446-0_14

Kritzinger, E. (2014). Online safety in South Africa – a cause for growing concern. In H. S. Venter, M. Laack, M. Coetzee, & M. M. Elaf (Eds.), *Information Security for South Africa (ISSA) 2014.* New York: IEEE. https://doi.org/10.1109/ISSA.2014.6950502

Kynoch, G. (2005). Crime, conflict and politics in transition-era South Africa. *African Affairs, 104*(416), 493-514. https://doi.org/10.1093/afraf/adi009

Lacson, W., & Jones, B. (2016). The 21st century DarkNet market: Lessons from the fall of Silk Road. *International Journal of Cyber Criminology, 10*(1), 40-61. https://doi.org/10.5281/zenodo.58521

Letsoalo, M. (2017, September 8). "Spooks" cash "used to spy on Cyril Ramaphosa". *Mail & Guardian*. Retrieved from https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril

Liff, A. P. (2012). Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies, 35*(3), 401-428. https://doi.org/10.1080/01402390.2012.66325 2

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cyber Security, 1*(1), 53-67. https://doi.org/10.1093/cybsec/tyv003

Lotz, B. (2017, October 23). Your ID number is online – why that's bad and what you can do. *Mail & Guardian*. Retrieved from https://mg.co.za/article/2017-10-23-your-id-number-is-online-why-thats-bad-and-what-you-can-do

AJIC 20-21-Jan-18-22h19.indd 106-107 1/21/2018 10:43:16 PM

Mapisa-Nqakula, N. (2016, May 11). Minister Nosiviwe Mapisa-Nqakula: Defence and Military Veterans Dept Budget Vote 2016/17. Text of speech. Retrieved from http://www.gov.za/speeches/minister-nosiviwe-mapisa-nqakula-defence-and-military-veterans-dept-budget-vote-201617-11

Matthews, J., Ginwala, F., & Nathan, L. (2008). *Intelligence in a constitutional democracy: A report to the Minister for Intelligence Services.* Pretoria: Ministry of Intelligence Services.

Mawela, T. (2017). Exploring the role of social media in the G2C relationship: A South African perspective. *Information Development, 33*(2), 117-132. https://doi.org/10.1177/0266666916639743

Mbelli, T. M., & Dwolatzky, B. (2016). Cyber security, a threat to cyber banking in South Africa: An approach to network and application security. In M. Qiu, L. Tao, & J. Niu (Eds.), *IEEE 3rd International Conference on Cyber Security and Cloud Computing.* New York: IEEE Computer Society. https://doi.org/10.1109/CSCloud.2016.18

McKinley, D. T. (2013). State and civil-political rights in South Africa. *Strategic Review for Southern Africa, 35*(1), 118-134.

McKinley, D. T. (2014). Secrecy and power in South Africa. In G. M. Khadiagala, P. Naidoo, D. Pillay, & R. Southall (Eds.), *New South African review 4: A fragile democracy - twenty years on.* Johannesburg: Wits University Press.

McKinley, D. T. (2016). *New terrains of privacy in South Africa: Biometrics/smart identification systems, CCTV/ALPR, drones, mandatory SIM card registration and FICA.* Johannesburg: Right2Know Campaign & Media Policy & Democracy Project. Retrieved from http://www.r2k.org.za/2016/12/15/research-new-terrains-of-privacy-in-south-africa/

McLeod, D. (2017, January 25). ICT white paper "not constitutional". *TechCentral.* Retrieved from https://techcentral.co.za/ict-white-paper-unconstitutional/71367/

Meseguer, C. (2005). Policy learning, policy diffusion, and the making of a new order. *The Annals of the American Academy of Political and Social Science, 598*(1), 67-82.

Microsoft. (2017). *Microsoft security intelligence report*. Retrieved from https://www.microsoft.com/en-us/security/Intelligence-report

Minister of Justice. (2015). *[draft] Cybercrimes and Cybersecurity Bill*. Minister of Justice and Correctional Services. Retrieved from http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf

Minister of Justice. (2017). *Cybercrimes and Cybersecurity Bill.* Minister of Justice and Correctional Services. Retrieved from http://pmg-assets.s3-website-eu-west-1.amazonaws.com/CyberCrimes-Bill-2017.pdf

Mokgoro, Y. (2014). *Report on interception of private communications.* Cape Town: Parliament of the Republic of South Africa. Retrieved from http://pmg-assets.s3-website-eu-west-1.amazonaws.com/160127report.pdf

Moyo, A. (2016a, July 15). Armscor plays down hack. *ITWeb*.

Moyo, A. (2016b, July 25). Armscor beefs up security. *ITWeb*.

Mutula, S. M., & Mostert, J. (2010). Challenges and opportunities of e-government in South Africa. *The Electronic Library, 28*(1), 38-53. https://doi.org/10.1108/02640471011023360

Nathan, L. (2009). Lighting up the intelligence community: An agenda for intelligence reform in South Africa. *African Security Review, 18*(1), 91-104. https://doi.org/10.1080/10246029.2009.9627518

Nathan, L. (2010). Intelligence bound: The South African Constitution and intelligence services. *International Affairs, 86*(1), 195-210. https://doi.org/10.1111/j.1468-2346.2010.00875.x

National Cybersecurity Hub (NCH). (n.d.). Website. Retrieved from https://www.cybersecurityhub.gov.za

Nelson Hall. (2015). *Analysis of South Africa as a BPO delivery location.* Cape Town: Business Process Enabling South Africa (BPESA).

North, D. C. (1990). *The economics of public issues* (8th ed.). New York: Harper and Row.

Norton. (2016). *2016 Norton cyber security insights report*. Retrieved from https://uk.norton.com/cyber-security-insights

Nyanda, S. (2010, February 19). Notice of intention to make South African National Cybersecurity Policy. *Government Gazette, 536*(32963).

O'Keeffe v Argus Printing and Publishing Company Ltd [1954] (3) SA 244 (C).

Organisation for Economic Co-operation and Development (OECD). (2012). *Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy.* Paris.

OECD. (2015). *Digital security risk management for economic and social prosperity.* Paris.

OECD. (2017). *Economic survey of South Africa 2017.* Paris. Retrieved from http://www.oecd.org/eco/surveys/economic-survey-south-africa.htm

Oversight Committee. (2016). *Law enforcement use of cell-site simulation technologies: privacy concerns and recommendations.* Washington, DC: Committee on Oversight and Government Reform, US Congress. Retrieved from https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf

Oxford, A. (2013, October 16). Who's who on South Africa's new Cyber Security Advisory Council. *htxt.africa*. Retrieved from http://www.htxt.co.za/2013/10/16/whos-who-on-south-africas-new-cyber-security-advisory-council/

Palmer, D. (2017, February 1). Misconfigured firewall blamed for hospital ransomware infection. *ZDnet*. Retrieved from http://www.zdnet.com/article/misconfigured-firewall-blamed-for-hospital-ransomware-infection/

Paret, M. (2016). Contested ANC hegemony in the urban townships: Evidence from the 2014 South African election. *African Affairs, 115*(460), 419-442. https://doi.org/10.1093/afraf/adw025

Peekhaus, W. (2014). South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence. *Journal of Information Policy, 4*, 570-596. https://doi.org/10.5325/jinfopoli.4.2014.0570

Portfolio Committee on Justice and Correctional Services. (2017). Have your say: The Cybercrimes and Cybersecurity Bill. Retrieved from https://www.parliament.gov.za/committee-notice-details/29

Primedia Broadcasting v Speaker (784/2015) [2016] ZASCA 142 (29 September 2016). Retrieved from http://www.saflii.org/za/cases/ZASCA/2016/142.html

Privacy International (PI). (2014, January 30). South African government still funding VASTech, knows previous financing was for mass surveillance. Retrieved from https://www.privacyinternational.org/node/305

PI. (2016). *State of privacy South Africa.* London. Retrieved from https://www.privacyinternational.org/node/968

AJIC 20-21-Jan-18-22h19.indd 108-109 1/21/2018 10:43:16 PM

Public Accounts Committee (PAC). (2017). *Protecting information across government. HC 769*. London: House of Commons. Retrieved from http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/publications/

Republic of South Africa (RSA). (1994). *White Paper on Intelligence.* Pretoria. Retrieved from http://www.gov.za/documents/intelligence-white-paper

RSA. (2006). Cryptography Regulations R.216. *Government Gazette, 489*(28594). Retrieved from http://www.gov.za/sites/www.gov.za/files/28594.pdf

RSA. (2010a). *Outputs and measures: Outcome 3: All people in South Africa are and feel safe*. Retrieved from https://www.gov.za/sites/default/files/outcome-3.pdf

RSA. (2010b). *Delivery agreement for outcome three: "All people in South Africa are and feel safe".* Pretoria.

RSA. (2016). Structure and functions of the South African government. Retrieved from http://www.gov.za/node/537988

Research ICT Africa (RIA). (2016). Submission to the Parliament of South Africa on "The cost to communicate in South Africa". Cape Town. Retrieved from http://www.researchictafrica.net/publications/Other_publications/2016_South%20Africa_Cost%20to%20Communicate%20Submission_RIA%20.pdf

Reuters. (2017, February 8). NSA contractor indicted over mammoth theft of classified data. Retrieved from http://www.reuters.com/article/us-usa-cybersecurity-nsa-contractor-idUSKBN15N2N4

Roberts, J. J. (2017, March 10). Sex toy maker pays $3.75 million to settle "smart" vibrator lawsuit. *Fortune*. Retrieved from http://fortune.com/2017/03/10/sex-toy-maker-settlement-smart-vibrator-lawsuit/

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2), 256-286. https://doi.org/10.1002/pam.20567

Roos, A. (2016). Data protection law in South Africa. In A. B. Makulilo (Ed.), *African data privacy laws* (pp. 189-227). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-47317-8

Roux, T. (2016). Constitutional courts as democratic consolidators: Insights from South Africa after 20 Years. *Journal of Southern African Studies, 42*(1), 5-18. https://doi.org/10.2139/ssrn.2501176

Schofield, A. (2016). *2016 JCSE ICT skills survey.* Johannesburg: Joburg Centre for Software Engineering (JCSE).

Schofield, A. (2017). *2017 JCSE ICT Skills Survey.* Johannesburg: Joburg Centre for Software Engineering (JCSE).

Schwab, A. (2016). *Recommendation for a second reading. A8-0211/2016.* Brussels: European Parliament. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0211+0+DOC+PDF+V0//EN

Shaw, M. (2017). *Hitmen for hire: Exposing South Africa's underworld.* Johannesburg: Jonathan Ball.

Shaw, M., & Thomas, K. (2016). The commercialization of assassination: "Hits" and contract killing in South Africa, 2000-2015. *African Affairs*, 1-24. https://doi.org/10.1093/afraf/adw050

Siemens. (2016). *African digitalisation maturity report 2017.* Munich. Retrieved from https://www.siemens.com/content/dam/internet/siemens-com/global/company/topic-areas/digitalization/pdf/survey/siemens-african-digitalization-report.pdf

Solomon, H. (2012). The demise of South Africa's intelligence community and the erosion of the liberal democratic state. *Africa Review, 4*(2), 157-172.

South African Banking Risk Information Centre (SABRIC). (n.d.). Website. Retrieved from https://www.sabric.co.za

South African Cyber Security Academic Alliance (SACSAA). (n.d.). Website. Retrieved from http://www.cyberaware.org.za/

South African Law Reform Commission (SALRC). (2003). *Privacy and data protection – issue paper.* Pretoria.

SALRC. (2005). *Privacy and data protection.* Pretoria. Retrieved from http://www.justice.gov.za/salrc/dpapers/dp109.pdf

Southall, R. (1994). The South African elections of 1994: The remaking of a dominant-party state. *The Journal of Modern African Studies, 32*(4), 629-655. https://doi.org/10.1017/S0022278X00015883

Southall, R. (2015). The coming crisis of Zuma's ANC: The party state confronts fiscal crisis. *Review of African Political Economy, 43*(147), 73-88. https://doi.org/10.1080/03056244.2015.1083970

State Security Agency (SSA) (2015). *The National Cybersecurity Policy Framework (NCPF). Government Gazette* (39475). Retrieved from https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Statistics South Africa (StatsSA). (2017). *Poverty trends in South Africa: An examination of absolute poverty between 2006 and 2011, 2015.* Pretoria.

Symantec. (2017). *Internet security threat report*. Retrieved from https://www.symantec.com/security-center/threat-report

Times Live. (2016, January 25). Cyber-crime: SA the most targeted on the continent. Retrieved from http://www.timeslive.co.za/local/2016/01/25/Cyber-crime-SA-the-most-targeted-on-the-continent1

Trusler, J. (2003). South African e-government policy and practices: A framework to close the gap. In R. Traunmüller (Ed.), *Electronic Government. EGOV 2003* (pp. 504-507). Berlin & Heidelberg: Springer. https://doi.org/10.1007/10929179_95

Turok, B. (2017). South Africa's lopsided economy. *New Agenda: South African Journal of Social and Economic Policy, 2017*(65), 6-9. Retrieved from http://hdl.handle.net/10520/EJC-900a1510b

UN General Assembly. (2010). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. A/RES/64/211.* New York. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

UN Human Rights Committee. (2016). *Concluding observations on the initial report of South Africa. CCPR/C/ZAF/CO/1.* Geneva.

UN Office on Drugs and Crime (UNODC). (2017). *Emerging crimes*. Retrieved from http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html#Cybercrime

Van der Westhuizen, C. (2013). South Africa and national security. *Index on Censorship*, *42*(2), 62-64. https://doi.org/10.1177/0306422013494290

AJIC 20-21-Jan-18-22h19.indd 110-111 1/21/2018 10:43:16 PM

Van Heerden, R., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. In IEEE (Ed.), *IST-Africa Week Conference.* New York: IEEE. https://doi.org/10.1109/ISTAFRICA.2016.7530663

Van Vuuren, J. J., Phahlamohlaka, J., & Leenen, L. (2012). Governance of cybersecurity in South Africa. Paper presented at11th European Conference on Information Warfare and Security, Laval, France, 5-6 July. Retrieved from http://hdl.handle.net/10204/6207

Van Vuuren, J. J., Phahlamohlaka, J., Leenen, L., & Zaaiman, J. (2014). An approach to governance of cybersecurity in South Africa. In Information Resources Management Association (Ed.), *Cyber behavior: concepts, methodologies, tools, and applications* (pp. 1583-1597). Hershey: IGI Global. https://doi.org/10.4018/978-1-4666-5942-1.ch082

VASTech. (n.d.). Website. Retrieved from http://www.vastech.co.za/

Vodafone. (2014). *Law enforcement disclosure report*. Retrieved from http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

Volz, D., & Shepardson, D. (2017, September 8). Criticism of Equifax data breach response mounts, shares tumble. *Reuters*. Retrieved from https://www.reuters.com/article/us-equifax-cyber/criticism-of-equifax-data-breach-response-mounts-shares-tumble-idUSKCN1BJ1NF

Wassenaar Arrangement. (2017). *The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies*. Retrieved from http://www.wassenaar.org

Watney, M. (2015). State-on-nationals' electronic communication surveillance in South Africa: A murky legal landscape to navigate? In H. S. Venter, M. Loock, M. Coetzee, M. M. Eloff, & S Flowerday (Eds.), *Information Security for South Africa (ISSA)* (pp. 1-6). Johanesburg: IEEE. https://doi.org/10.1109/ISSA.2015.7335047

Wiik, J., & Kossakowski, K.-P. (2005). Dynamics of incident response. In FIRST (Ed.), *FIRST 2005* (pp. 1-24). Retrieved from https://first.org/conference/2005/papers/speaker14-paper-1.pdf

Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. (2006). Effectiveness of proactive CSIRT Services. Paper presented at Forum for Incident Response and Security Teams (FIRST), Baltimore, MD, 25-30 June 2006. Retrieved from https://www.first.org/conference/2006/papers/kossakowski-klaus-papers.pdf

Wolf, L. (2011). The prosecuting discretion: A power under administrative law or criminal law? *Tydskrif vir die Suid-Afrikaanse Reg, 2011*(4), 703-729.

Wolf, L. (2015). The National Prosecuting Authority (NPA) in a nimbus between the executive and the judicature. *Administratio Publica, 23*(4), 30-53.

Wolfpack. (2013). *2012/13 The South African cyber threat barometer.* Johannesburg. Retrieved from http://us-cdn.creamermedia.co.za/assets/articles/attachments/41981_sa_2012_cyber_threat_barometer_medium_res.pdf

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired.* Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zuma v DA (771/2016 & 1170/2016) [2017] ZASCA 146 (13 October 2017). Retrieved from http://www.saflii.org/za/cases/ZASCA/2017/146.html

An Analysis of Cyber-Incidents in South Africa

Brett van Niekerk
Honorary Research Fellow, School of Management, IT and Governance, University of KwaZulu-Natal, Westville, Durban

Abstract
Cybersecurity concerns are present in all nations, but the exact nature of the threats differs depending on the country and/or region. Therefore there is a need to assess the threats and impacts for specific countries. This article presents a high-level analysis of "newsworthy" cyber-incidents that affected South Africa. The 54 incidents that are considered are categorised according to impact type, perpetrator type, and victim type, and the trends are assessed. It was found that the most common impact type was data exposure, which was also one that had increased noticeably in recent years. The most prevalent perpetrator type was found to be hacktivists, which had also exhibited a recent increase in activity. A particularly concerning trend was the recent high number of incidents of data exposure caused by error, a trend running contrary to the drive to improve cybersecurity. It was also found that of the incidents considered, 54% targeted state-owned or political entities as victims. In general, the results appeared consistent with global reported trends.

Keywords
advanced persistent threat, data breach, defacement, distributed denial of service, financial theft, system penetration

DOI: https://doi.org/10.23962/10539/23573

Recommended citation
Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113-132. https://doi.org/10.23962/10539/23573

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

AJIC 20-21-Jan-18-22h19.indd 112-113 1/21/2018 10:43:17 PM

1. Introduction

Concerns over cybersecurity are growing globally, fuelled by reports of ever-larger data breaches and a lack of skilled cyber-security professionals (Fearn, 2017). However, most organisations and nations seem to be at a loss of how to effectively respond. For instance, even though UK organisations have been found to generally consider cyber-security important, only 44% have implemented a cyber-security strategy (Ashford, 2017). Slay, quoted in Tate (2017), indicates that Australia has a lack of experienced cyber-security professionals. Reports from Kenya indicate that cyber-security is lagging, despite increased uptake of Internet services (Matinde, 2017). Similarly, reports in South Africa suggest that cyber-security is "reaching a critical point" in the country (*SABC News*, 2017).

Whilst the concerns of security are common across all regions, the exact nature of the threat types and motivations vary geographically as illustrated in Brown and Rudis (2017). Therefore it is necessary to assess the relevant trends in one's region to ensure the security measures and strategies are aligned to the threat activity. This article presents a high-level analysis of "newsworthy" cyber-incidents that targeted South Africa. The next section scans relevant literature, followed by a description of the methodology used. Summaries of the incidents are provided, after which the analysis is presented. The results are discussed with reference to the literature, and the article is then concluded.

2. Literature

There are different types of cyber-attacks, and some receive more hype than others. Receiving significant attention are instances of nation-state cyber-espionage, which are closely linked to advanced persistent threats (APTs). These have been found to be constantly present in the global cyber-threat environment, but the number of organisations affected by these is low unless they are in the specific target group for the attackers (Brown & Rudis, 2017). Ransomware is another threat operated by cyber-criminals that is receiving much attention. The number of ransomware payloads increased internationally from 18% of detections in January 2016 to 66% in November 2016. Only 1% of ransomware detections occur in Africa meaning that all the other populated continents, however, are much more heavily affected (Malwarebytes Labs, 2017).

In addition to the state-sponsored persistent attacks and criminal ransomware attacks mentioned above, the major threat types include: insider threats, either malicious or accidental, resulting in security incidents; attacks by hacktivists who are politically or ideologically motivated; and attacks by individual hackers who are trying to learn or show off, such as the "script kiddies" who make use of existing tools (Andress & Winterfield, 2014).

