Good Governance Perspectives in Public Administration and Cybersecurity

M Subban
School of Management, Information Technology and Governance
University of KwaZulu-Natal

V Jarbandhan
School of Public Management, Governance and Public Policy
University of Johannesburg

ABSTRACT

The governance of cybersecurity has come into sharp focus in recent times. The proliferation of events from the alleged cyberinterference in elections to the breaching of sensitive information, for example, health and personal records of users globally; has become an area of concern. South Africa has not been insulated from these attacks, with the City of Johannesburg being a case in point. The frequency of these cyberbreaches points to the seriousness of the governance challenges facing the techno-economy. Government intervention around cybersecurity is pluralistic in nature as it focuses on areas such as sovereignty, terrestrial space and democratic governance. This article attempts to critically examine technology-led public administration and information governance to ensure open, transparent, efficient and effective service delivery. It is important to grasp what constitutes good governance in cybersecurity. Moreover, it is important to advance and regulate the cyberspace for responsible and sustainable practice. This article utilises a meta-synthesis and draws on contemporary literature to explore the current knowledge, views, trends and approaches in acting pre-emptively to promote good governance in cybersecurity. The aim of this article is to propose a framework that South Africa could follow in implementing a cybersecurity policy. One of the main findings of this article is the clarion call for increased accountability and transparency, together with new forms of resilience. As a value-add, the article explores cybersecurity regulation as an important aspect of good cybergovernance amidst the onslaught of the Fourth Industrial Revolution. The practical implication is that by introducing cybercentric measures in e-governance, a more reflective approach could bring about positive changes and measures in how information is managed, disseminated and governed while improving service delivery in the 21st century and beyond.

INTRODUCTION

Technology-driven societies require, *inter alia*, universal access to the internet, increased e-governance and digital government services. While governments strive to provide these services through e-platforms and to increase connectivity to foster economic growth, education and improve public participation through social media platforms, the threat posed through breaching these platforms remains real. Threats from foreign powers, cybercriminals and cyberterrorists remain a real challenge. While cyberspace is the domain of communication in 'real time', the governance of cybercentric citizens and cybersecurity has come into sharp focus in recent times. There is a growing proliferation of events such as cyberinterference and hacking into sensitive e-mail accounts, which points to the seriousness of the challenge facing cybercitizens and the public at large. A perusal of the current literature relating to cybersecurity in South Africa has started to gain momentum in recent years as an evolving aspect of information security and governance. However, internationally the topic has gained traction due to the numerous cyberattacks that have been launched against advanced information societies, thereby threatening both the public and private sector information systems.

The South African government's intervention around cybersecurity is pluralistic in nature, emerging in its focus on areas such as sovereignty, terrestrial space and democratic governance. Sovereignty, as is contextually understood within the physical domain is easy to police; however, in cyberspace sovereignty as it is traditionally understood, becomes a blurred concept. Strong democratic governance is important to protect the rights of cyber- citizens that could otherwise be trampled upon in the cyberinformation arena. It can be said that, control systems are increasing in complexity making them more difficult to secure (Wyman 2017:16).

Given the above background this article seeks to address the following practical questions to gain a greater insight into the governance issues related to cybersecurity.

- What constitutes good governance in cybersecurity?
- What is the role of government in relation to cybersecurity and governance?
- How can cybercitizens be protected?
- What is the future of public administration amidst the prevalence of cybersecurity?

The article has the potential to contribute to our understanding of the bigger discussion around cybersecurity, and calls for more deliberate and strategic action from public sector leaders, public institutions and the citizenry at large as all key stakeholders embrace the Fourth Industrial Revolution (4IR) (Van der Steen, Van Twist and Bressers 2018:389).

The article commences with a discussion of cybersecurity in the South African context. Conceptual definitions are put forward regarding governance. Some key dimensions to addressing good governance *vis-à-vis* cybersecurity are explored. Information is a strategic resource and the need for integration of information is emphasised in the subsequent discussion. This is followed by a discussion of e-governance and cybersecurity. Next, the relationship between Public Administration, New Public Management and cybersecurity is described. A discussion of cyber-enabled governance and Public Administration follows. The 4IR contextualises the discussion with Public Administration in the latter part of the article. The 'new age' of cyberresilience in Public Administration is explored thereafter. Data protection and security information management precedes the recommendations put forward which includes a cybersecurity awareness toolkit and a cyberterrorism life-cycle model. The future of public administration in the cyberage is explored, followed by concluding remarks.

Relational aspects of cybersecurity, cybercitizens and governance

Below is a discussion of cyber-related concepts as it relates to governance.

Cybersecurity

Cyberattacks are regarded as one of the top global security risks of the highest concern over the next decade (World Economic Forum Global Risks Report 2019). Although government and the corporate sector are engaging in promoting effective cybersecurity measures and strategies, the budget spend on cybersecurity continues to escalate given the alarming rate of invasions and breaches. A three-pronged approach to addressing cybersecurity is advocated by the World Economic Forum as: Prevent, Detect, and Respond. Cybersecurity typologies significantly include a platform of resilience, cooperation and transparency towards cyber-stability (World Economic Forum Global Risks Report 2019).