It has been reported that South Africa lost approximately ZAR50 billion in 2014 due to cyber-incidents, and that over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (*SABC News*, 2017). Estimates in 2011 put the financial losses from cyber-attacks at ZAR 3.7 billion in direct losses and ZAR6.5 billion in indirect costs (Norton South Africa, 2012). The threat will become more widespread going forward as the number of South African Internet users increases, aided by the African continent's increasing undersea capacity (Song, 2017).

The South African legislative context relating to online privacy and security is expanding. The foundational act from which the other acts derive is the Electronic Communications and Transactions Act (ECT) of 2002 (RSA, 2002). The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) was also promulgated in 2002 (RSA, 2002). The Protection of Personal Information (POPI) Bill was released in 2009, and enacted in 2013 (RSA, 2009; RSA, 2013), but has yet to come into full effect. The National Cybersecurity Policy Framework was released at the end of 2015 (SSA, 2015), followed by drafts of the Cybercrimes and Cybersecurity Bill (Department of Justice and Correctional Services, 2017).

Patrick (2015) has illustrated a lack of information flow regarding cyber-security in government departments, and the need for response teams. Chandarman (2016) has found that South African students sometimes over-estimate their knowledge regarding security threats and techniques, possibly putting them at risk. Dlamini and Modise (2012) interrogated awareness initiatives in the country up to 2012 and found that the focus of the initiatives appeared to be on tertiary institutions and schools. It thus seems clear that the cyber-security landscape in South Africa has room to improve.

3. Methodology

The research for this article analysed a number of documented cyber-incidents related to South Africa. The data were identified through scrutiny of published reports, news items, postings to email mailing lists, cross-referencing via document reference lists, and targeted online searches for additional information on documented incidents. A total of 54 incidents spanning 23 years, from April 1994 to end-2016, were identified. These were classified in a manner similar to that used in the work of Miller and Rowe (2012) and Van Niekerk (2017). Miller and Rowe (2012) analysed security incidents related to industrial control systems (ICS), categorising them by impact type and attack vector. In Van Niekerk (2017), security incidents affecting the transportation sector were considered, categorised by threat type and impact.

AJIC 20-21-Jan-18-22h19.indd 114-115 1/21/2018 10:43:17 PM

Impact categories
For this study, the impacts were categorised as follows:

- data exposure, where records have been released;
- financial, where there was an attempt (successful or otherwise) to steal money;
- denial of service, where operations or services were affected;
- defacement, where webpages were altered;
- data corruption, where data was modified; and
- system penetration, where illegitimate access to networks or systems was achieved, but no other activity was apparent.

Perpetrator categories
The categorisation of the perpetrators (or key perpetuating factors) was as follows:

- hacktivist, where the perpetrator was affiliated to online activist groups making political statements;
- criminal, where the perpetrator was affiliated to criminal groups usually seeking financial gain;
- accidental/misconfiguration, where the incident was as a result of misconfigured systems;
- individual hacker, where the incident appeared to be to prove or develop individual skills;
- nation-state espionage, where the incident relates to state-sponsored threats;
- malware, where malware was discovered but no perpetrator or motivation can be established; and
- insider, where the perpetrator had legitimate access but acted maliciously for personal gain or reasons.

The incidents were analysed according to perpetrators and impacts, in terms of overall prevalence and trends over time. A pivot table is used to determine the prevalent threat-impact pairs.

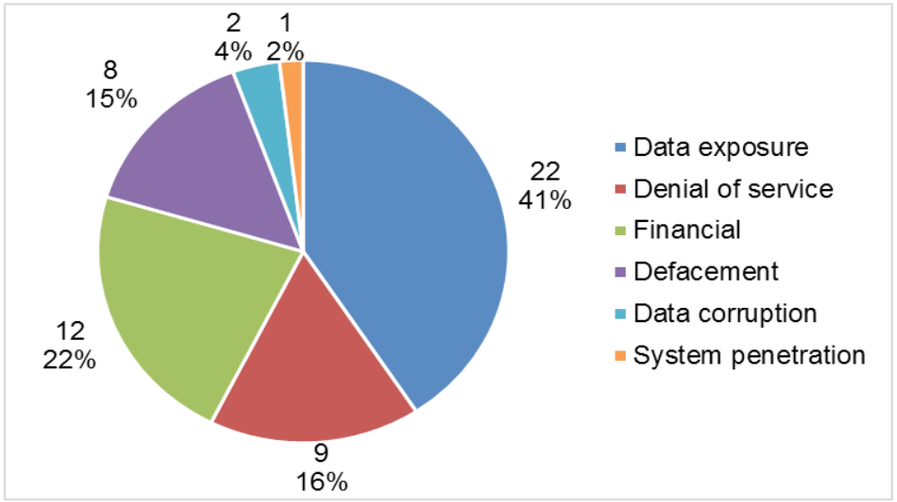
Victim categories
In order to determine if there is a noticeable relationship between the threat types and impacts associated with public organisations, the victims were categorised as:

- state/political organisations; or
- other.

4. Findings and analysis

Impact type
Figure 1 below shows the percentage distribution of the 54 incidents across the six impact types. As is evident, data exposure is the most prominent impact type. Financial, denial of service. and defacement are also noticeable.

Figure 1: Impact type



The findings are detailed according to their impact categories, moving from the most common impact category (data exposure) to the two least-common categories (data corruption, system penetration).

Data exposure
Data exposure was found to be the most common impact category. In 2008, the whistleblower site Wikileaks posted an unredacted version of a Competition Commission report about possible unethical practices by South African banks after removing the redaction (HomeGrownHoney, 2009). In 2010, a state hospital in the Western Cape was found to have an insecure site, and thousands of patient records could be accessed (Stone, 2010).

Advanced persistent threat (APTs) infections were also documented. An organisation in South Africa fell victim to the APT1 espionage group attributed to Chinese hackers, with the first major report occurring in 2010 (Mandiant, 2013). In 2012 the

AJIC 20-21-Jan-18-22h19.indd 116-117 1/21/2018 10:43:17 PM

Red October cyber-espionage campaign (attributed to Russian hackers) was detected, after having possibly operating for five years undetected, with various targets in a number of countries affected, including infecting a diplomatic organisation in South Africa (Limer, 2013; Paganini, 2013).

Servers hosting the espionage tool FinFisher, usually employed by governments to track dissent, were detected in South Africa in 2013. The South African government denied using this tool (Vermeulen, 2013). Also in 2013, the Sednit/APT28 cyber-espionage campaign, attributed to Russian hackers, targeted South African embassies via an infected document sent to the embassies purporting to be from the Department of International Relations and Cooperation (ESET, 2016; FireEye, 2014).

The South African Police Service suffered a hack in 2013 that resulted in the release of approximately 16,000 details of whistleblowers and victims. The attack appeared to be by the group Anonymous in response to the police killings of striking mineworkers at the Marikana mine (Roane, 2013; Tubbs, 2013). Also in 2013, a fast-food outlet's point-of-sale system was infected with the Dexter malware designed to steal customers' credit card information (*MyBroadband*, 2013b). (Though this breach resulted in financial loss to the banks, the attack listed here only compromised the credit card information, and will therefore was classed as data exposure.)

Accidental data exposure incidents also occurred in 2013. A flaw in mobile operator Vodacom's portal allowed any subscriber to access high level account summary information linked to any phone number (Muller, 2013). The City of Johannesburg's invoicing portal was found to have vulnerabilities that could expose personal information, and the website was taken offline by the City – but then appeared to be operational a few days later with the vulnerability still present (*MyBroadband*, 2013a).

The year 2014 also saw both accidental and malicious data exposures. A flaw was discovered in mobile operator Cell C's portal, allowing access to a number of customer records (*MyBroadband*, 2014). Altech Autopage suffered an accidental release of records (Patrick, 2015; Safenet, 2014). The South African National Roads Agency Limited (Sanral) E-Toll website was hacked, making the site vulnerable to release of personal details (Vermeulen, 2014). WooThemes was compromised, giving hackers access to financial information (Patrick, 2015; Safenet, 2014).

In 2016, Anonymous launched #OpAfrica, and its first South African target was an online job portal, V-Report, compromising 33,000 records (Vermeulen, 2016a). The state's Government Communication and Information System (GCIS) was compromised shortly after V-Report, exposing the data of 1,500 government employees (Fripp, 2016; Vermeulen, 2016a). A number of web pages hosted by an

unnamed service provider were the next target for #OpAfrica, with 2,500 websites claimed to have been compromised (Fripp, 2016). Hackers affiliated with #OpAfrica compromised the state-owned arms procurement agency Armscor's invoicing portal, releasing a number of purchasing information records (Van Zyl, 2016c). Cinema chain Ster Kinekor was hacked, with a release of approximately 6 million records in 2016 (Cave, 2017). The Chinese-linked group known as APT10 were involved in the Cloud Hopper espionage campaign in late 2016, or which there were South African victims (PwC and BAE Systems, 2017). As the majority of infections were late 2016, it is assumed this is the compromise date for the South African victims.

Accidental exposure again featured in 2016. The eThekwini Municipality (Durban) e-services portal was found to release customer information when the URL was edited, and the website was taken down to correct the error (Venktess, 2016). The e-billing portal of mobile operator MTN was found to be providing users with access to bills of other customers, and the website was taken offline to correct the error (*MyBroadband*, 2016).

Financial

The first instance of financial impact identified in the documents occurred in 2003, when Absa bank lost approximately ZAR500,000 due to a hack (Thiel, 2004). Hackers targeted three South African banks in 2006, managing to transfer cash from bank accounts into prepaid accounts held with mobile operators. It appeared that information gained from key loggers (devices or software to record a user's keystrokes) and phishing were used to conduct the hacks (Oiaga, 2006).

In July 2009, a criminal group acquired, via threats to an engineer at Vodacom, duplicate SIM cards that allowed for interception of online banking one-time PIN codes (OTPs) for bank accounts they had compromised via phishing. The group managed to steal in excess of ZAR7 million from the compromised accounts (Dingle, 2009; Van Rooyen, 2009). The Land Bank initially lost ZAR8 million stolen through fraudulent transfers in December 2010 after hackers compromised the bank's IT security possibly with inside help, but managed to recover most of money (Potgieter, 2011).

A credit card payment provider, PayGate, was compromised in August 2012, affecting four of the major banks and compromising "hundreds of thousands" of credit card details (Arde, 2012, p. 18). Though no details of financial losses were released, it is assumed that the banks suffered financial losses (Ajam, 2012; Arde, 2012). Compromised passwords resulted in the National Department of Water Affairs losing ZAR2.84 million in 2011 (Patrick, 2015; Rasool, 2012). Postbank, the South African Post Office's financial institution, had ZAR42 million stolen in January 2012 after hackers accessed servers via an employee's workstation (Patrick,

AJIC 20-21-Jan-18-22h19.indd 118-119 1/21/2018 10:43:17 PM

2015; Rasool, 2012; Swart & Afrika, 2012). In 2013, over ZAR15 million was lost by the Department of Minerals and Energy after login credentials were stolen by criminals using a keystroke logging device (Patrick, 2015; Tengimfene, 2013).

In 2014, state-owned electricity provider Eskom's payroll system was hacked by employees, but the employees were prevented from making transfers by Eskom's anti-corruption units (Patrick, 2015; Speckman, 2015). In the same year, the Gautrain Management Agency's bank account nearly lost ZAR800 million to a hack (Patrick, 2015; Speckman, 2015). In 2015, the Road Traffic Management Corporation lost ZAR8.5 million to a series of illegal transfer by hackers (Mkhwanazi, 2015; Patrick, 2015). In 2016, Standard Bank was targeted by hackers, who managed to steal approximately ZAR300,000 via thousands of ATMs in Japan (Van Zyl, 2016b).

Denial of service

A South African petrochemical company's supervisory, control and data acquisition system was infected by the PE Sality virus in 2009, denying the operator's visibility of operations for eight hours until the infected servers were recovered (Cusimano, 2010; Pretorius, 2016). The aforementioned Sanral E-Toll website came under a denial-of-service attack in 2012, but the attack was not successful (*SANews*, 2012). It is assumed this attacker was conducted by hacktivists, given the ongoing controversy over the e-toll project.

In 2013, the website of the national ruling party, the African National Congress (ANC), was made inaccessible due to a distributed denial of service (DDoS) attack by Anonymous Africa (different from Anonymous #OpAfrica) (Vermeulen, 2016b). Also in 2013, the Independent Online news website was targeted and access disrupted (Vermeulen, 2016b), and mobile operator MTN and affiliated service providers suffered a service outage due to a DDoS attack (ITNewsAfrica, 2013). MTN again suffered performance degradation in 2015 due to a DDoS attack (TelecomSpeak, 2015).

Anonymous Africa returned in 2016 by targeting the South African Broadcasting Corporation (SABC), whose website was unavailable due to the DDoS attack, with the hackers stating that the attack was in protest against corruption and the recent censoring of protests (Vermeulen, 2016b). Also in 2016, the websites of the news channel ANN7, *The New Age* newspaper, and computing company Sahara were targeted with DDoS attacks, in protest against perceived corruption by their owners and the South African government (Van Zyl, 2016a). A series of denial-of-service attacks was conducted against the Economic Freedom Fighters political party (Gorton, 2016).

Defacement

The websites of five major universities (University of Stellenbosch, Natal University, Rhodes University and the University of the Witwatersrand and University of Cape Town) were defaced by hackers in 2003. Each website appeared to be attacked by a different hacker, and international hackers were suspected (Porter, 2003). In 2004, 45 company websites in Cape Town and Stellenbosch were defaced by a group known as Spykids, who appeared to be motivated by a desire for recognition (Thiel, 2004). In January 2005, hackers from Morocco, known as Team Evil, defaced approximately 260 South African websites, replacing the legitimate websites with anti-US messages (Mbongwa & Makua, 2005).

In 2008, the Democratic Alliance political party's website was compromised and was offline for over a week; a spokesperson stated that it appeared to be common hacking, implying that is was not a targeted or political attack (*Mail & Guardian*, 2008). The ANC Youth League website was defaced, with a fake message supposedly from the then Youth League president Julius Malema stating he was stepping down (Redelinghuis, 2011).

Three government websites were defaced by Moroccan hackers in 2012, protesting the official South Africa position on Western Sahara (Saville, 2012). The Administrative Adjudication of Road Traffic Offences website was defaced by a Bangladeshi hacker in 2013, who posted a message notifying the website owner to secure the website (*ITWeb,* 2013). Approximately 20 websites, including Sasol, were defaced by a Moroccan hacktivist in 2014, again protesting the South African position on Western Sahara (Ackroyd, 2014).

Data corruption, system penetration

These two categories are the smallest, and are therefore presented together. They also represent the earliest three attacks reported. It is reported that in 1994 a right-wing hacker attempted to disrupt the first democratic elections in South Africa, but was detected after moving votes from the ANC to three right wing parties (Plaut, 2010). Stats SA's website was targeted by hackers in 1999, who replaced data with negative comments about Telkom (*BBC News*, 1999). A teenage hacker managed to penetrate through Telkom (the state telephony operator) in 1998, however no damage was done. The teenager was arrested (Reuters, 1998).

Trends in impact type

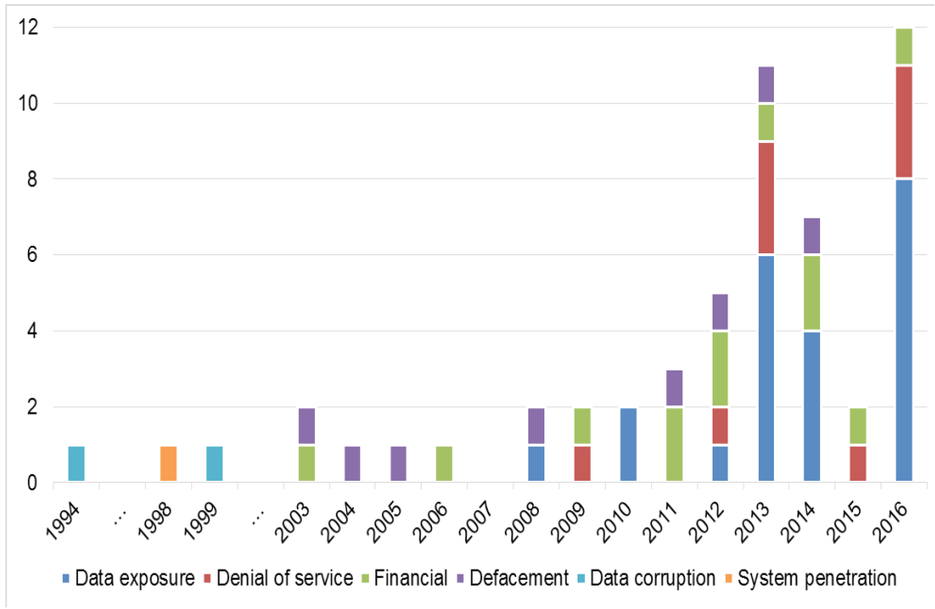
Figure 2 below illustrates the trends for each of the six impact types between April 1994 and end-2016. As can be seen, there were significant spikes in data exposure attacks in 2013, 2014 and 2016, and of denial of service attacks in 2013 and 2016. The number of financial-impact attacks, the third-most-common kind, remained largely stable from 2011 to 2016; and defacements, the fourth-most-frequent mode of attack, remained at a consistent level between 2011 and 2014 but were not found to be present in 2015 or 2016.

AJIC 20-21-Jan-18-22h19.indd 120-121 1/21/2018 10:43:17 PM

Thus, the financial-crime motivation for hacking appears to be remaining somewhat constant, whereas the data exposure and denial of service motivations, often indicators of hacktivism and protest – i.e., they commonly used to discredit or exact revenge -- appear to be on the rise in the South African context.

Finally, it is interesting to note that after reaching a total of 11 instances in 2013, there were declines in 2014 (7 instances) and 2015 (2 instances), before a spike to 12 instances in 2016, the largest number recorded for any of the years studied – an apparent indication that cybersecurity measure are still not being effectively applied in South Africa, and/or that attempts at perpetration are becoming increasing complex and skilful.

Figure 2: Trends in impact type



Perpetrator type

Figure 3 presents the percentage distribution of the perpetration types. Hacktivist perpetrators – i.e., perpetrators affiliated to online activist groups making political statements – were found to be the most common, followed by criminals, then individual hackers, and then instances of accidental/misconfiguration due to non-malicious insiders.

Figure 3: Perpetrator type

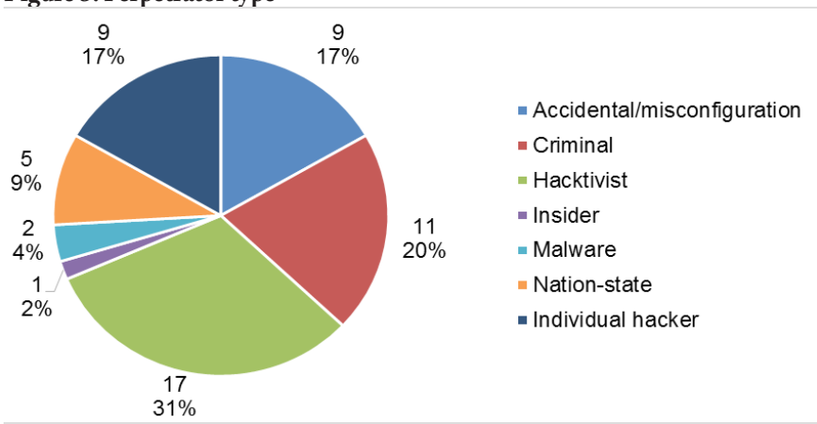
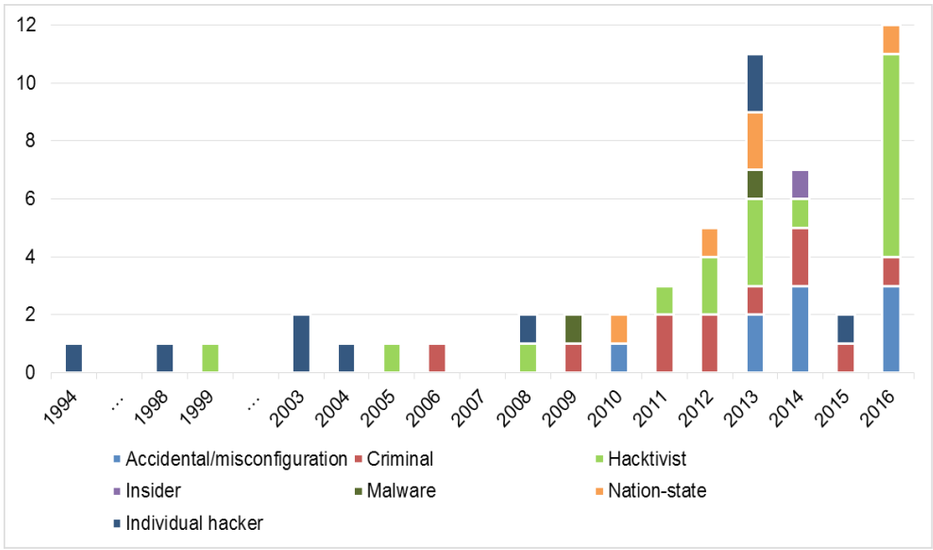


Figure 4 illustrates the trends in perpetrator type. Hacktivist perpetration has been present, off and on, since 1999, with slight increases in 2012 and 2012, and a sharp spike in 2016, indicating a growing protest and revenge dimension in South Africa's cybersecurity risk profile. Another concerning trend is the increasing prevalence of cases of accidental/misconfiguration due to non-malicious insiders, non-existent before 2010 but representing three cases in each of 2014 and 2016. It was found that nation-state cyber-espionage perpetrators have only been active in South African cyberattacks since 2010, whereas individual hackers have had an intermittent presence throughout.

Figure 4: Trends in perpetrator type



AJIC 20-21-Jan-18-22h19.indd 122-123 1/21/2018 10:43:18 PM

Table 1 is a pivot table associating the perpetrator types to the impact types. The strongest association is between criminal hackers and a financial attacks (10 instances), followed by accidental/misconfiguration due to non-malicious insiders resulting in data exposure (9 instances). These are followed by hacktivists exposing data (6 instances) and hacktivists denying service (6 instances), and then nation-state espionage perpetration seeking to expose (and presumably gain) data.

Whilst the prevalence of criminal activity is almost a given, data exposure due to error (accidental/misconfiguration) is presumably much more easily prevented than criminal activity should be of particular concern to South African institutions.

Table 1: Impacts by perpetrator type

	Impacts						
	Data exposure	Denial of service	Financial	Deface-ment	Data corruption	System penetration	Totals
Accidental/ miscon-figuration	9						**9**
Criminal	1		10				**11**
Hacktivist	6	6		4	1		**17**
Insider			1				**1**
Malware	1	1					**2**
Nation-state espionage	5						**5**
Individual hacker		2	1	4	1	1	**9**
Totals	22	9	12	8	2	1	54

Victim type

Figure 5 presents the distribution of victims in terms of state/political entities and other entities. As can be seen, it was found that attacks targeting the state/political entities represented more than half of the 54 attacks documented.

Figure 5: Victim type

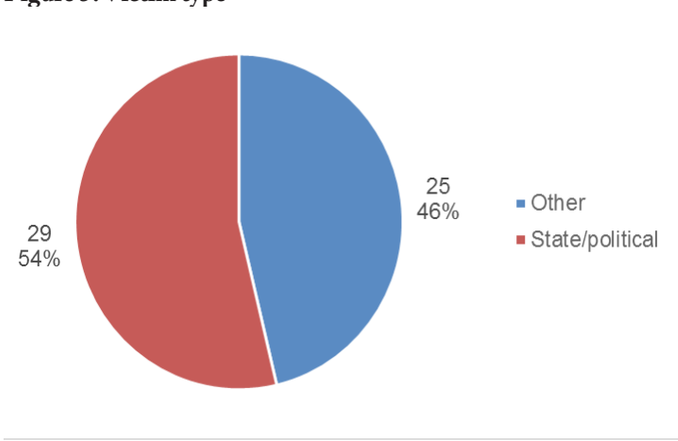


Figure 6 below llustrates the trends over time for the two victim categories. While the first attack on a state/political entity was detected in the first year of study, 1994, the first attacks on a non-state/political entity was only documented in 2003. However, in two of the most recent years studied, 2014 and 2016, attacks on non-state/political entities outnumbered state/political breaches.

Figure 6: Trends in victim type

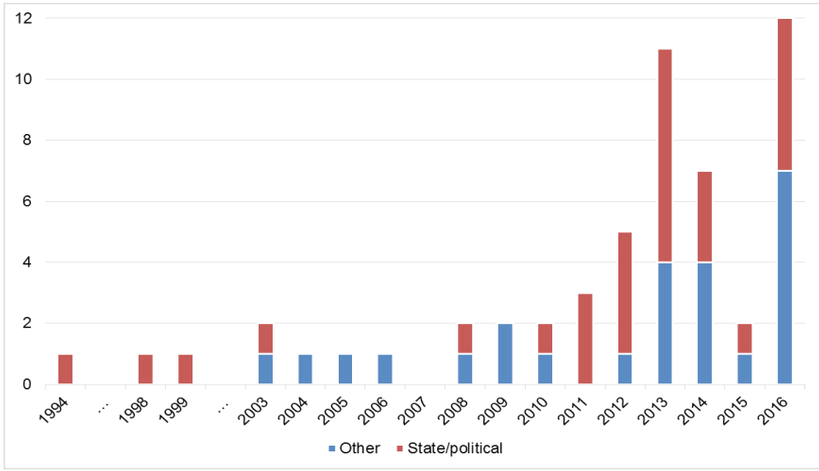


Table 2 below is a pivot table illustrating associations been impacts and victim types. There does not appear to be any significant difference between the distribution of impact types for the two victim types

AJIC 20-21-Jan-18-22h19.indd 124-125 1/21/2018 10:43:18 PM

Table 2: Impacts by victim type

	Impacts						
	Data exposure	Denial of service	Financial	Defacement	Data corruption	System penetration	Totals
Other	12	5	5	3			**25**
State/ political	10	4	7	5	2	1	**29**
Total	22	9	12	8	2	1	54

Table 3 below presents the perpetrator types associated with each of the two victim types. As before, nothing significant can be determined from these figures. The fact that hacktivists and nation-state perpetrators targeted state and political victims more than other organisations is logical. The state or political may have more impact from most perpetrators due to a lack of information security capability at those organisations.

Table 3: Perpetrator by victim type

	Perpetrator							
	Acci-dental/ mis-config-uration	Criminal	Hacktivist	Individual hacker	Insider	Malware	Nation-state espionage	Total
Other	5	5	7	4		2	2	25
State/ political	4	6	10	5	1		3	29
Total	9	11	17	9	1	2	5	54

5. Conclusions

This research has shown that in South Africa, the leading perpetrators of cyber-attacks are hacktivists and criminals. The top two cyber-attack impacts are data exposure and financial theft. The top two perpetration-impact combinations are criminals resulting in financial impact, and accidental/misconfiguration resulting in data exposure.

Given the prevalence of cyber-crime globally, the criminal appearance as a top perpetrator, linked to a top impact, is unsurprising. As Internet connectivity in Africa increases and a greater percentage of the population has Internet access, we can expect the rate of cyber-crime to increase, targeting, among others, new entrants who are not yet fully aware of the security risks. Due the increasing financial impact of cyber-incidents, it is imperative that the legislative environment is enabled to afford corporations protection and support law-enforcement in combatting cyber-attacks.

The increase in hacktivism in South Africa, notable in the data for 2016, can be linked to increased political tensions in the country (Vermeulen, 2016b). Even some of the non-state/non-political organisations targeted were linked to perceived government corruption (Van Zyl, 2016a). None of the organisations targeted, nor the way they were targeted, appeared to have any major direct impact on national stability or the national economy. However, there are at present certain large state-owned enterprises in South Africa, also linked to the political scandals, which have not yet been targeted. Should, for instance, the major electricity provider, Eskom, be attacked and for some reason operations hindered, there could be significant socioeconomic ramifications.

The numerous instances of cybersecurity threats caused by accidental/misconfiguration perpetration is concerning, as they have all occurred since the POPI Bill of 2009. It is possible that the Bill resulted in increased awareness and, in turn, an increase in exposures being reported. However, it still suggests that organisations, both state/political and other neglecting their responsibility to ensure that the systems are configured correctly. A possible solution will be to focus cyber-security awareness training on IT professionals in the country, in order to assist in creating a secure culture and an improvement of security in system development. Moreover, once the POPI Act is fully enforced and organisations are held fully accountable for such breaches, more effort may be given to discovering flaws, thereby reducing the accidental exposure.

Nation-state espionage is relatively low, and this is consistent with the findings of the report by Brown and Rudis (2017). At the same time, it is interesting to note that two of the nations most commonly associated with cyber-espionage campaigns – Russia and China – belong to a club of countries, the BRICS, of which South Africa is also a member along with Brazil and India. As can be seen from the revelations of the United States and Western European nations spying on each other, even allied countries conduct espionage operations against each other. Therefore as global tensions rise, South Africa should not be surprised if economic friendly countries increase espionage activities to monitor its politics and foreign policy. This concept, known as the "cyber-security dilemma", is discussed by Buchanan (2017). This in turn may also instigate an increase of international hacktivist activity.

AJIC 20-21-Jan-18-22h19.indd 126-127 1/21/2018 10:43:18 PM

Overall, the prevalence of perpetration factors and actors, and the impacts, that this study found in South Africa are consistent with reported international cyber-incident trends. A limitation of this study is that the data available were limited to what is reported publicly. Until it is mandatory for South African organisations to report cyber-incidents, it will be difficult to conduct in-depth assessments of the composition of threat activities and their impacts.

References

Ackroyd, B. (2014, December 4). Cyber hacktivist strikes SA sites again. *ENCA*. Retrieved from http://www.enca.com/technology/cyber-hactivist-strikes-sa-sites-again

Ajam, K. (2012, November 10). Alarm over credit card breach. *The Independent on Saturday*.

Andress, J., & Winterfield, S. (2014). *Cyber warfare: Techniques, tactics and tools for security practitioners* (2nd ed). Waltham, MA: Elsevier.

Arde, A. (2012, November 17). Hack attack a costly lesson for banks, *The Independent on Saturday*.

BBC News. (1999, September 13). Hackers deface SA stats site. Retrieved from http://news.bbc.co.uk/2/hi/africa/446392.stm

Brown, R., & Rudis, B. (2017). *Rapid7 threat report 2017 Q1*. Retrieved from https://www.rapid7.com/globalassets/_pdfs/research/rapid7-threat-report-2017-q1.pdf

Buchanan, B. (2017). *The cybersecurity dilemma*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

Cave, K. (2017, March 24). Cinema chain hack sees data security take centre stage in South Africa. *IDG Connect*. Retrieved from http://www.idgconnect.com/blog-abstract/25679/cinema-chain-hack-security-centre-stage-south-africa

Chandarman, R. (2016). *Cybersecurity awareness of students at a private higher education institute in South Africa*. Master's dissertation, University of KwaZulu-Natal, Westville, Durban.

Cusimano, J. (2010). DCS virus infection, investigation and response: A case study. Presentation to Industrial Control Systems Joint Working Group (ICSJWG) Fall Conference, 25-28 October, Seattle.

Department of Justice and Correctional Services. (2017). *Cybercrimes and Cybersecurity Bill*. Pretoria.

Dingle, S. (2009, July 15). Anatomy of an SMS banking scam. *FIN24.com*. Retrieved from http://www.fin24.com/articles/default/display_article.aspx?ArticleId=2638902

Dlamini, Z., & Modise, M. (2012). Cyber security awareness initiatives in South Africa: A synergy approach. In V. Lysenko (Ed.), *7th International Conference on Information Warfare and Security* (pp. 98-107). Seattle: University of Washington.

ESET. (2016, October). *En route with Sednit: Part I: Approaching the target*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf

Fearn, N. (2017, March 29). Critical lack of skills could be the biggest security challenge. *IDG Connect*. Retrieved from http://www.idgconnect.com/abstract/25505/critical-lack-skills-biggest-security-challenge

FireEye. (2014). APT28: A window into Russia's cyber espionage operations? Retrieved from https://www2.fireeye.com/apt28.html

Fripp, C. (2016, February 12). Anonymous begins #OpAfrica: Claims thousands of SA sites compromised. *htxt.africa*. Retrieved from http://www.htxt.co.za/2016/02/12/anonymous-makes-good-on-promise-goes-after-sa-government-websites/

Gorton, B. (2016, June 14). Anonymous Africa goes after "racist" EFF and their "Godfathers" Zanu PF. *Sowetan Live*. Retrieved from http://www.sowetanlive.co.za/news/article16983627.ece

HomeGrownHoney. (2009, January 7). Hackers expose South African banks. *ITWeb*. Retrieved from http://mydl.itweb.co.za/index.php?option=com_myblog&show=hackers-expose-south-african-bankshtml&Itemid=

ITNewsAfrica. (2013, August 30). MTN victim of cyber attack. Retrieved from http://www.itnewsafrica.com/2013/08/mtn-victim-of-cyber-attack/

ITWeb. (2013, May 6). No damage during Aarto hacking. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=63798

Limer, E, (2013). Meet Red October: The global cyber-espionage ring that spent 5 years in the shadows. *Gizmodo*. Retrieved from http://gizmodo.com/5975793/meet-red-october-the-global-cyber+espionage-ring-that-spent-5-years-in-the-shadows

Mail & Guardian. (2008, August 15). Hacker compromises DA website. Retrieved from https://mg.co.za/article/2008-08-15-hacker-compromises-da-website

Malwarebytes Labs. (2017). *State of malware report 2017*. Retrieved from https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf

Mandiant. (2013, February 19). *APT1: Exposing one of China's cyber espionage units*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Matinde, V. (2017, March 10). Cybersecurity must play catch up as more Kenyans move online. *IDG Connect*. Retrieved from http://www.idgconnect.com/abstract/25318/cybersecurity-play-catch-kenyans-online

Mbongwa, L., & Makua, J. (2005, January 13). Moroccan hackers blamed for website blitz. *Independent Online*. Retrieved from http://www.iol.co.za/news/south-africa/moroccan-hackers-blamed-for-website-blitz-231419

Miller, B., & Rowe, D. C. (2012). A survey of SCADA and critical infrastructure incidents. In RIIT '12 (Ed.), *Proceedings of the 1st Annual Conference on Research in Information Technology* [RIIT '12], (pp 51-56), New York: ACM. https://doi.org/10.1145/2380790.2380805

Mkhwanazi, S. (2015, October 12). Roads agency account hacked for R8.5m. *Independent Online*. Retrieved from http://www.iol.co.za/capetimes/roads-agency-account-hacked-for-r8-5m-1.1928834

Muller, R. (2013, December 30). My Vodacom security flaw exposes subscriber details. *MyBroadband*. Retrieved from https://mybroadband.co.za/news/security/94234-my-vodacom-security-flaw-exposes-subscriber-details.html

MyBroadband. (2013a, August 21). City of Joburg exposes private information again. Retrieved from https://mybroadband.co.za/news/security/84929-city-of-joburg-exposes-private-information-again.html

MyBroadband. (2013b, October 15). Mass security breach of fast food payment systems in SA. Retrieved from http://mybroadband.co.za/news/security/88985-mass-security-breach-of-fast-food-payment-systems-in-sa.html

MyBroadband. (2014, January 5). Big Cell C security flaw uncovered. Retrieved from https://mybroadband.co.za/news/security/94332-big-cell-c-security-flaw-uncovered.html

AJIC 20-21-Jan-18-22h19.indd 128-129 1/21/2018 10:43:18 PM

MyBroadband. (2016, May 30). MTN exposing subscribers' personal details online. Retrieved from https://mybroadband.co.za/news/cellular/166734-mtn-exposing-subscribers-personal-details-online.html

Norton South Africa (2012) *Norton cybercrime report 2012*. Retrieved from http://za.norton.com/cybercrimereport/promo?inid=uk_hho_downloads_home_link_cybercrimereport

Oiaga, M. (2006, July 4). Three South African banks hit by hackers. *Softpedia*. Retrieved from http://news.softpedia.com/news/Three-South-African-Banks-Hit-by-Hackers-28590.shtml

Paganini, P. (2013, January 17). Red October, RBN and too many questions still unresolved. Security Affairs blog. Retrieved from http://securityaffairs.co/wordpress/11779/cyber-crime/red-october-rbn-and-too-many-questions-still-unresolved.html

Patrick, H. (2015). *Security information flow in the public sector: KZN health and education*. PhD thesis. University of KwaZulu-Natal, Durban.

Plaut, M. (2010, October 26). Book says hacker tried to stop Mandela coming to power. *BBC News*. Retrieved from http://www.bbc.com/news/world-africa-11630092

Porter, B. (2003, August 8). Hackers target SA universities. *News24*. Retrieved from http://www.news24.com/SciTech/News/Hackers-target-SA-universities-20030808

Potgieter, D. (2011, January 8) Absa intercepts land bank swindle. *Saturday Star*. Retrieved from http://www.iol.co.za/business/companies/absa-intercepts-land-bank-swindle-1.1009423

Pretorius, B. H. (2016). *Cyber-security and governance for industrial control systems (ICS) in South Africa*. Master's dissertation, University of KwaZulu-Natal, Durban.

PricewaterhouseCoopers (PwC), & BAE Systems. (2017). Operation Cloud Hopper. Retrieved from https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

Rasool, F. 2012. Postbank heist signals policy gap, *ITWeb*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=50818

Redelinghuis, K. (2011, March 30). ANC Youth League website hacked by "Warbird". *Memeburn*. Retrieved from http://memeburn.com/2011/03/anc-youth-league-website-hacked/

Republic of South Africa (RSA). (2002a). Electronic Communications and Transactions Act 25 of 2002.

RSA. (2002b). Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 70 of 2002.

RSA. (2009). Protection of Personal Information (POPI) Bill 9 of 2009.

RSA. (2013). Protection of Personal Information (POPI) Act 4 of 2013.

Reuters. (1998, June 11). South Africa police arrest teen hacker. Retrieved from http://lists.jammed.com/ISN/1998/11/0032.html

Roane, B. (2013, May 22). SAPS website hacked. *The Star*. Retrieved from http://www.iol.co.za/news/crime-courts/saps-website-hacked-1.1520042

SABC News. (2017, April 19). Cyber-attacks reaching a critical point in SA. Retrieved from http://www.timenews.co.za/timenews-sabc-news-cyber-attacks-reaching-a-critical-point-in-sawednesday-19-april-2017

Safenet. (2014). Breach database: Top data breaches. Retrieved from http://www.breachlevelindex.com/#!breach-database

SANews. (2012, December 21). Attack on e-toll website foiled. Retrieved from http://www.sanews.gov.za/south-africa/attack-e-toll-website-foiled

Saville, M. (2012, December 9). Three SA government websites hacked. *Mail & Guardian*. Retrieved from https://mg.co.za/article/2012-12-09-three-government-websites-hacked

Song, S. (2017). African undersea cables – Interactive. Many Possibilities blog. Retrieved from https://manypossibilities.net/african-undersea-cables-interactive

Speckman, A. (2015). Cybercriminals are on the prowl. *BDLive*. Retrieved from http://www.bdlive.co.za/businesstimes/2015/02/01/cybercriminals-are-on-the-prowl

State Security Agency (SSA). (2015). *National cybersecurity policy framework*. Pretoria.

Stone, A. (2010, April 25). Patient records for all to see. *I-Net*. Retrieved from http://news.za.msn.com/local/article.aspx?cp-documentid=153155730

Swart, W., & wa Afrika, M. (2012, January 15). It was a happy New Year's Day for a gang who pulled off...R42m Postbank heist. *Times Live*. Retrieved from https://www.timeslive.co.za/news/south-africa/2012-01-15-it-was-a-happy-new-years-day-for-gang-who-pulled-offr42m-postbank-heist

Tate, S. (2017, April 19). Why Australia will lose a cyberwar. *Vice*. Retrieved from https://www.vice.com/en_au/article/why-australia-will-lose-a-cyberwar

TelecomSpeak. (2015, May 18). Cyber attack targets MTN Data Centre. Retrieved from http://www.telecomspeak.com/2015/05/18/cyber-attack-targets-mtn-data-centre

Tengimfene, N. (2013). Media statement on progress made by the Justice, Crime Prevention & Security cluster in the fight against corruption. Pretoria: Government Communication and Information System (GCIS).

Tubbs, B. (2013, May 22). SAPS hack spells negligence. *ITWeb*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=64268:SAPS-hack-spells-negligence&catid=265

Van Niekerk, B. (2017). Analysis of cyber-attacks against the transportation sector. In M.E. Korstanje (Ed.), *Threat mitigation and detection of cyber warfare and terrorism activities* (pp. 69-92), Hershey PA: IGI. https://doi.org/10.4018/978-1-5225-1938-6.ch004

Van Rooyen, K. (2009, July 18). Hidden price of a banking scam. *The Times*. Retrieved from http://www.thetimes.co.za/News/Article.aspx?id=1036132

Van Zyl, G. (2016a, June 15). Hack attack threat for Gupta sites, Oakbay and Sahara down. *Fin24*. Retrieved from https://www.fin24.com/Tech/Cyber-Security/anonymous-threatens-hack-attacks-on-gupta-websites-20160615

Van Zyl, G. (2016b, June 30). Standard Bank computer was hacked in R300m ATM fraud hit – report. *Fin24*. Retrieved from http://www.fin24.com/Tech/Cyber-Security/standard-bank-computer-was-hacked-in-r300m-atm-fraud-hit-report-20160630

Van Zyl, G. (2016c, July 12). Anonymous "hacks" Armscor website. *Fin24*. Retrieved from http://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712

Venktess, K. (2016, September 8). eThekwini municipality website leaks user data – Expert. *Fin24*. Retrieved from http://www.fin24.com/Tech/News/ethekwini-municipality-website-leaks-user-data-expert-20160908

Vermeulen, J. (2013, May 14). Spyware servers in South Africa: the plot thickens. *MyBroadband*. Retrieved from http://mybroadband.co.za/news/security/77110-government-spyware-servers-in-south-africa-telkom-govt-mum.html

AJIC 20-21-Jan-18-22h19.indd 130-131 1/21/2018 10:43:19 PM

Vermeulen, J. (2014, January 8). E-toll website flaw a cyber-attack: Sanral. *MyBroadband*. Retrieved from https://mybroadband.co.za/news/security/94554-e-toll-website-flaw-a-cyber-attack-sanral.html

Vermeulen, J. (2016a, February 12). Anonymous hacks SA government database, *MyBroadband*. Retrieved from http://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html

Vermeulen, J. (2016b, June 13). This is how I took down the SABC: Anonymous hacker. *MyBroadband*. Retrieved from http://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html

Students' Cybersecurity Awareness at a Private Tertiary Educational Institution

Rajesh Chandarman
MCom Graduate, School of Management, IT and Governance, University of KwaZulu-Natal, Westville, Durban

Brett van Niekerk
Honorary Research Fellow, School of Management, IT and Governance, University of KwaZulu-Natal, Westville, Durban

Abstract
Internet-based attacks have become prevalent and are expected to increase as technology ubiquity increases. Consequently, cybersecurity has emerged as an essential concept in everyday life. Cybersecurity awareness (CSA) is a key defence in the protection of people and systems. The research presented in this article aimed to assess the levels of CSA among students at a private tertiary education institution in South Africa. A questionnaire tested students in terms of four variables: cybersecurity knowledge; self-perception of cybersecurity skills, actual cybersecurity skills and behaviour; and cybersecurity attitudes. The responses revealed several misalignments, including instances of "cognitive dissonance" between variables, which make the students potentially vulnerable to cyber-attacks. The findings demonstrate the need for targeted CSA campaigns that address the specific weaknesses of particular populations of users.

Keywords
cybersecurity awareness (CSA), password management, cyberbullying, phishing, malware, identity theft, pirated content

DOI: https://doi.org/10.23962/10539/23572

Recommended citation
Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, *20,* 133-155. https://doi.org/10.23962/10539/23572

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

AJIC 20-21-Jan-18-22h19.indd 132-133 1/21/2018 10:43:19 PM

1. Introduction

As is widely reported in the media, cyber-attacks are increasing in quantity and sophistication (Symantec, 2013). In most cases it is the weakest link in cybersecurity – the human element – that is the target for the increasing number of online criminals who are perpetrating an ever-greater variety of cybercrimes. The need for cybersecurity awareness (CSA) campaigns is thus undisputed, as these remain the first line of defence in providing employees and stakeholders with the know-how to interact safely online. International cybersecurity best practices advocate for CSA, and this filters into organisational policies and standards. An example in the education sector is the cybersecurity awareness campaigns and material provided by Educause (2017). Countries such as Australia, Canada, the UK and the US have implemented CSA campaigns supported by national committees and strategies (Cyber Aces Foundation, 2014; Office of Australian Info Officer, 2014; Rosewarne, 2013). Compared to these countries and others in Africa such as Mauritius and Kenya, South Africa has been found wanting in its CSA efforts (Doyle, 2015).

In South Africa, section 51(6) (g) of the draft Cybercrimes and Cybersecurity Bill specified that there is a need to (Minister of Justice and Correctional Services, 2015):

> (ii) promote and provide guidance in development and implementation of situational analysis and awareness campaigns concerning the risk environment of the South African cyberspace;
>
> (vi) cybersecurity training, education, research and development programmes amongst other initiatives.

For the purposes of this article, cybersecurity is defined as the protection of cyberspace itself, of the tangible or intangible technologies that support cyberspace, of electronic information, and of the users in their personal, societal and national capacities (Von Solms & Van Niekerk, 2013). Awareness is conceived of as comprising knowledge, self-perception of skills, actual skills and behaviour, and attitudes, and the inter-relationship among these elements.

In August 2014, it was reported that Russian cyber-criminals compromised 500 million email addresses and 1.2 billion passwords and usernames (*BBC News*, 2014). In April 2015 the names and social security numbers of approximately 280,000 AT&T US customers were sold to various third parties after being stolen by employees at call centres in the Philippines, Mexico and Colombia. As a result, AT&T was fined USD25 million by the US communications regulator, the Federal Communications Commission (Ruiz, 2015). In the same month, hackers allegedly from Islamic State compromised the social media pages and website of French television network TV5Monde, and disrupted the broadcasts of all 11 channels (Ashford, 2015).

The South African economy lost approximately ZAR1 billion in 2014 due to identity theft, of which there were approximately 4,000 reported cases (Compuscan, 2014). Insufficient awareness around cybercrimes is a possible reason for the South African Banking Risk Information Centre (SABRIC) reporting that over ZAR2.2 billion was lost in 2013 due to online fraud, identity theft and scams (*BusinessTech*, 2014).

Students are considered one of the computer-user profiles that is most vulnerable to cyber-attacks, as they are often careless and sometimes reckless in their computer usage and spend copious amounts of their time using technology (Aliyu, Abdallah, Lasisi, Diyar & Zeki, 2010). The persistent psychological need to remain connected via an increasing variety of electronic devices further exposes individuals to online risks (Mochiko, 2016).

There have been very few studies of CSA in South Africa, even fewer focusing on students attending South African public tertiary institutions, and, before this study, no studies of CSA among students at private tertiary institutions could be found. The research presented in this article, which was conducted for a Master's dissertation (Chandarman, 2016), sought to fill this gap by investigating the private tertiary students' online activity, and their knowledge, self-perception of skills, actual skills and behaviours, and attitudes, as they relate to cybersecurity issues. Among the aims of the research was to determine the degree of necessity of an intensive, focussed CSA training and education campaign tailored to the needs of the audience, as opposed to a general awareness campaign that is common to all audiences. The subject matter included in the survey, in order to evaluate the students' CSA, included: password management, cyberbullying, social engineering (including phishing and online scams and fraud), malware, identity theft, and general secure behaviour (e.g., downloading and sharing "pirated" film and TV content, using pirated software).

2. Literature review and analytical framework

An adapted version of the theory of planned behaviour (TPB) framework was used for the study. The TPB framework, originally proposed by Icek Ajzen, was found to be suitable because it has been used in investigating individuals' ethical behaviour and decisions in respect of adoption of, and compliance with, computer security measures (Ifinedo, 2012; Lee & Kozar, 2005; Leonard, Cronan, & Kreie, 2004). However, the TPB framework does not explicitly consider the case for CSA, and therefore it needed to be adapted. To adapt the framework, previous studies on CSA were considered, in order to determine necessary CSA variables and possible relationships among the variables. These earlier studies also formed a baseline against which the results of this study could be compared.

Furnell, Gennatou and Dowland (2002) found that organisations and individuals were unsure as to what they should be doing to improve their cybersecurity or how to achieve this, despite acknowledging that it was an issue that needed to be addressed.

AJIC 20-21-Jan-18-22h19.indd 134-135 1/21/2018 10:43:19 PM

The key to providing clarity, according to the National Institute of Standards and Technology (NIST, 2003), is CSA training and education. In addition to providing direction on security policies and how to properly use and protect IT resources and information, NIST SP 800-16 (1998) indicated that all employees in every organisation should have a basic literacy and awareness of information security. A range of topics for CSA training were suggested in NIST SP 800-50 (2003): data backup, malware protection, web usage, email and attachments, password usage and management, and social engineering.

A study by Rajan (2010) investigated the relationship between the likelihood of users falling victim to phishing (a form of social engineering which uses emails to maliciously solicit information from computer users, such as login or financial account details) and their awareness of the topic. The study concluded that people fell victim to phishing despite having knowledge and understanding of the importance thereof. This was attributed to incorrect behaviour patterns regarding online security. The use of simulated phishing emails to generate user awareness was investigated by Dodge and Ferguson (2006). Their study intended to assess the awareness levels of students at the United States Military Academy in order to inform their awareness programme. The study found that conducting the exercise, in addition to aiding them in tailoring their awareness drive, itself increased awareness. A similar study by Steyn, Kruger and Drevin (2007), focusing on higher education staff in the Western Cape Province of South Africa, found that email security considerations should be prioritised for education and awareness activities. These studies illustrate that *both* correct awareness and correct attitudes are essential in addition to knowledge in promoting secure behaviour online. Mishra (2014) found that many users exhibit a misperception that an installed anti-virus programme is sufficient to prevent compromise of their computers, and that a number believe that firewalls are the same as anti-virus applications.

An advanced cyber-espionage campaign employing both malware and social engineering to target governments, journalists and businesses in Southeast Asia and India over a 10-year period was discovered by FireEye in April 2015 (Lennon, 2015). The Heartbleed vulnerability was disclosed and made news headlines as the biggest security vulnerability in the history of IT in April 2014 (Mitre, 2014). Later that month, users were advised to use an alternative to Internet Explorer due to a severe vulnerability in the browser where malware could be unknowingly installed via webpages browsed (Rosenblatt, 2014). In September 2014 a number of distributed denial of service (DDoS) attacks and Botnet activity were recorded globally within an hour of the ShellShock/BashDoor vulnerability being disclosed (TroyHunt, 2014). These incidents illustrate the necessity of awareness regarding the need for patching and updating of machines, in addition to the need for awareness regarding phishing and social engineering, in order to protect against sophisticated attacks, ransomware, and other attacks.

A study by Pramod and Raman (2014) found that students in higher education are not ignorant of security concerns regarding smartphones, but at the same time are not fully aware of all the security risks and necessary security practices. Pretorius and Van Niekerk (2015) recommended training and awareness campaigns after finding vulnerabilities in industrial control systems due to users' insecure password management, unapplied software patches, and outdated or uninstalled anti-virus and malware protection. These studies further illustrate how there can be misalignment among cybersecurity attitudes, knowledge, and behaviour.

Victims of identity theft may suffer heavy consequences, including damaged credit scores and financial charges (Janssen, 2014). Wlasuk (2012) found that if identity information data held by higher education institutions was sold on the cyber black market, they would potentially be worth billions of dollars. A 2014 Kaspersky and B2B report found that South African Internet users generally had the misperception that cyber-criminals would see no value in their account credentials (*MyBroadband*, 2015). An exploratory study of college students by Mensch and Wilkie (2011) found that a false sense of security, in relation to personal information protection, is created by the installation of security applications and tools. Butler and Butler (2014) concluded that South Africans consider convenience a higher priority over security, and that only 23% of South African users regularly change their passwords despite 70% indicating that they are aware that this is good practice. These findings show that knowledge does not necessarily translate into good practice.

Kim (2014) found that many college students in the US did not participate in information security awareness training, even though they appeared to understand the need and importance of the training. Another finding of the study was that the students' security learning occurred piecemeal, from a number of sources, and that to develop sustainable secure behaviour they needed to participate more in focussed information security and awareness training. This again illustrates the potential for disconnections between good secure practice and having sufficient knowledge and understanding.

If security practices are too time-consuming or difficult, users will try to circumvent the controls in place, which may also reduce the effectiveness of previous and current awareness campaigns. Influencing strategies are required in addition to the knowledge transfer and awareness in order to positively alter behaviours and attitudes (Bada & Sasse, 2014). Peltier (2005) found that a baseline of the cybersecurity perception levels, attitudes, knowledge and skill, and the relationships amongst these, are required to guide the training.

Hagen and Albrechtsen (2009) concluded that an e-learning tool that they assessed was a suitable mechanism for the initial creation of common values and attitudes to build a corporate information security culture. Kaur and Mustafa (2013) investigated

AJIC 20-21-Jan-18-22h19.indd 136-137 1/21/2018 10:43:19 PM

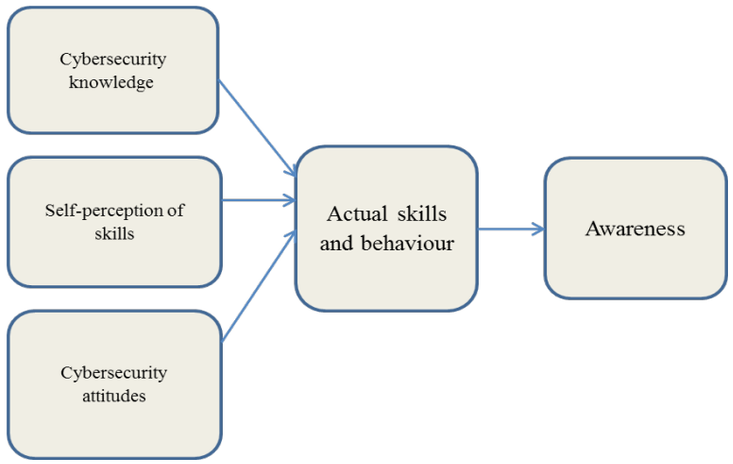
how information security awareness of Malaysian small and medium enterprise employees was affected by attitude, behaviour, and knowledge. The study found that attitude and behaviour had significant relationships with information security awareness, but knowledge did not. This is consistent with the findings of Bada and Sasse (2014). Aliyu et al. (2010) found that, among Malaysian IT and education students, IT usage was affected by attitudes and perceptions towards computer ethics and security. Bakar, Chang and Saidin (2013) investigated e-commerce consumers' practices, knowledge and attitudes, and found that there was little knowledge or education regarding legal provisions, and that fostering better behaviours and attitudes was required to mitigate the likelihood of the consumers falling victim to cyber-criminals.

Aliyu et al. (2010) found that university students in Malaysia were major violators of computer ethics and security, as they were often reckless when posting content and browsing and were frequently involved in illegal usage via sharing and downloading of counterfeit software, TV series and movies. Due to a range of factors including laziness and economic standing, the students were found to not be practising safe computing in general (Aliyu et al., 2010).

The general consensus that emerges from the literature is that training and education are key initiatives to generate CSA and ameliorate poor online security behaviour. The studies considered in the literature also suggest that knowledge, self-perception of skills, actual skills and behaviours, and attitudes, are all relevant to assessing CSA, and that knowledge alone is typically not sufficient to ensure CSA, i.e., knowledge is often a weak variable.

Accordingly, our adapted version of the TPB framework investigated CSA via focus on relationships among four core variables: (1) *knowledge*, (2) *self-perception of skills*, (3) *actual skills and behaviour*, and (4) *attitudes*.

Figure 1: The TPB framework adapted to the CSA study



3. Methodology

The study followed an exploratory approach, using non-probability sampling. The study site consisted of three campuses of a private tertiary education institution in South Africa's KwaZulu-Natal Province, and a convenience sample of students was taken (i.e., those who attended lectures at an appropriate time for the researcher to gather data).

Data were collected via a questionnaire that received a total of 1,231 responses over two semesters (528 respondents online in the first semester, and 703 respondents for the paper-based questionnaire in a second semester). The results were analysed using the SPSS statistical software package, employing: descriptive statistics to assess individual topics and variables; Pearson Correlation and chi-square to assess relationships among variables; and Cronbach Alpha to assess significance.

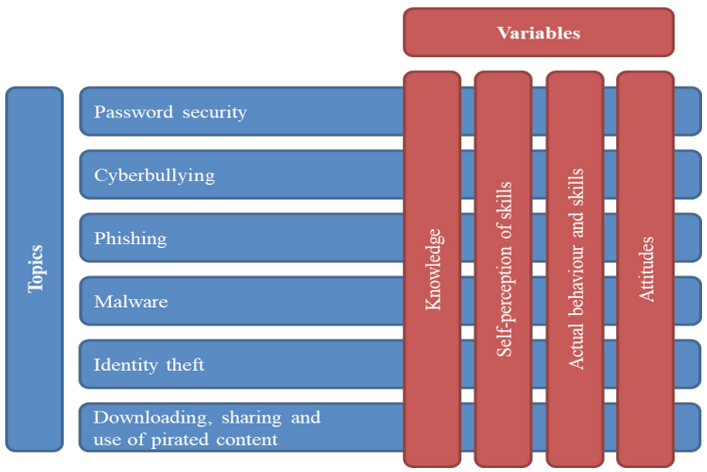
A high-level outline of the questionnaire is as follows:

- section 1: The student's demographic information
- section 2: the student's online usage
- section 3: the student's cybersecurity knowledge
- section 4: the student's self-perception of cybersecurity skills
- section 5: the student's actual cybersecurity skills and behaviour
- section 6: the student's cybersecurity attitudes

The focus of this article is on the data generated by answers to questions in sections 3 to 6. Figure 2 below visualises the variables and topics considered.

AJIC 20-21-Jan-18-22h19.indd 138-139 1/21/2018 10:43:20 PM

Figure 2: Variables and topics in the study



4. Findings

Cybersecurity knowledge

The "knowledge" category (section 3) offered students multiple-choice-format responses to factual questions regarding the six cybersecurity matters that were the focus of the research. Only one answer for each question was accepted as correct. The student responses were recoded numerically in binary fashion: as "2" if they answered the question correctly and "1" if they got the question wrong or indicated that they did not know answer. Frequency analysis was then conducted for the responses to each question. Figure 3 provides the frequency analysis.

Of note in Figure 3 are the significant lack of knowledge of what phishing is (56% answered incorrectly or did not know), and the significant lack of knowledge of the purpose of anti-virus software (43% answered incorrectly or did not know).

Figure 3: Students' knowledge of six cybersecurity matters
(N = 1188, 1197, 1193, 1191, 1182, 1196)

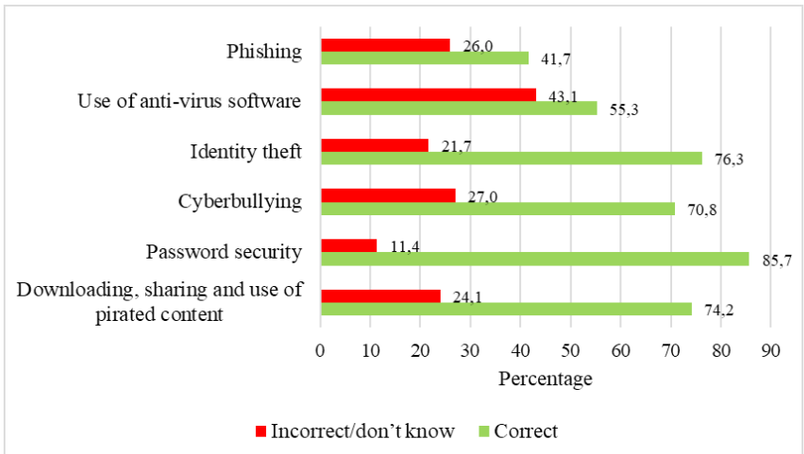


Table 1 below shows the section 3 responses prior to binary recoding. Approximately 38% of respondents selected "I do not know" for the phishing question, and 41% of respondents thought that anti-virus software was protection against "every possible attack".

Table 1: Cybersecurity knowledge before recoding (shown as % of responses)

3.1. What is phishing?	**%**
Unsolicited requests (spam) to fool receivers into divulging personal information	39.6
Disguised hyperlinks and sender addresses	6.1
Viruses being downloaded onto your devices	1.4
Your device being hacked to steal information	12.5
I do not know	37.9
Spoilt/blank	3.8
3.2. What is anti-virus software used for?	**%**
Disrupt and covertly steal information from your devices	0.7
Updating your software and systems	1
Protect your computer devices against malicious code	53.7
Preventing every possible attack on your computer devices	40.7
I do not know	2.3
Spoilt/blank	2

AJIC 20-21-Jan-18-22h19.indd 140-141 1/21/2018 10:43:20 PM

The findings shown in Table 1 suggest that that the respondents' knowledge levels in respect of phishing and anti-virus software were inadequate. Such knowledge deficits can lead to unsafe practices, and can be exploited by cyber-criminals.

Self-perception of cybersecurity skills

The results from the section 4 on self-perception of cybersecurity skills are presented in Table 2 below. The section consisted of six statements – one for each of the six cybersecurity matters that were the focus of the research – to which the respondent was asked to indicate her or his level of agreement based on a five-point Likert scale (1 = "strongly disagree", 5 = "strongly agree").

Table 2: Self-perception of cybersecurity skills

	N	Mean	Std. deviation	Std. error mean
4.1 I am confident I can identify a phishing email or a social engineering attack	1193	**3.19**	1.186	.034
4.2 I am adequately protected from malware, scareware and spyware	1197	**3.43**	1.059	.031
4.3 I am well liked and will never be a victim of cyberbullying	1207	**3.14**	1.152	.033
4.4 I do not post anything that will cause me to be a victim of identity theft	1207	**3.94**	1.030	.030
4.5 My passwords are strong enough. Nobody can guess them	1204	**3.95**	1.022	.029
4.6 Sharing downloaded (*) movies and TV series with my friends is OK	1206	3.03	1.228	.035

* "downloaded" in this context referred to content downloaded illegally without paying for it (i.e., "pirated" content)

A Cronbach Alpha test was done on the responses to all six statements, yielding a result of $\alpha = 0.668$. Since this figure was less than 0.7, the test was therefore recalculated with question 4.6 excluded, resulting in an acceptable score of $\alpha = 0.707$.

The first five statements generated a mean score > 3 and a $p < .0005$, indicating a significant level of agreement with the statements. Thus, overall, the students exhibited generally favourable self-perceptions of their cybersecurity skills. However, at the same time, four of the statements received a large percentage of neutral responses: the phishing (32%); malware, scareware and spyware (31%); cyberbullying (37%); and sharing downloaded movies and TV series (35%) statements. These neutral responses implied that the students in question had not developed an opinion

or stance on these areas, suggesting a lack of comprehensive CSA.

Actual cybersecurity skills and behaviour

Table 3 below shows the seven scenarios respondents were asked to respond to in part B of section 5 of the questionnaire, which was focused on determining the students' actual cybersecurity skills and behaviour. Part B focussed on responses to scenarios, whereas Part A focussed on self-reporting of behaviour.

Table 3: Text of questions on actual cybersecurity skills and behaviour

5.11 You receive an email from your bank that your account needs to be verified because the bank has installed new software. You are required to click on a link provided and supply the necessary personal verification information. You must respond within the next 24 hours otherwise your bank account will be blocked and frozen. What do you do? a) Click on the link and provide the personal information requested so the security matter can be addressed without your account being frozen. b) Ignore it. It looks like a scam, so you delete the message without responding. c) You are suspicious but aren't sure if this is a scam or not. You respond to the text message, asking questions to determine if the situation. is legitimate before you provide the information requested. d) Phone the bank to check if this is true. e) Report the matter to the police.
5.12 I update my Windows/Apple, anti-virus, browser and other software: a) Once a month. b) When I remember. c) When I am reminded. d) Never.
5.13 The mouse cursor on your screen starts to move around on its own and click on things on your desktop. What do you do? a) Call someone so that they can see. b) Disconnect your computer devices from the network/ internet. c) Unplug your mouse. d) Turn your computer device off. e) Run your antivirus.

AJIC 20-21-Jan-18-22h19.indd 142-143 1/21/2018 10:43:20 PM

Table 3 (cont.): Text of questions on actual cybersecurity skills and behaviour

5.14 Your friend sends you an email with a screensaver they say you will love. What will you do?

a) Download it onto your device, since you trust your friend.
b) Forward the message to other friends to share it.
c) Call an IT professional and ask them to install it for you.
d) Delete the message.
e) None of the above.

5.15 "At campus yesterday, Josh was mucking around with a water spray gun and wet John's pants. It was hilarious because it really looked like John wet his pants and Tyson even got a photo! We were all joking about it and calling John 'Little Johnnie' and saying stuff like, 'Do you need your nappy changed, Baby John?' Then last night some of us got onto Facebook and we told everyone about it, and put the photo up too. Everyone said how funny it was, and they thought of some really funny things to tease John with today!" What is your opinion on this scene?

a) Hilarious.
b) Most people think this is funny
c) Hmm, made me laugh, but .. not sure if it was fair.
d) This hurt someone's feelings.
e) Yuck, this was deliberate and only done to hurt someone (emotionally and/or physically).

5.16 If someone searches for information about me on the internet, they would find:
i. My name
ii. My photograph
iii. My telephone number
iv. My home address
v. My bad habits (and things I would be embarrassed about)
vi. Pictures of my holidays
vii. My family members

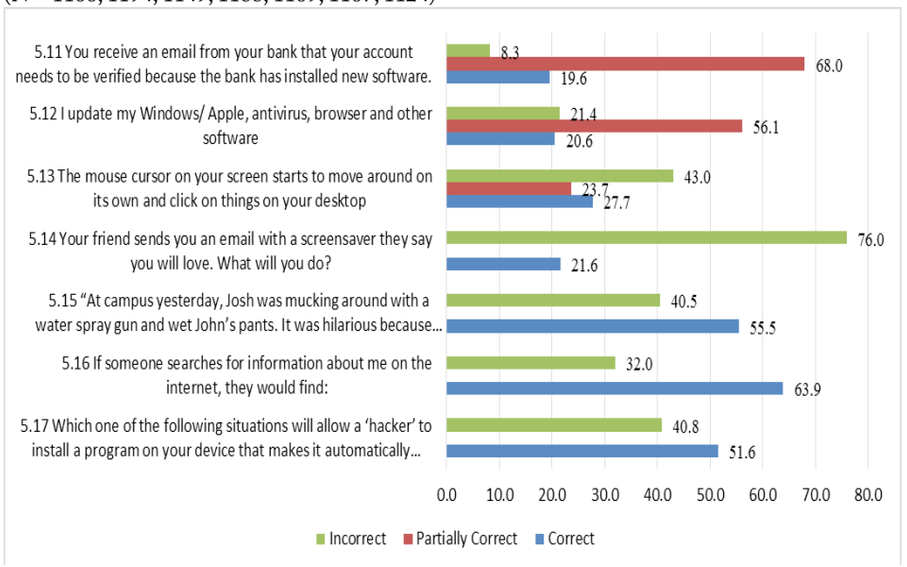
a) All of the above.
b) 2 to 3 of the above.
c) 4 to 5 of the above.
d) A few of the above.
e) None of the above.

5.17 Which one of the following situations will allow a "hacker" to install a program on your device that makes it automatically send out tons of spam email from your device without your knowledge?

a) Out of date software patches.
b) No anti-virus installed or out of date anti-virus.
c) Clicking an unknown link or attachment.
d) Downloading unknown or unsolicited programs onto your computer device.
e) All of the above.

Figure 4 provides a summary of the frequency analysis for responses to each of the seven scenarios.

Figure 4: Actual cybersecurity skills and behaviour
(N = 1166, 1194, 1149, 1188, 1169, 1167, 1124)



Notable findings shown in Figure 4 are the large percentage (76%) of unsafe responses regarding opening a screensaver received from a friend (question 5.14), the large percentage (68%) of only partially correct (i.e., only partially safe) responses regarding response to a bank phishing email (question 5.11), and the large percentage (56.1%) of only partially correct responses to the question regarding updating of software (question 5.12). All these findings indicate unsafe cybersecurity skills and behaviour.

The Cronbach Alpha test was calculated, with questions 5.5 and 5.10 excluded as they were inverted, i.e. negative questions. For the remaining five questions, a result of $\alpha = 0.766$ was returned, indicating a high reliability. The Chi-square analysis (shown below in Table 4) for the whole group indicated that certain responses showed significant results. For example, the only partially correct responses for question 5.11 were significant ($\chi 2$ (2, N = 827) = 765.666, $p < .0005$.

AJIC 20-21-Jan-18-22h19.indd 144-145 1/21/2018 10:43:20 PM

Table 4: Chi-Square results for cybersecurity skills and behaviour questions

Question	Result	N	df	Chi-square	p
5.11	partially correct (i.e., partially safe)	827	2	756.666	p < .0005 *
5.12	partially correct	683	2	306.226	p < .0005
5.13	incorrect (i.e., unsafe)	523	2	79.770	p < .0005
5.14	incorrect	925	1	368.892	p < .0005
5.15	correct (i.e., safe)	676	1	28.648	p < .0005
5.16	correct	778	1	129.667	p < .0005
5.17	correct	628	1	15.502	p < .0005

* SPSS reports a *p* of .000 as *p* < .0005

Cybersecurity attitudes

The responses to the questions on cybersecurity attitudes (section 6 of the questionnaire) are presented in Table 5 below. Generally the results were encouraging, as students indicated generally low levels of agreement with the statements, all of which were statements for which agreement would represent a potentially unsafe/ harmful attitude. The one worrying exception was in the responses to question 6.1, where students exhibited an overly trusting view towards content sent via email from the email accounts of their friends – a level of trust that could make the receiver susceptible to malicious content.

Reliability for the eight questions in section 6 was tested using Cronbach Alpha, which returned $\alpha = 0.713$. It can therefore be concluded that the responses were consistent and a reliable measure of respondent attitudes towards the six cybersecurity matters.

Table 5: Cybersecurity attitudes

	N	Mean	Std. deviation	Std. error mean
6.1 My friends would not send me anything malicious or scams through email.	1170	**3.62**	1.122	.033
6.2 Updating my security software and Windows /Apple is too time consuming, annoying and uses up my bandwidth/ data bundle.	1168	2.69	1.122	.033
6.3 The security settings and tools slow me down and are pesky. I turn them off or disable them.	1166	2.39	1.004	.029
6.4 It is a waste of time to change passwords because you can still get hacked	1163	2.47	1.062	.031
6.5 It is too difficult to remember difficult passwords; therefore I use my name or something easy to remember.	1171	2.34	1.203	.035
6.6 Posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their face.	1169	1.76	1.024	.030
6.7 It is OK to download (*) movies and TV series because the companies that make them are rich and I really cannot afford it (I am a student).	1169	2.53	1.143	.033
6.8 If I pirate software I will not get updates and security patches, but I don't need [updates and patches]	1162	2.29	.998	.029

* "download" in this context referred to downloading of "pirated" film and TV content (i.e., content acquired illegally, without the required authorisation obtained or payment made)

5. Analysis

Misalignments in relationships among CSA variables

With respect to phishing, correlation results illustrated weak negative relationships between student *self-perceptions of skills* and (1) their *actual skills and behaviour*, and (2) *attitude*, on the matter. This indicates that while the students had a favourable perception of their security protection and their skills in this area, their actual skills and behaviour, and attitudes, were not as safe as their perceptions implied they were.

In respect of pirated content, while most students reported *actual skills and behaviour* suggesting they engaged in piracy, most at the same time also held the correct *attitude* towards pirated content, i.e., the attitude that it can be dangerous. This indicates students will engage in behaviour even though they know it is wrong.

Similarly, in respect of cyberbullying, despite a majority of students reporting

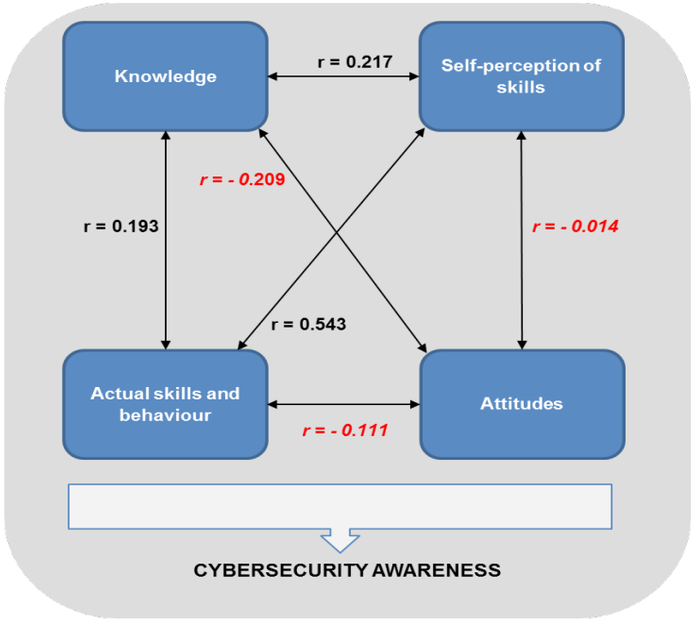
AJIC 20-21-Jan-18-22h19.indd 146-147 1/21/2018 10:43:21 PM

favourable *self-perceptions of skills and behaviour* for avoiding cyberbullying behaviour when posting messages online, the majority also gave *attitude* responses indicating a potentially harmful attitude towards posting offensive pictures and messages.

For passwords, most students reported an *attitude* that it was difficult to remember complex passwords and so they used simple ones like their names (question 6.5), a potentially harmful attitude. Yet, at the same time, for the majority, the *self-perceptions of skills and behaviour* suggested they had strong passwords (question 4.5), results in the negative correlation ($r = -.196$, $p < .0005$). These are clear contradictions and disconnects among responses to the CSA variables.

To determine general correlations between the four variables – knowledge, self-perception of skills, actual skills and behaviour, attitudes – based on data from all the questions on the six cybersecurity topics, Pearson Correlation Coefficients were calculated for each, as presented in Figure 5.

Figure 5: Relationships between variables



It can be seen in Figure 5 that there are positive correlations amongst *knowledge*, *self-perception of skills*, and *actual skills and behaviour*. The strongest positive correlation is the relationship between *self-perception of skills* and *actual skills and behaviour*, with the other correlations having relatively low values. This indicates that *knowledge*, *self-perception of skills*, and *actual skills and behaviour*, have positive, albeit small, impacts

on each other. Meanwhile, all three of these variables are negatively correlated with *attitudes,* which is to say that: the more correct the *attitudes*, the lower the levels of *knowledge*, *self-perception of skills*, and *actual skills and behaviour* appear to be. The strongest negative correlation is between *knowledge* and *attitudes,* indicating that poor knowledge results in a good attitude, or vice versa. These negative correlations indicate a form of cognitive dissonance.

The dilemmas of cognitive dissonance on CSA matters

We saw above, in the "Findings" section and in the first part of this "Analysis" section, that: there are shortcomings in some areas of the students' cybersecurity *knowledge*, *actual skills and behaviour*, and *attitudes;* and in some of the cybersecurity areas for which the majority of students had strong *self-perception of skills,* the majority at the same time showed evidence of weak *actual skills and behaviour*, which implies a false sense of security. This misalignments and disconnects are concerning, and they were exhibited, in particular, in respect of the topics of (1) cyberbullying, (2) password security, (3) identity theft, and (4) phishing. It is thus evident that there are shortcomings in the CSA of many of the private tertiary students surveyed.

One of the most concerning results in the *knowledge* category (see Figure 3 and Table 1) was that over half of the students reported a weak understanding of phishing. And adding to the worrying nature of this finding was the fact that, at the same time, the majority of students gave a contradictory *self-perception* answer on the same topic, by indicating they are confident in being able to identifying a phishing email. This finding aligns to findings of the study by Kaur and Mustafa (2013), which concluded that there is no significant relationship between knowledge and true information security awareness. Similarly, Bada and Sasse (2014) reported that knowledge alone is insufficient for true awareness. Phishing attacks are becoming more prevalent, resulting in increased media attention on the topic, and increased attempts at education and awareness. Yet the CSA messaging in respect of phishing does not seem to be reaching the students, or they are ignoring it. This situation is precarious, as the results indicate the students have a false sense of security, which may make them more susceptible to falling victim.

Parbanath (2011) found that consumers exhibited a large degree of concern over the disclosure and protection of their personal information, yet at the same time, in contradictory fashion, had limited knowledge of the relevant legislation. The students surveyed in this research appeared to exhibit an analogous contradiction: concerned about phishing yet not managing to acquire the necessary knowledge. This confirms that knowledge alone is not enough, and that it needs to be combined with training, as in the phishing simulation exercise by Dodge and Ferguson (2006).

The majority of students professed to the correct *actual skills and behaviour* on phishing by agreeing that they will not open suspicious email attachment, which

AJIC 20-21-Jan-18-22h19.indd 148-149 1/21/2018 10:43:21 PM

corresponds to their *self-perception* that they can identify phishing attempts. But as discussed above, this does not correspond with their knowledge. Rajan's (2010) study found that those with knowledge and understanding of phishing still fell victim. And in spite of the widespread attention that phishing has received in recent years, a 2014 study by the University of California and Google reported that phishing attempts still succeeded 45% of the time (Beres, 2014).

The students surveyed seemed clearly to have a false sense of security. In the *actual skills and behaviour* section of the questionnaire, some of the answers provided were partially correct (e.g., the students would verify with the bank regarding a suspicious email). However, South Africa's banks, and awareness initiatives by SABRIC (2015), have clearly indicated that banks will not request details by email. Therefore the most clearly correct answer was to ignore and immediately delete the email.

Another worrying result was that over 40% of the respondents gave the view, in the *knowledge* section of the questionnaire (see Table 1), that an anti-virus program is sufficient protection against all possible attacks, and that, accordingly, they were well protected while online. This finding is consistent with Mishra's (2014) study, which reported that most computer users consider anti-virus software as adequate protection and think that firewalls and anti-virus software are the same (though modern Internet security applications do often include firewall functionality). Mensch and Wilkie's (2011) findings also indicated that a false sense of security may be gained by the installation of security tools, when in fact there is still vulnerability to other attacks such as identity theft and phishing.

In addition to their positive *self-perceptions of skills* in respect of phishing and anti-virus tools, the students also exhibited confidence in the strength of their passwords. Yet the students reported that it is too difficult to remember complex passwords so they stick to easy ones, and that they find changing passwords a waste of time. These are insecure behaviours. NIST SP 800-50 (2003) recommends regular changing of passwords, different passwords for different systems, as well as a minimum degree of password complexity. This should be enforced by CSA training (McCrohan, Engel, & Harvey, 2010). On a more positive note, the students confirmed their passwords should be kept secret. This contradicts the findings from the study by Steyn, Kruger and Drevin (2007), who found that over half the staff surveyed were happy to give out their passwords. As Steyn, Kruger and Drevin's (2007) study is more than 10 years old, we can perhaps assume that there has been some improvement in awareness of the need to keep passwords secret. Combined with the fact that the students considered it unacceptable to use the institution's network for messaging and social media, it could also indicate a link to heightened desire for privacy or secrecy.

The students also generally indicated positive *self-perception* in respect of not allowing themselves to fall victim to cyberbullying. However, research has found

that sometimes perpetrators do not realise their actions are cyberbullying, and, at the same time, incidents often go unreported by the victims (Oosterwyk, 2010). This may to some extent explain the respondent students' perception that they would not fall victim to cyberbullying.

Overall, positive *self-perceptions* were reported by the students for the various cybersecurity issues. Such confidence is misplaced when not linked to correct *knowledge*, *actual skills and behaviour*, and *attitudes*.

In respect of *actual skills and behaviour*, the responses indicated that the students allowed for system and anti-virus updates, downloaded from reputable sites, checked their privacy settings, and were careful about entering personal information and what they posted online. These results indicate secure behaviour, which is consistent with Pramod and Raman's (2014) study which found tertiary education students are familiar with broad security issues. However, at the same time, there was a high percentage of incorrect responses for skills in dealing with suspicious files (76%) and dealing with situations when a hacker gains access to a computer (43%).

For the *attitudes* category, the most significant and strongest result was that students agree that they would not receive scams or malicious emails from their friends. This is a potentially harmful attitude, as most friends share jokes and funny/interesting videos and images with family and friends, and these attachments are possible delivery mechanisms for malware. Malware could thus be unwittingly transmitted. Therefore this trust is misplaced. Also in respect of attitudes, the students correctly disagreed with the statements: that it is acceptable to post offensive pictures and bad messages about their peers; that it is time-consuming and annoying to update security software; that they turn off security settings; that patches and updates are not required; and that it is acceptable to download movies. The rejections of these statements represent appropriate cybersecurity *attitudes*. However, several of these responses do not align with the students' *actual skills and behaviour*. It would seem that, to some extent, the students know what the acceptable norms are, but are willing to forgo following many of the norms at personal level. This is one of several instances of apparent cognitive dissonance revealed by the findings.

6. Conclusions

Cognitive dissonance in respect of cybersecurity matters – of the sort displayed by the students who were the respondents in this research – is a phenomenon that is targeted by cyber-criminals (Kritzinger & Von Solms, 2010), indicating that the students are vulnerable to cyber-attacks.

The number of potential victims can be reduced by increasing CSA (Department of Communications, 2013), making cybercrime less profitable. This cognitive dissonance found to be present among the students is a vulnerability that cyber-

AJIC 20-21-Jan-18-22h19.indd 150-151 1/21/2018 10:43:21 PM

criminals exploit regularly, and indicates the need for a targeted CSA intervention to address the shortcomings of the specific population. The findings also suggest that generic awareness campaigns are no longer sufficient, and that an assessment of a target population is required to first identify the population's CSA shortcomings prior to designing the awareness campaign.

As CSA is a common issue affecting all computer and Internet users in South Africa, awareness levels in the country need to be assessed by surveying a large spectrum of the population. In order to achieve a baseline of CSA in South Africa, a "generic" CSA survey should be designed to be applicable across population segments, organisations, demographics and economic groups. The baseline data can be used over a period of time in larger longitudinal studies to monitor the effectiveness of implemented CSA initiatives. Deeper qualitative studies in CSA, investigating the underlying reasons and motives for specific users' knowledge, self-perceptions, actual skills and behaviour, and attitudes, also need be conducted to enhance understanding of the inter-relationships among these variables within various population segments.

Acknowledgements
This article is published as an extension to the first author's Master's dissertation (Chandarman, 2016).

References

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, Jakarta, 13-14 December. https://doi.org/10.1109/ict4m.2010.5971884

Ashford, W. (2015, April 10). French TV5Monde network cyber attack the latest in destructive trend in system intrusions. *Computer Weekly*. Retrieved from http://www.computerweekly.com/news/4500244107/French-TV5Monde-network-cyber-attack-the-latest-in-destructive-trend-in-system-intrusions

Bada, M., & Sasse, A. (2014). *Cyber security awareness campaigns Why do they fail to change behaviour?* Global Cyber Security Capacity Centre. Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Bakar, E. A., Chang, L. L., & Saidin, A. Z. (2013). Knowledge, attitude and practices of consumers in e-commerce transactions. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 5th International Conference. Rabat, 26-27 March. https://doi.org/10.1109/ict4m.2013.6518903

BBC News. (2014, August 6). Russia gang hacks 1.2 billion usernames and passwords. Retrieved from http://www.bbc.com/news/technology-28654613

Beres, D. (2014, July 11). Google study finds email scams are more effective than you'd expect. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2014/11/07/phishing-scams_n_6116988.html

BusinessTech. (2014, September 14). Internet fraud and phishing costs SA R2.2 billion. Retrieved from http://businesstech.co.za/news/general/68212/sa-internet-fraud-and-phishing-costs-r2-2-billion

Butler, R., & Butler, M. (2014). An assessment of the human factors affecting the password performance of South African online consumers. In N. Clarke, & S. Furnell (Eds), *Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2014)* (pp. 150-160), Plymouth, UK, 8-9 July.

Chandarman, R. (2016). *Cybersecurity awareness of students at a private higher education institute in South Africa*. Master's dissertation, University of KwaZulu-Natal, Westville, Durban.

Compuscan. (2014). Identity fraud on the increase. Retrieved from https://www.compuscan.co.za/identity-fraud-increase

Cyber Aces Foundation. (2014). US cyber challenge: Cyber quests April 2014. Retrieved from http://uscc.cyberquests.org

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security 29*(2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

Department of Communications (DoC). (2013). *Review report: E-commerce, cybercrime and cybersecurity – status, gaps and the road ahead*. Pretoria: Government of South Africa. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Review_Report_e-commerce_cybercrime%20and%20cybersecurity_final_0.pdf

Dodge R. C., & Ferguson A. J. (2006). Using phishing for user email security awareness. In S. Fischer-Hübner, K. Rannenberg L. Yngström. & S. Lindskog (Eds.), *Security and privacy in dynamic environments*. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May, Karlstad, Sweden. https://doi.org/10.1007/0-387-33406-8_41

Doyle, K. (2015, May 19). SA security policy trails Africa. *ITWeb*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=143303

Educause. (2017). Awareness campaigns. Retrieved from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352-357. https://doi.org/10.1108/09576050210447037

Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security, 17*(5), 388-407. https://doi.org/10.1108/09685220911006687

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Janssen, C. (2014). *Techopedia*. Retrieved from http://www.techopedia.com/it-dictionary

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In IEEE (Ed.), *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286-290). https://doi.org/10.1109/icriis.2013.6716723

AJIC 20-21-Jan-18-22h19.indd 152-153 1/21/2018 10:43:21 PM

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126. https://doi.org/10.1108/imcs-01-2013-0005

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement, *Computers & Security, 29*(8), 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Kyobe, M., Matengu, S., Walter, P., & Shongwe, M. (2012). Factors inhibiting recognition and reporting of losses from cyber-attacks: The case of government departments in the Western Cape Province of South Africa. In N. Tadgh (Ed.), *6th European Conference on Information Management and Evaluation* (pp. 159-167). Reading, UK: ACP.

Lee, Y., & Kozar, K. (2005). Investigating factors affecting the anti-spyware system adoption. *Communications of the ACM*, *48*(8),72-77.https://doi.org/10.1145/1076211.1076243

Lennon, M. (2015, April 12). FireEye uncovers decade-long cyber espionage campaign targeting South East Asia. *Security Week*. Retrieved from http://www.securityweek.com/fireeye-uncovers-decade-long-cyber-espionage-campaign-targeting-south-east-asia

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What are influences of ethical behaviour intentions – planned behaviour, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143-58. https://doi.org/10.1016/j.im.2003.12.008

Malandrino, D., Scarano, V., & Spinelli, R. (2013). How increased awareness can impact attitudes and behaviors toward online privacy protection. In IEEE (Ed.), *2013 International Conference Social Computing (SocialCom)* (pp. 57-62). https://doi.org/10.1109/socialcom.2013.15

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security, *Journal of internet Commerce, 9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14*(2), 91-153.

Minister of Justice and Correctional Services. (2015). *Cybercrimes and Cybersecurity Bill.* Draft for public comments. Republic of South Africa.

Mishra, U. (2014). Is anti-virus a necessary evil? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434470

Mitre. (2014, April). The Heartbleed Bug. Retrieved from http://heartbleed.com/

Mochiko, T. (2016, November 22). Cybercrime "will rise" with internet of things. *Business Live*. Retrieved from https://www.businesslive.co.za/bd/life/gadgets-and-gear/2016-11-22-cybercrime-will-rise-with-internet-of-things

MyBroadband. (2015, April 22). South Africans underestimate password value. Retrieved from http://mybroadband.co.za/news/security/124870-south-africans-underestimate-password-value.html

National Institute of Standards and Technology (NIST). (1998). *Information technology training requirements: A role-and performance-based model*. NIST Special Publication 800-16. Washington, DC: US Department of Commerce.

NIST. (2003). *Building an information technology security awareness and training program*. NIST Special Publication 800-50. Washington, DC: US Department of Commerce.

Office of the Australian Information Commissioner (OAIC). (2014). Privacy Awareness Week resources 2014. Retrieved from http://www.oaic.gov.au/news-and-events/privacy-awareness-week-2014/resources-2014#training

Oosterwyk, G., & Parker, M. (2010). Investigating bullying via the mobile web in Cape Town schools. Paper presented to the 2010 Annual Conference on WWW Applications, Durban, South Africa, 22-24 September. Retrieved http://www.zaw3.co.za/index.php/ZA-WWW/2010/paper/view/239

Parbanath, S. (2011). *Personal information security: Legislation, awareness and attitude*. Master's dissertation. University of KwaZulu-Natal, Westville, Durban.

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security, 14*(2), 37-49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research, 9*(23), 19133-19144.

Pretorius, B., & Van Niekerk, B. (2015). Cyber-security and governance for ICS/SCADA in South Africa. In J. Zaaiman, & L. Leenen (Eds.), *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 241-251). Reading, UK: ACP.

Rajan, M. (2010). *Internet phishing hook, line and hopefully not sunk*. MBA thesis, University of KwaZulu-Natal, Durban.

Rosenblatt, S. (2014, April 28). Stop using Microsoft's IE browser until bug is fixed, US and UK warn. *CNET*. Retrieved from http://www.cnet.com/news/stop-using-ie-until-bug-is-fixed-says-us

Rosewarne, C. (2013). *2012/3: The South African cyber threat barometer*. Retrieved from https://www.wolfpackrisk.com/research/south-african-cyber-threat-barometer

Ruiz, R. (2015, April 8). F.C.C. fines AT&T $25 million for privacy breach. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2015/04/08/f-c-c-fines-att-25-million-for-privacy-breach/?ref=topics

South African Banking Risk Information Centre (SABRIC). (2015). Website. Retrieved from https://www.sabric.co.za

Steyn, T., Kruger, H. A., & Drevin, L. (2007). Identity theft – empirical evidence from a phishing exercise. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. Von Solms (Eds), *New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC 11 22nd International Information Security Conference (SEC 2007)* (pp. 193-203). https://doi.org/10.1007/978-0-387-72367-9_17

Symantec. (2013). *2013 Norton report: Cost per cybercrime victim up 50 percent*. Retrieved from http://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029_01

TroyHunt. (2014). Everything you need to know about the Shellshock Bash bug. Retrieved from http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wlasuk, A. (2012, June 29). Higher education – the perfect security storm. *Security Week*. Retrieved from http://www.securityweek.com/higher-education-perfect-security-storm

AJIC 20-21-Jan-18-22h19.indd 154-155 1/21/2018 10:43:22 PM

THEMATIC REPORTS

AJIC 20-21-Jan-18-22h19.indd 156-157 1/21/2018 10:43:22 PM

Potential Contribution of Drones to Reliability of Kenya's Land Information System [1]

Patricia Kameri-Mbote
Professor, School of Law, University of Nairobi

Muriuki Muriungi
Tutorial Fellow, School of Law, University of Nairobi; and MSc Candidate, University of Oxford

Abstract
Kenya has sought in recent years to digitise its land information system in order to increase reliability and accessibility, both of which are critical to securing land rights, minimising land disputes, and increasing investment in the sector. This thematic report argues for deployment of drone technology in order to increase the reliability of Kenya's digital land records.

Keywords
land information system, land records, surveying, mapping, land rights, land disputes, digitisation, drones, Kenya

DOI: https://doi.org/10.23962/10539/23500

Recommended citation
Kameri-Mbote, P., & Muriungi, M. (2017). Potential contribution of drones to reliability of Kenya's land information system. *The African Journal of Information and Communication (AJIC)*, *20*, 159-169. https://doi.org/10.23962/10539/23500

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

1 Elements of this thematic report were presented in draft form at the Annual World Bank Conference on Land and Poverty, 20-24 March 2017, Washington, DC, https://www.conftool.com/landandpoverty2017/index.php?page=browseSessions&form_session=594#paperID333

AJIC 20-21-Jan-18-22h19.indd 158-159 1/21/2018 10:43:22 PM

1. Introduction

Kenya is engaged in spirited attempts to digitise its land records. The manual system was fraught with multiple challenges: human error, opportunities for corruption due to missing files, incomplete land information, difficulties in accessing records, and cases of multiple titling – all of which served to make land rights generally insecure in Kenya. The Ministry of Lands and Physical Planning has embarked on an ambitious process of digitising existing land records, in a bid to enhance both data reliability and security of tenure.

In addition to digitisation of existing records, we propose increased use of drone (unmanned aerial vehicle) technology in support of land mapping, particularly in remote areas, in order to enhance the accuracy of the data in the registries that are in the process of being digitised. The data obtained through the use of drones could facilitate more accurate delineation of boundaries among land holdings, thus minimising contestation. Unlike maps created through traditional surveys, those generated through the use of drone technology have more details, enabling the recognition of various landmarks and buildings (*Asian Survey and Mapping,* 2016). Another advantage of drone technology is that it is rapid, enabling mapping and surveying of as many as 40 hectares in a single day (*Asian Survey and Mapping*, 2016).

Up to 60% of surveying costs under the traditional surveying method are the logistical costs incurred by a survey team (Almenteros, Arnante, & Dealca, 2016). Using drone technology eliminates the need for on-the-ground logistic teams, thus obviating these costs (Almenteros et al., 2016). Moreover, drones are able to map large areas in a short span of time, thus enabling rapid land-mapping and titling.

2. Land information in Kenya

Kenya's antiquated manual land information system is traceable to 1902 when the then-Recorder of Titles under the British colonial regime used to keep titles under the Registration of Titles Act (RTA) system (Wayumba, 2013). These paper records are prone to wear and tear, loss, theft, being hidden, or even being deliberately misplaced. The manual land recording system has also been associated with double allocation of title for a single piece of land, missing files, and erroneous (sometimes fraudulent) transfers of titles (*Business Daily*, 2015). Frustration encountered by people transacting land rights has acted as a disincentive to engaging and investing in the sector (Ayodo, 2014). A simple search may take over a week due to bureaucracy and interference by cartels and brokers who seek to benefit from the system (Ayodo, 2014). The *Doing Business in Kenya Report 2016* was critical of Kenya's dearth of digitised land records, particularly outside Nairobi (World Bank, 2016).

The tenacity of Kenya's manual land records in registries around the country is remarkable considering the digitisation efforts that have been pursued over the years (Mutiga, 2009; Mbaka, 2013; Wanzala, 2015). The failure to secure a fully digitised

land information system can be attributed to: resistance by actors within the land sector who perceive digitisation as a threat; lack of adequate human and financial resources; lack of political will and leadership; and torn, missing and incomplete land records (Mbaria, 2009; Ntonjira, 2016).

Following the post-election violence of late 2007 and early 2008 occasioned by a disputed Presidential election and the identification of land disputes as a contributing factor to the violence (Kameri-Mbote & Kindiki, 2008), land reform emerged as an agenda necessitating immediate action. This fed into the finalisation of the National Land Policy in 2009, which, inter alia, called for digitisation of land records to avert fraud (Ministry of Lands, 2009). This was not the first time that computerisation and digitisation of land records had been suggested (see (Republic of Kenya, 2008), but inclusion of this matter in the National Land Policy signaled a more serious consideration, and digitisation is now a statutory obligation, as enshrined under sections 9 and 10 of the Land Registration Act of 2012.

According to the Land Governance Assessment Framework (LGAF) Report of 2014-2015 prepared for the World Bank, which assessed the status of land governance in Kenya, the manual land-recording system is inefficient, time-consuming and militates against timeous decision making (Kameri-Mbote, 2016). A Commission set up to investigate illegal and irregular allocations of land in Kenya found that that uncertainty generated by multiple titles over single pieces of land "has the potential of disrupting the land market and jeopardising the general development of the country" (Republic of Kenya, 2004).

Meaningful social and economic development are threatened in the absence of secure land rights (Besley & Ghatak, 2009), which in turn are dependent on reliable and easily accessible land information. Recent contestations over ownership of prime pieces of land in Nairobi are apt illustrations of the problematic nature of land governance in Kenya and the difficulties that arise in determining the ownership of land in the absence of reliable information. A scandal relating to alleged "grabbing" of a 144-acre piece of land in the prime Karen estate in the south of Nairobi is a case in point (Nyassy, 2014). Various individuals claimed ownership of the land, and some had sold the land to third-party purchasers (Nyassy, 2014). Politicians and other leaders were allegedly linked to the fraud, but investigations to determine the real owners of the land were unsuccessful (Nyassy, 2014).

Similar disputes have arisen over land in Nairobi's prime Westlands and Parklands areas, regarding renewal of leases (Achuka, 2016; Mutavi, 2016). Instances abound where cartels are alleged to have colluded with officials from the Ministry to put up notices requesting application for renewal of leases on parcels of land, in default of which they dispossess owners of the land (Mutavi, 2016). There is also evidence of cases where lessees whose leases are expiring and who should have the first right of

AJIC 20-21-Jan-18-22h19.indd 160-161 1/21/2018 10:43:22 PM

reversion are evicted violently (Ombati, 2016).

Contestation over ownership of land allegedly belonging to the United States International University (USIU), pitting a former President of Kenya Daniel Moi against two investors, also sheds light on the lack of clarity on land ownership (Agoya, 2016; Wasuna, 2016). Lands targeted by cartels have even included lands housing public entities. Such was the case in the Lang'ata area of Nairobi when land belonging to a public primary school was at issue (Muthoni, 2015).

Thus, the importance of reliable and publicly accessible land information cannot be over-emphasised. At present in Kenya, surveying for cadastre maps (maps showing land ownership and boundaries) is largely done through varying spatial referencing systems by physical surveyors (Wayumba, 2013). This has contributed to difficulties in integration of survey plans to create a seamless map (Kuria, Kasaine, Khalif, & Kinoti, 2016). Survey data such as Registry Index Maps and survey plans are not in a common referencing framework, resulting in inconsistencies in the interpretation of survey plans and disputes (Kuria, Kasaine, Khalif, & Kinoti, 2016). Cognizant of these shortcomings, the Ministry of Lands and Physical Planning's National Spatial Plan is seeking to modernise land registries (including making them more publicly accessible), is establishing a Kenya National Spatial Data Infrastructure (KNSDI) centre, and has embarked on various processes to build an updated, easily accessible and reliable National Land Information Management System (NLIMS) (Ministry of Lands and Physical Planning, 2017; GSDI, 2016). The NLIMS processes include digitisation of land paper records in various registries across the country (*Daily Nation*, 2017). In order to digitise land records, the Ministry has in particular operationalised an Electronic Records Management System (ERMS) and up-scaled the digital access systems (Ministry of Lands and Physical Planning, 2017). It is worth noting that the Ministry has on different occasions disrupted normal services at its headquarters in Ardhi House, Nairobi to load its land paper records onto electronic platforms in a bid to digitise (Omulo, 2017). Various registries including Kisumu, Meru, Mombasa, Kwale, Kilifi, Eldoret, Bungoma, Kiambu, Thika, and the Central Registry in Nairobi, are digitised, in a process that began in September 2016 (Omulo, 2017).

The Constitution of Kenya of 2010 provides in Article 35(1)(a) for the right to access information held by the State and other persons, especially where it is required for enforcement of one's fundamental rights and freedoms (Republic of Kenya, 2010). To implement this provision, Kenya enacted the Access to Information Act 31 of 2016, which provides that the government or a public authority shall provide the information requested within 21 days of such request (sect. 9), unless such request falls within any of the listed exceptions (sect. 6) (Republic of Kenya, 2016). Kenyan individuals or corporations may lawfully demand information from public entities

including the Ministry and other state entities responsible for land administration and governance.

Article 60 of the Constitution recognises secure land rights, indirectly imposing a duty on state entities to ensure that they have proper and reliable records in this regard. Section 7(2) of the Land Registration Act 3 of 2012 provides that the Registrar of each Land Registry shall make information relating to land accessible to any person upon payment of the prescribed fee (Republic of Kenya, 2012). Section 9 of the same statute provides that the Land Registrar shall maintain the register and any document in a secure, reliable and accessible format, including electronic files. Section 10 provides that subject to the right to access information under the Constitution, the Registrar shall make information accessible to the public by electronic means or other means as prescribed by the Chief Land Registrar. These statutory provisions mandate state agencies to put in place mechanisms to facilitate the relaying of updated records and to enhance accessibility by the public. The National Broadband Strategy identifies the digitisation of land registries and the development of the aforementioned KNSDI as focus areas for implementation.

3. Drones and mapping of land information

Mapping land information using drone technology involves the use of GPS-enabled drones to conduct aerial surveys. Drones are able to capture high-resolution images, which are then used by land planners to not only identify, but also digitise the record of boundaries of any land (Pablo & Petzold, 2016). Drones' advantages over the traditional methods of mapping are: increased speed, increased reliability, and fewer costs than with sending surveyors out to physically map (Pablo & Petzold, 2016). Drones also have the advantage of easily reaching remote, largely unsurveyed areas (Pablo & Petzold, 2016).

Drones have been previously employed in Kenya for recreational activities such as photography and security (Bonyo, 2015). Their use was, however, halted by the government in 2015, pending the promulgation by the Kenya Civil Aviation Authority (KCAA) of regulations to guide their usage and address possible breaches of security and infringement on privacy (Johnson, 2015). The KCAA finalised rules in 2017 (KCAA, 2017) to guide the licensing, approval and flying of drones in Kenya (Kuo, 2017). Various license-seekers, estimated at around 1,000, prompted the drafting and approval of the regulations to use drones for various purposes (Andae, 2016). For instance, the Ol Pejeta Conservancy had sought permission to use drones to fight poaching (Andae, 2016). In the regulations, the KCAA has categorised the use of drones into: those for recreation and sports; for private use excluding sports and recreation; and for commercial activities (Njoroge, 2016). The agency also classifies drones in accordance with their weight and uses in the rules, which also impose criminal liability for breach (Njoroge, 2016). The regulations have filled the

AJIC 20-21-Jan-18-22h19.indd 162-163 1/21/2018 10:43:23 PM

regulatory vacuum, which, without doubt, hindered further acquisition and usage of the technology for various beneficial purposes.

Several countries have harnessed drones to enhance the reliability and accessibility of their land-mapping. We now describe two such examples, in Tanzania and The Philippines.

Tanzania

In 2014, Tanzanian media reported several clashes over land among farmers in the country's northern Maynard region (Makoye, 2016). In 2016, it was reported that farmers in the southwest region of Morogoro killed hundreds of livestock on grounds that the livestock-owners had let the animals roam onto their land and destroy their crops (Makoye, 2016). These conflicts were to some extent caused by unclear demarcations of land boundaries (Makoye, 2016). It was this challenge that the Tanzanian government sought to overcome using drone technology. In a project supported by the World Bank and the Tanzania Commission for Science and Technology, boundaries were mapped with drones and over 300,000 land titles were issued to citizens (Makoye, 2016).

The initial use of drone technology in Tanzania, before its use in land-mapping, was for mitigation of the effects of floods in the capital Dar es Salaam. With over 70 per cent of the population in the capital living in informal settlements prone to flooding (Soiselo, 2016), drones were used to help to generate accurate maps of the localities and thus assist administrators in drawing up accurate plans to protect persons at risk in flood-prone areas (Makoye, Drones help communities map flood risk in Dar es Salaam slums, 2017).

The Philippines

The Philippines has applied drone technology in mapping land for surveying and titling (Asian Survey and Mapping, 2016). The country has around 24 million parcels of land, of which only about half are surveyed and titled (Pablo & Petzold, 2016). The high costs associated with surveying land were cited as one of the reasons for the many pieces of unsurveyed and untitled land (Pablo & Petzold, 2016). In a bid to accelerate the process of titling, the Asia Foundation partnered with the Foundation for Economic Freedom and Omidyar Network in a project that used drones to conduct land surveys (Pablo & Petzold, 2016). A study found that use of drones was more cost-effective and faster than the conventional surveying methods (Almenteros et al., 2016). The study recommended a policy change in Philippines to allow the use of drones as one of the official techniques in land mapping and surveying (Almenteros et al., 2016)

4. Recommendations

There are several steps that the Kenyan government should take so as to be able to use drones in support of development of a more reliable national land information system. The aforementioned KNSDI is only possible through the prudent use of information and communication technologies (ICTs) (Odongo & Rodriques, 2016), and drones need to be among the ICTs used.

The Ministry of Lands and Physical Planning should apply to the Communications Authority of Kenya for authorisation and spectrum allocation for use of drone technology to capture land-mapping data. At the same time, land data generated through drone technology can only be reliable if it is protected from hacking and tampering, both of which are currently major concerns with Kenyan land data. Indeed, there is evidence that that processes of digitisation and computerisation of records, and land reforms generally, have been thwarted severally by interested parties and cartels (Kariuki, 2017). Accordingly, the Computer and Cybercrimes Bill of 2017 (Republic of Kenya, 2017) needs to become law, so as to prevent fraud and address other vulnerabilities in respect of land-mapping. It is also necessary to to fast-track the enactment of the Data Protection Bill of 2013, to deal with privacy concerns. To support the use of drones, there is need for capacity building beyond traditional disciplines such as survey and the use of multidisciplinary approaches to capture land information. The Ministry responsible for land can also apply for allocation of spectrum to enable it deploy technology effectively.

Land information management in Kenya is currently unreliable and inaccessible. Efficient and effective land information management can improve security of land rights in Kenya and neutralise land cartels and intermediaries who act as gatekeepers in Land Registries and open the way for corruption. While technology is not a silver bullet or a panacea, and indeed can be manipulated – as fraud in Kenya's Integrated Financial Management Information System (IFMIS) has shown (Okoth, 2017) – properly managed use of drones can improve the reliability of land information in Kenya, thus contributing to more secure land rights, more investment, and fewer opportunities for fraud.

References

Association for Progressive Communications (APC). (2014). *Global information society watch 2014: Communications surveillance in the digital age.* Retrieved from http://giswatch.org/2014-communications-surveillance-digital-age

Achuka, V. (2016, December 24). Dispute over Nairobi property creates confusion over who is responsible for alleged vandalism. *Daily Nation*.

Agoya, V. (2016, October 6). Moi in court over disputed prime Nairobi land sale. *Daily Nation*.

Almenteros, M. I., Arnante, A., & Dealca, R. L. (2016). *Drones: A gamechanger in land surveying and titling.* Quezon City, Philippines: Foundation for Economic Freedom (FEF). Retrieved from http://landrightsph.org/resources/news-and-events/drones-a-gamechanger-in-land-surveying-and-titling/

AJIC 20-21-Jan-18-22h19.indd 164-165 1/21/2018 10:43:23 PM

Andae, G. (2015, January 19). Defence ministry to regulate use of drones on safety fears. *Business Daily*.

Andae, G. (2016, August 14). Kenya drone licence seekers hit 1,000. *Business Daily*.

Asian Survey and Mapping. (2016, July 11). Philippines accelerate land mapping with drones. Retrieved from https://asmmag.com/features/feature/11197-philippines-accelerate-land-mapping-with-drones.html

Ayodo, H. (2014, February 21). Manual land records a nightmare. *Standard Digital*.

BBC News. (2013, November 7). Kenya launches Huduma e-centre to cut bureaucracy.

Besley, T., & Ghatak, M. (2009). Property rights and economic development. In D. Rodrik, & M. Rosenzweig (Eds.), *Handbook of development economics* (pp. 4525-4595). London: Elsevier. https://doi.org/10.1016/b978-0-444-52944-2.00006-9

Bonyo, K. (2015, June 4). Everything you need to know about drones in Kenya. Blog post. Retrieved from http://www.kenbonyo.com/everything-you-need-to-know-about-drones-in-kenya/

Business Daily. (2015, February 12). Editorial: Digitisation of land records must succeed at all costs. Retrieved from http://www.businessdailyafrica.com/analysis/Digitisation-of-land-records-must-succeed-at-all-costs/539548-2622044-2x1c5v/index.html

Cisco. (2009, July 23). Seacom goes live. Retrieved from https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=5035494

Dolson, D., Hahn, N., Palminteri. S., Dinerstein, E., Konuche, J., Chang'a, A., Keyyu, J., Mwakatobe, A., & Goss, A. (2016). *Farmer-elephant coexistence: Unmanned aerial vehicles (UAVs) for Reducing elephant crop-raiding.* Azle, TX: International Elephant Foundation.

Daily Nation. (2017, January 16). Hasten digitization of all land records.

Famy Care Limited v Public Procurement Administrative Review Board & another & 4 others, 2013 eKLR (High Court 2013).

Global Spatial Data Infrastructure Association (GSDI). (2016, March 22). Kenya: New Geo-Spatial Data Centre to house National Spatial Data Infrastructure Secretariat.

Gordon Institute of Business Science (GIBS). (2013). *Digital disruption: Changing the rules of business for a hyper-connected world.* Authored with Dimension Data. University of Pretoria.

Ihucha, A. (2014, November 15). Tanzania now bans private drones from overflying its national parks, cites security. *The East African*.

Internet World Stats. (2016). *Africa 2016 population and Internet users statistics for 2016*.

Johnson, E. (2015, December 15). *Kenya basically bans all drone use — despite potential benefits they may yield*. Retrieved from http://www.pri.org/stories/2015-12-15/kenya-basically-bans-all-drone-use-despite-potential-benefits-they-may-yield

Kameri-Mbote, P. (2016). *Kenya land governance assessment framework report (LGAF).* Nairobi: World Bank. https://doi.org/10.1596/28502

Kameri-Mbote, P., & Kindiki, K. (2008). Trouble in Eden: How and why unresolved land issues landed "peaceful Kenya" in trouble in 2008. *Forum for Development Studies*, *35*(2), 167-193. https://doi.org/10.1080/08039410.2008.9666408

Kameri-Mbote, P., Mony-Odhiambo, F., Muriungi, M., & Nyawira, O. (2016). *Spectrum management and regulation in Kenya: Engendering inclusive access to technology and information.* Nairobi: Ford Foundation.

Kariuki, J. (2017, January 2). Nairobi blames ministry cartels for land theft. *Daily Nation*.

Kenya Civil Aviation Authority (KCAA). (2017). The Civil Aviation (Remotely Piloted Aircraft Systems) Regulations, 2017. Retrieved from https://www.airport-uav.com/wp-content/uploads/2016/03/RPAS-DRAFT-Regulations-2017.pdf

Kuo, L. (2017, February 14). Kenya has approved the commercial use of drones. *Quartz Africa*. Retrieved from https://qz.com/910113/kenya-has-approved-the-commercial-use-of-drones/

Kuria, D., Kasaine, A., Khalif, A., & Kinoti, S. (2016). Developing a national land information management system - the Kenyan strategy. Paper presented to the Annual World Bank Conference on Land and Poverty, Washington, DC, 14-18 March.

Lindley, J., & Colton, P. (2016, May 3). *Game of drones*. https://doi.org/10.1145/2793107.2810300

Makoye, K. (2016, September 8). Tanzania turns to drones to bring peace in bitter fight for land. *Reuters*.

Makoye, K. (2017, January 4). Drones help communities map flood risk in Dar es Salaam slums. *Reuters*.

Manske, J. (2014). *Innovations out of Africa: The emergence, challenges and potential of the Kenyan tech ecosystem.* Berlin: Vodafone Institute for Society and Communications.

Mbaka, J. (2013, September 3). Lands ministry to digitise records, says Charity Ngilu. *Standard Digital*.

Mbaria, C. N. (2009). Kenya's experience towards the establishment of land information management system: Automation of Kenya's land records. Presentation slides. Nairobi: Ministry of Lands.

Ministry of Lands. (2009). *Sessional paper No. 3 of 2009 on National Land Policy.* Nairobi.

Ministry of Lands and Physical Planning. (2017, January 2). Key achieved projects. Retrieved from http://www.ardhi.go.ke/?page_id=216

Moime, D. (2016, April 25). Kenya, Africa's Silicon Valley, epicentre of innovation. Venture Capital for Africa. Retrieved from https://vc4a.com/blog/2016/04/25/kenya-africas-silicon-valley-epicentre-of-innovation/

Mulaku, G. (2012). *Land information management in Kenya: An integrated approach.* Department of Surveying, University of Nairobi.

Murungi, M. (2011). *Cyber law in Kenya.* The Netherlands: Kluwer International.

Mutavi, L. (2016, December 22). High Court restrains NLC from resolving Nairobi land dispute. *Daily Nation*.

Muthoni, K. (2015, January 14). Disputed land belongs to Langata Road Primary School, declares Mohamed Swazuri. *Standard Digital*.

Mutiga, M. (2009, November 14). Digitisation of land records to attack rot at head office. *Daily Nation*.

Mutuku, D. (2015, July 14). How Huduma is transforming public service. *Standard Digital*.

Nairobi Law Monthly Company Limited v. Kenya Electricity Generating Company (KENGEN) & 6 others, 2013 eKLR (High Court 2013).

National Treasury. (2016, December 1). Tender document for digitisation of land records in various registries. Retrieved from http://supplier.treasury.go.ke/site/tenders.go/index.php/public/tender_view/9999

Ncube, M., & Ondiege, P. (2016). *Silicon Kenya: Harnessing ICT innovations for economic development.* Abidjan: African Development Bank.

Ndemo, B. (2016, April 11). iHub is evolving to help more start-ups grow and compete. *Daily Nation*.

AJIC 20-21-Jan-18-22h19.indd 166-167 1/21/2018 10:43:23 PM

Ng'aru, S. W., & Wafula, M. K. (2015). Factors influencing the choice of Huduma Centers' services (A case study of Mombasa Huduma [Center]). *International Journal of Scientific and Research Publications*, *5*(6), 1-9. https://doi.org/10.6007/ijarbss/v5-i6/1660

Njoroge, K. (2016, March 31). Authority limits civilian drone operators to height of 400ft. *Business Daily*.

Ntonjira, L. (2016). Challenges of developing land information management systems (LIMS) for county governments in Kenya. Presentation slides. 11th ESRI Eastern Africa User Conference, Nairobi: 2-4 November.

Nyassy, D. T. (2014, October 17). Probe Karen land scam, Ngilu tells ethics team. *Daily Nation*.

Nyongesa, L. N. (2012, January 1). GIS-based national land information management system (NLIMS). Paper for FIG Working Week 2012, Rome, 6-10 May.

Obwocha, B. (2014, November 25). Government, Safaricom sign deal for Sh15 billion security surveillance system. *Daily Nation*.

Odongo, R. O., & Rodriques, A. J. (2016). *Metadata models and standards for Kenya National Spatial Data Infrastructure: A case study of 12 government ministries.* School of Computing and Informatics, University of Nairobi.

Ogutu, J. (2015, May 18). How ICT drives Kenya's economic growth. *Standard Digital.*

Okoth, E. (2017, January 8). State audit finds serious loopholes in Ifmis system. *Daily Nation*.

Okuku, J., Bregt, A., & Grus, L. (2014). Assessing the development of Kenya National Spatial Data Infrastructure (KNSDI). *South African Journal of Geomatics*, *3*(1), 95-112.

Okuttah, M. (2015, May 24). Safaricom's security system live in Nairobi, Mombasa. *Daily Nation*.

Olopade, D. (2014). *The bright continent.* New York: Houghton Mifflin Harcourt.

Ombati, C. (2016, December 5). Elderly couple violently evicted from house in Westlands, Nairobi over lease dispute. *The Standard.*

Omulo, C. (2017, January 15). Digitisation of Lands records to disrupt services. *Daily Nation*.

Onoma, A. K. (2010). Endogenous contributions to institutional change. In *The politics of property rights institutions in Africa* (pp. 176-193). Cambridge: Cambridge University Press. https://doi.org/10.1017/cbo9780511691942.009

Pablo, M. C., & Petzold, O. (2016). *Using drone technology to improve land titling in the Philippines.* Pasig, Philippines: The Asia Foundation.

Peake, A. (2013). *Kenya's ICT sector, mobile money and the transformation to a middle-income country.* Tokyo: Center for Global Communications (GLOCOM).

Pilling, D. (2016, April 27). Kenyans start to roam Silicon Savannah. *Financial Times*.

Republic of Kenya. (2004). *Report of the Commission of Inquiry into the Illegal/Irregular Allocations of Land.* Nairobi: Government Printer.

Republic of Kenya. (2008). *First medium term plan (2008-2012): Kenya Vision 2030.* Nairobi.

Republic of Kenya. (2010, August 27). Constitution of Kenya 2010. Retrieved from https://www.kenyaembassy.com/pdfs/the%20constitution%20of%20kenya.pdf

Republic of Kenya. (2012, April 27). Land Registration Act 3 of 2012, Cap 300. Retrieved from http://extwprlegs1.fao.org/docs/pdf/ken112133a.pdf

Republic of Kenya. (2016, September 7). Access to Information Act 31 of 2016. Retrieved from http://kenyalaw.org

Republic of Kenya. (2017, June 13). *Computer and Cybercrimes Bill, 2017*. Retrieved from http://kenyalaw.org

Smith, D. (2014, June 4). Internet use on mobile phones in Africa predicted to increase 20-fold. *The Guardian*.

Soiselo, D. (2016, November 1). Using drones to map and model flood risks in Dar es Salaam, Tanzania. *Floodlist*.

Sunday, F. (2015, September 14). Safaricom banks on new spectrum to deepen its 4G services. *Standard Digital.*

UAV Systems International. (2016, February 1). *Kenya drone laws*. Retrieved from https://uavsystemsinternational.com/drone-laws-by-country/kenya-drone-laws/

Wanzala, J. (2015, October 31). Experts: Digitising land records requires Sh10b. *Standard Digital.*

Wanzala, J. (2016, December 8). Nairobi County to digitise lands registry by February. *Standard Digital.*

Wasuna, B. (2016, August 31). Equity Bank's Mwangi joins USIU's land battle with Moi. *Business Daily*.

Wayumba, G. O. (2013, February 28). *An evaluation of the cadastral system in Kenya and a strategy for its modernization.* PhD thesis, University of Nairobi.

Wayumba, G. (2013). The structure of the cadastral system in Kenya. *Journal of Land Administration in Eastern Africa*, *1*(1), 6-20.

World Bank. (2010). *Kenya economic update.* Edition No. 3. Washington, DC. https://doi.org/10.1596/27776

World Bank. (2016). *Doing business in Kenya 2016*. Retrieved from http://www.doingbusiness.org/~/media/WBG/DoingBusiness/Documents/Subnational-Reports/DB16-Sub-Kenya.PDF

World Bank. (2016). *Tanzania: Using drone technology to secure land rights*. Retrieved from http://www.worldbank.org/en/news/video/2016/07/25/tanzania-using-drone-technology-to-secure-land-rights

AJIC 20-21-Jan-18-22h19.indd 168-169 1/21/2018 10:43:23 PM

Reflections on Legal Uncertainties for e-Commerce Transactions in Cameroon [1]

Caroline Joelle Nwabueze
Post-Doctorate Research Fellow, at the South African Research Chair in Law, Society and Technology, College of Law, University of South Africa (UNISA), Pretoria

Abstract
This thematic report appraises legal provisions currently governing e-commerce transactions in Cameroon, in particular the matter of online contracts for sales of goods and services. There are uncertainties for Cameroonian consumers in the legal provisions at both regional level – via the Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA, the Organisation for the Harmonisation of Business Law in Africa) – and at Cameroonian national level. The report recommends steps to be taken to remedy the uncertainties.

Keywords
e-commerce, online transactions, online contracts, OHADA, consumer protection

DOI: https://doi.org/10.23962/10539/23499

Recommended citation
Nwabueze, C. J. (2017). Reflections on legal uncertainties for e-commerce transactions in Cameroon. *The African Journal of Information and Communication (AJIC)*, *20,* 171-180. https://doi.org/10.23962/10539/23499

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

1 This thematic report draws on the contents of the author's paper presented at the International Colloquium on Consumer Protection, University of Yaoundé II, Cameroon, in January 2017. The author's participation in the conference was supported by sponsorship from the South African Research Chair in Law, Society and Technology, University of South Africa (UNISA), by South Africa's Department of Science and Technology (DST), and by the National Research Foundation (NRF) of South Africa.

AJIC 20-21-Jan-18-22h19.indd 170-171 1/21/2018 10:43:23 PM

1. Introduction

Increased use of computers, Internet and other information and communication technology (ICT) tools have led to tremendous changes in the practices of commerce (Bolton, 2009). ICT-enabled mechanisms have engendered a vast electronic marketplace for the conclusion of contracts for sale of goods and services. The global e-commerce system draws much of its power from the savings it enables in terms of cost, time, distance, and efficiency (Boss, 2015). Internet-enabled e-commerce is allowing for continuous changes in the way companies do business (Estrella-Faria, 2009). Accordingly, if e-commerce is to fulfill its economic empowerment potential, legal systems do need to be adjusted so as to accommodate the emerging business practices.

A core difficulty is that distance selling in the course of e-transactions in the cyberspace was never envisaged by the legislator of the traditional law of contracts (Pistorius, 2004). Purchasing goods or services on this basis does mean that it is difficult for the customer to examine them prior to concluding a contract (Lloyd, 2014). The principles of law of contracts are old, shaped for a world of ink and paper (Pistorius, 2004). Their transplantation in e-commerce contract formation raises numerous questions. Specifically, it is crucial to have clear legal entitlements for online expression of an offer, and online acceptance of an offer, in order to preserve contract enforceability.

In this report, I set out some of the issues at play for contract formation (offer and acceptance) in the new environment of electronic commerce. I then give a sense of how the African regional inter-governmental legal organisation, the Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA, the Organisation for the Harmonisation of Business Law in Africa), has engaged with e-commerce matters to date, followed by consideration of how one OHADA Member State, Cameroon, has engaged at national level. I then identify gaps that will need to be addressed by lawmakers at either OHADA or Cameroonian national level in order for e-commerce to achieve its full potential as a source of economic empowerment in Cameroon.

2. Contract formation in the online sphere

It is universally recognised that consent to an "invitation to treat" (i.e., an offer to sell) plays an unequivocal role in the formation of a contract in the field of business. This consent provides both parties with clarity and certainty as to the terms and object of the transaction, and their acquiescence in respect of the characteristics of the goods or services to be provided in terms of the transaction. Security in a commercial agreement cannot be ascertained in the absence of certainty that both parties have effectively agreed to the transfer of the goods, and to the terms of the transfer.

A difficulty with the online realm, as legal scholar Dahiyat (2011) explains, is the absence of face-to-face encounter between buyer and seller:

> [because] it is likely that online parties will have no previous or personal knowledge of their partners, it is difficult to expect them to be sure of the identity and correctness of their partners or to know whether an electronic order is in fact placed by the person who pretends to be the offeror. It may also be very difficult for them to determine precisely whether the content of an order is altered during its transmission from the sender to the recipient. (Dahiyat, 2011, p. 298)

The rules of ethics and contractual loyalty in business agreements require that the parties to a contract must have received full knowledge of the terms of the offer before giving their agreement. Such rules can become strained in the context of online contract formation for online transactions. Face-to-face interaction in the course of formation of business agreement in the paper-based environment is susceptible to fewer mistakes than in the online environment.

Online business transactions make use of the Internet or other electronic media in the pre-contractual period of negotiation. During this period, the two parties, the seller and the buyer, have potentially conflicting interests. These contrasting interests coupled with distance and online impersonalisation have the potential to make it difficult for parties to the agreement to determine precisely whether the offer (or acceptance), as electronically expressed, clearly reflects the intent of the other party. Because of the foregoing, it is important for legislation to take into account the issues peculiar to online commercial contracts, during which, among other things, consumers are potentially exposed to fraudulent practices (Erasmus, 2011).

One example of a fraught issue is whether a click on an icon on the website of a vendor – in the case, for example, of click-through agreements (also known as "click-wrap agreements") – can qualify as unequivocal assent. In other words, is the consumer bound into an online contract by clicking on an icon provided on a trader's website? This question has been raised before numerous courts.

In the case in *Davis v. HSBC Bank Nevada, N.A.*, the plaintiff filed a class action complaint alleging among others false advertising. The plaintiff contended that the relevant portions of the terms and conditions were not visible without scrolling down on the trader's website. The court found that the plaintiff's failure to read the terms and conditions before checking the box accepting the terms was irrelevant to determining enforceability. The court reasoned that the contested annual fee was "within the plaintiff's observation", and therefore binding.

AJIC 20-21-Jan-18-22h19.indd 172-173 1/21/2018 10:43:24 PM

In another case, *Jerez v. JD Closeouts*, the court found that if the "terms of sale" are simply buried or "submerged" in multiple layers of web pages, and such terms are not specifically brought to the consumer's attention, their content will not be deemed part of the parties' agreement. Thus, uncertainty still exists as to whether or not a click by the consumer constitutes a legally recognisable act signifying one's intent to be contractually bound as such where terms were unilaterally imposed (Snail, 2008, p. 4).

3. Legal provisions in OHADA

OHADA is an inter-governmental body, established by treaty in 1993, that currently has 17 Member States, including Cameroon. With the exception of Comoros (an East African island state), all OHADA Member States are in Central and West Africa. And with the exception Equatorial Guinea (a formers Spanish colony), all OHADA members are former French colonies.[2]

One of OHADA's core functions is the issuance of Uniform Acts, which are directly applicable in all Member States. OHADA Uniform Acts do not, however, prevent the Member States from enacting specific legislation in the same sphere as that covered by a Uniform Act, provided the national legislation does not conflict with the Act (Martor, Pilkington, Sellers, & Thouvenot, 2007).

On e-commerce matters, the relevant OHADA instrument is the 2010 revised OHADA Uniform Act on General Commercial Law, which became effective in Member States in 2011. At the level of the Union Economique et Monétaire Ouest Africaine (UEMOA, West African Economic and Monetary Union), Regulation No. 15/2002/CM/UEMOA on Payment Systems aims at development of business transactions among UEMOA Member States (UEMOA, 2002). However, while the Regulation does contribute to modernising the UEOMA monetary market, it is silent on online transactions.

The UN Convention on Contracts for the International Sale of Goods (CISG), adopted in 1980, is the fundamental legal instrument regulating the sale of goods at the international level (UNCITRAL, 1980). However, CISG does not refer to electronic commerce. The 1996 UN Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce requires that UNCITRAL Member States ensure that such contracts are legally binding on the parties (UNCITRAL, 1996).

2 OHADA's Member States are Benin, Burkina Faso, Cameroon, Central African Republic, Côte d'Ivoire, Congo, Comoros, Gabon, Guinea, Guinea Bissau, Equatorial Guinea, Mali, Niger, the Democratic Republic of Congo (DRC), Senegal, Chad and Togo.

However, as of late 2017, among the 17 OHADA Member States, only Central African Republic, Congo, and Senegal have ratified the UNCITRAL Model Law's provisions.[3]

On consumer protection matters, OHADA has not produced any legal provisions, leaving development of consumer protection legislation to national OHADA Member State legislators. The Napoleonic Civil Code is the fundamental text of law used to regulate sale of goods and consumer related aspects in the OHADA countries.

The aforementioned 2010 revised OHADA Uniform Act on General Commercial Law includes significant provisions in respect of (1) validity of electronic documents and (2) validity of electronic signatures.

Validity of electronic documents

Under Chapter 2 of the revised Uniform Act, the formalities performed by the Registre du Commerce et du Credit Immobilier (RCCM, Trade and Credit Register) in respect of electronic documents and electronic transmissions, have the same legal effect as those accomplished with documents in paper form, in particular as regards their legal validity and their probative force (Art. 82). Thus, the Act gives the possibility, to the parties in an online transaction, to present documents in electronic form as substitutes for paper-based documents. Documents in electronic form are recognised as equivalent when they are established and maintained by a reliable technical process which at all times guarantees the origin of the document in electronic form and its integrity during electronic processing and electronic transmission. Under the revised Uniform Act, the origin of documents in electronic form and their integrity during electronic processing and electronic transmission must be guaranteed by reliable technical processes. OHADA has, accordingly, established a Technical Committee for the Standardisation of Electronic Procedures.

Validity of electronic signatures

The revised Uniform Act recognises as valid ("qualified") an electronic signature carried via a reliable technical process that guarantees: the origin of documents in electronic form at all times; and the documents' integrity during processing and electronic transmission. Article 83 provides that a valid electronic signature applied to a document is one that makes it possible to identify the signatory and for the signatory to express consent to the obligations arising from the signature.

Further, the Act states that the electronic signature, in order to be valid, must: be linked to only the signatory; allow the signatory to be properly identified; have been

3 See http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html

AJIC 20-21-Jan-18-22h19.indd 174-175 1/21/2018 10:43:24 PM

created by means which the signatory can retain under her/his exclusive control; and be linked to the document to which it relates in such a way that any subsequent modification of the document is detectable. And a valid electronic signature under the Act must: be generated by a signature-creation software and signature-verification software; and include an electronic certificate, authenticating the signatory, that is produced by an electronic certification service provider. The Act does not specify whether the signature-creation software should be two different pieces of software, or two elements of a single piece of software. The Act gives authority to the Technical Committee for the Standardisation of Electronic Procedures to determine the criteria to be fulfilled in order to be an electronic certification service provider.

The Act recognises the right of the parties to the online transaction to use the dispositions of Member States' domestic law to palliate (i.e., moderate) OHADA regulations regarding the technical constraints applied to the components of the electronic signature, so that it is deemed to be qualified (Art. 84). Judgements by the French Supreme Court (Cour de Cassation) provide some African OHADA judges with inspiration when it comes to the recognition of electronic signatures. The validity of use of a secure device for creating electronic signatures has, for example, received judicial blessing in France. In a judgment of 6 April 2016, the French Cour de Cassation confirmed the ruling of the Montpellier District Court in a dispute related to the validity of an electronic signature (Cour de Cassation, 2016). The judge in the case considered that the electronic contract had been established and kept in a manner that guaranteed its integrity, because the signature had been identified by a reliable process guaranteeing the link between the electronic signature and the act to which it was attached.

While the aforementioned provisions of the OHADA Uniform Act constitute encouraging developments for OHADA Member States' consumers in e-commerce transactions, several important matters are not fully addressed in the OHADA instrument and must thus be addressed via national instruments. The Act is silent on necessary details in online business practices such as terms of offer in electronic transactions, and online transaction security. Accordingly, several e-commerce matters have been left up to the Member States' sovereign lawmaking. I now examine what has been done at the national level in Cameroon.

4. Legal provisions in Cameroon

Located on the Gulf of Guinea in West Africa, Cameroon has a population of approximately 20 million people. Due to its varied colonial history, during which the country experienced periods of German, British and French control, Cameroon has a dual – or bijural – legal system, with English common law operating in certain regions (primarily in the west), and French civil law operating in other regions (DocuSign, n.d.). Cameroon's legal instruments relevant to this report are its Law No. 2010/021

of 21 December 2010 governing e-commerce and its Law No. 2011/012 of 06 May 2011 on consumer protection.

Article 10 of the 2010 e-commerce law stipulates that the law regulating the formation of traditional written contracts will apply to electronic contracts in respect of agreement, validity, and enforcement. But, as explained above, transposing traditional notions of commercial law to a purely electronic environment raises certain fundamental issues with respect to formation of contract. Two such issues are: (1) presumption of reception of documents related to an online transaction; and (2) presumption of conclusion of a contract for an online transaction.

Presumption of reception of documents related to an online transaction

In the eyes of the law, at what particular period of time a message sent by a party in the course of an online transaction, is supposed to have taken legal effect? Such understanding is primordial to the successful conclusion of the online agreement by both parties.

Article 12(3) of Cameroon's Law on e-commerce underlines that: "The order, the confirmation of acceptance of the offer and the acknowledgement of receipt are presumed to have been received when the receiving party was able to access the documents". The law does not clarify what is meant by "able to access the documents" in an online environment. Does this refer to the consumer ability to read, or to open, or to click on, or to merely notice the mentioned document on the trader's website? This lack of clarity, which generates uncertainty in the practice of online trade, must be the subject of legal amendments.

Presumption of conclusion of a contract for an online transaction

Article 12 of Cameroon's Law on e-commerce (Law No. 2010/021 of 21 December 2010) stipulates that:

- A contract cannot be concluded unless the offeree was given the opportunity to access and review the details of the offer prior confirming his acceptance. (Art. 12(1))

- Within 5 days, the offeror must acknowledge receipt of the online order sent to him. (Art. 12(2))

However, the above-mentioned conditions of Article 12 do not apply to contracts exclusively concluded through emails, individual communications, or transactions between persons knowledgeable in the field. This implies that offer and acceptance sent through emails do not need further time for review or acknowledge receipt. The email stands as offer or acceptance, with the exception of contracts concluded between professionals (Art. 12(4), Law No. 2010/021 of 21 December 2010). It is

AJIC 20-21-Jan-18-22h19.indd 176-177 1/21/2018 10:43:24 PM

my view that this presumption of conclusion of an electronic contract in an online environment constitutes an abuse of consumers' rights. In the particular context of the computer illiteracy of a large number of Cameroonians, opportunities should be given to online consumers to access and review the terms of the offer, prior to being bound as a matter of law. Enforceability should vary according to the methods of offer or acceptance used (Van Der Merwe et al., 2016).

Given the uncertainties in Cameroon's e-commerce law in respect of online contract formation, it becomes relevant to consider whether Cameroon's 2011 consumer protection law is of assistance.

The consumer protection law

Article 3(c) of Cameroon's consumer protection law (Law No. 2011/012 of 06 May 2011) establishes:

> The principle of information according to which consumers have the access to information to enable them to make an informed choice during any transaction concerning the supply of technology, goods, and services. (Art. 3(c), Law No. 2011/012 of 06 May 2011)

Chapter 3 of the above-mentioned law protects the consumer's economic and technological interests. More specifically, Article 5(2) declares that: "[a] competent court may declare contractual clauses void", when such clauses:

- Exempt, exclude, reduce or limit the liability of suppliers or service providers for defects, deficiencies or shortages of any kind in technology, the good supplied or service rendered;
- Imply the loss of rights and freedoms guaranteed to consumers, or limit the exercise thereof;
- Create unjust, unreasonable, unfair or repressive contractual terms or conditions, or that transfer liability for defects, deficiencies or shortages not immediately obvious to the consumer;
- Impose a unilateral arbitration clause. (Art. 5(1), Law No. 2011/012 of 06 May 2011)

Because the national legislator in Cameroon did not define the standards of "informed choice", it could be difficult to argue that a trader by placing an icon on the website of the online shop linking to the terms and conditions, is liable for practising misinformation for assuming the contract concluded once the consumer has clicked on the icon. It is the author's view that common law principles designed for a "bricks and mortar" world could be adapted in order to be effective in a digital environment. An online provided offer/acceptance should reflect in this sense the essential characteristics of precision and clarity. It should represent a proposal sufficient in terms of legal contracting to enable an informed acceptance by the consumer.

5. Recommendations

A new OHADA instrument

One possible solution to the legal uncertainties outlined above is for OHADA Member States to collaborate in development of an OHADA regional instrument on consumer protection. Such an instrument could alleviate the current uncertainties in the legal provisions of Cameroon (and other OHADA Member States) in respect of online contracts. Moreover, such an instrument could, in addition to legislating on e-commerce matters, legislate on other important consumer matters such as: consumer participation in financial markets, consumer over-indebtedness, consumer contact with defective goods, unfair competition, and access to redress. This OHADA instrument could either take the form of a Uniform Act binding on all OHADA Member States, or a Model Law serving as a standard for Member States.

Strengthened Cameroonian provisions

Another option is for Cameroon to take steps at its sovereign national level to strengthen the protection of consumers in online business transactions. Such steps could be taken via a detailed law specific to online transactions, or via upgrades to the existing e-commerce and consumer protection laws to fill the gap of uncertainty in the digital business environment.

References

Bolton, D. (2009). Shrink-wrap and click-wrap contracts. *Precedent, 95*. Retrieved from http://www.austlii.edu.au/au/journals/PrecedentAULA/2009/97.pdf

Boss, A. E. (2015). Practicing e-legally. The United Nations Convention on the Use of Electronic Communications in International Commerce. In S. Linton, G. Simpson, & W. A. Schabas (Eds.), *For the sake of present and future generations: Essays on international law, crime and justice in honour of Roger S. Clark* (pp. 555-573). Leiden, Netherlands: Brill. https://doi.org/10.1163/9789004270725_035

Cour de Cassation. (2016). Cour de Cassation, Chambre Civile 1. Audience publique du mercredi 6 avril 2016. No. de pourvoi: 15-14631.

Dahiyat, E. A. R. (2011). The legal recognition of electronic signatures in Jordan: Some remarks on the Electronic Transactions Law. *Arab Law Quarterly, 25*(3), 297-309. https://doi.org/10.1163/157302511x568538

Davis v. HSBC Bank Nevada, N.A., 691 F.3d 1152, 1162 (9th Cir. 2012).

DocuSign. (n.d.). eSignature legality in Cameroon. Retrieved from https://www.docusign.com/how-it-works/legality/global/cameroon

Erasmus, C. (2011). *Consumer protection in international electronic contracts.* Master of Laws dissertation, Northwest University, Potchefstroom, South Africa. Retrieved from http://dspace.nwu.ac.za/bitstream/handle/10394/6917/Erasmus_C.pdf?sequence=2

Estrella-Faria, J.-A. (2009). Legal aspects of electronic commerce: Rules of evidence, contract formation and online performance. In Xiamen Academy of International Law (Ed.), *Collected courses of the Xiamen Academy of International Law, vol. 2*. Leiden, Netherlands: Brill. https://doi.org/10.1163/ej.9789004180932.i-474.21

AJIC 20-21-Jan-18-22h19.indd 178-179 1/21/2018 10:43:24 PM

Jerez v. JD Closeouts, LLC, 943 N.Y.S.2d 392, 394 (Dist. Ct. 2012).
LawTeacher. (n.d.). Electronic contracts. Retrieved from https://www.lawteacher.net/free-law-essays/contract-law/electronic-contracts.php
Lloyd, I. J. (2014). *Information technology law* (7th ed.) New York: Oxford University Press.
Martor, B., Pilkington, N., Sellers, D. S., & Thouvenot, S. (2007). *Business law in Africa: OHADA and the harmonisation process* (2nd ed.). Retrieved from https://www.bookdepository.com/OHADA-Harmonization-Process-Boris-Martor/9781846730726
Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA). (2010). Uniform Act on General Commercial Law [revised]. OHADA Official Gazette Special Issue of 15 February 2011.
Pistorius, T. (2004). Click-wrap and web-wrap agreements. *South African Mercantile Law Journal, 16*(4), 568-576. http://hdl.handle.net/10520/EJC54132
Republic of Cameroon. (2010). Law No. 2010/021 of 21 December 2010 governing e-commerce.
Republic of Cameroon. (2011). Law No. 2011/012 of 06 May 2011 on consumer protection.
Snail, S. (2008). Electronic contracts in South Africa – a comparative analysis. *Journal of Information, Law and Technology, 2*. Retrieved from https://warwick.ac.uk/fac/soc/law/elj/jilt/2008_2/snail
UN Commission on International Trade Law (UNCITRAL). (1980). United Nations Convention on Contracts for the International Sale of Goods (CISG). Vienna. Retrieved from https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf
UNCITRAL. (1996). UNCITRAL Model Law on Electronic Commerce. Vienna. Retrieved from http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
Union Economique et Monétaire Ouest Africaine (UEMOA). (2002). Regulation No. 15/2002/CM/UEMOA relatif aux systemes de paiement dans les etats membres de l'union economique et monetaire ouest africaine (UEMOA). Retrieved from http://www.bu.edu/bucflp-fig/files/2012/01/Regulation-No.152002CMUEMOA-on-Payment-Systems-in-the-Member-States-of-WAEMU.pdf
Van Der Merwe, D., Roos, A., Nel, W., Eiselen, S., & Nel, S. (2016). *Information and communications technology law*. Durban: LexisNexis South Africa.

AJIC 20-21-Jan-18-22h19.indd 180-181 1/21/2018 10:43:24 PM

AJIC 20-21-Jan-18-22h19.indd 182-183 1/21/2018 10:43:24 PM

THE AFRICAN JOURNAL OF INFORMATION AND COMMUNICATION (AJIC)

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

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

AJIC 20-21-Jan-18-22h19.indd 184 1/21/2018 10:43:25 PM