Cybercitizens

Citizenship is a birthright. Equal participation in democratic processes is based on individual rights, which are founded on the constitution or other legal enactments. In theory, at any rate, no distinctions, in this respect, can be countenanced. By contrast, the cash nexus governs a customer's access and relation to the market. The measure of worth depends on purchasing power. While both buyers and sellers may select one another accordingly, by contrast a citizen's access to services provided by the government is based on rights and needs. A democratic state is clearly not at liberty to favour or discriminate. It would be fair to argue, accordingly, that whatever its other merits, the market paradigm has serious limitations when it comes to public management in democratic societies (Argyriades 2003:526).

Governance

The term 'governance' has become a more or less neutral concept focusing on steering mechanisms in a certain political unit that could place emphasis on the interaction of the state, as an example. It can be said, that the concept of governance is used as a normative one in public administration discourse, often contextualised in various public institutional environments. It embodies a strong value judgement in favour of the state or government (Drechsler in de Graaf and Asperen 2016:406).

The concept of governance has four important dimensions which include: public sector management, accountability, legal framework for development, information and transparency meant for development (The World Bank 1989 in Kaur and Sitlhou 2017:252). Important features of good governance are ensuring accountability, establishing credibility of institutions and providing effective, efficient and responsive administration. "Good governance depends on administrative patterns, political will, citizens' awareness and participation. It follows then, that an effective and efficient governance pattern is the primary objective and foundational value of public administration" (The World Bank 1989 in Kaur and Sitlhou 2017:252).

The concept of good governance

From the early 1990s, the discourse on 'good governance' has become more prevalent (Bevir 2009 in De Graaf and Asperen 2016:406). What 'good governance' means can be contextualised in various aspects of public service delivery and public administration. The concept is used in many different ways, but most scholars agree that it was the World Bank in 1989 that introduced the concept into modern-day discourse that focuses on the promotion of economic development as a case in point. The purpose of good governance in the article, however, is the promotion of what can be called public service motivation, which is often equated with a desire to serve the public interest, or more generally with altruism (Dur and Zoutenbier

2014:145 in De Graaf and Asperen 2016: 417). Democratic governance is about the protection of the rights of citizens. Right to information is a tool in the hands of the citizens. They seek information from various government functions, processes and persons responsible to carry out specific tasks (Kaur and Sithlou 2017:259). The manner in which information is communicated, managed and protected is a vital aspect of good governance perspectives in public administration.

Definitions of good governance constantly shift, changing in response to and along with trends and circumstances. A review of public administration literature reveals four distinct governance perspectives that each highlights unique values: "Old" Public Administration, "New" Public Management, Network Governance, and Societal Self-organisation. These perspectives guide public sector leaders' perception of government's role in society and of its role more specifically as a civil servant. It influences the perception of politicians' responsibilities, and the value, place, and interplay of citizens with government (Bozeman 2007; Mosher 1982 in Van der Steen *et al.* 2018:388). Public sector leaders and public administrators play a significant role in the governance of information.

Within the traditional public administration perspective of governance, public goals are determined in political processes and policies are formulated for translating political decision into concrete actions. Public sector leaders subsequently execute and perform these policies in practice towards achieving defined goals. The bureaucracy ensures the standardisation of response by government. Public interest and objectivity are important values, as well as equality and equity (Hartley 2005; Kaufman 1967; Van Eijck 2011; Wilson 1989 in Van der Steen *et al* 2018: 91).

The second perspective of governance, which focused on efficiency and effectiveness of delivery output, was that of New Public Management (NPM) as discussed by authors such as Ferlie, Lynn and Pollit (2007). NPM represented a turn in the debate about governance, lamenting what is seen as widespread "waste" in traditional governmental bureaucracy. Legalistic values still matter, but are instrumental for achieving results (Osborne & Gaebler 1992). As NPM grew in prominence, many private-sector management techniques and instruments were introduced into public organisations, such as performance targets, deregulation, efficiency, contract management, and financial control. These are then translated into values for civil servants: a focus on measurable "SMART" results, and efficient and effective execution of policies (Eijck 2014; Pollitt & Bouckaert 2004 in Van der Steen *et al.* 2018:391).

The subsequent perspective is that of Networked Governance which focuses on the collaboration of government organisations and societal actors and reflects the displacement of government as the central actor (Ansell & Gash 2007). This is often related to the move from government to governance, and the "solving of wicked problems" (Christensen & Lægreid 2007) that typically require cross-institutional action. That is why civil servants have to operate in networks. This inherently involves interaction, finding mutually acceptable definitions of the problem and looking for joint solutions. As a result, other actors become guiding factors in the process. In this perspective, a "good civil servant" is a networker who builds relations with other social actors to create and execute policies that are co-produced with others (Alford 2009; Dentchev & Heene 2004; Hartley 2005; Klijn & Koppenjan 2000; Pestoff 2006; Stoker 2006 in Van der Steen *et al.* 2018:391–2).

Lastly, the governance perspective of "societal self-organisation" has gained increased academic and practical attention (Bekkers 2007; Bourgon 2011, 2009; Van der Steen *et al.* 2016). This perspective centres the production of public value on a self-reliant citizenry. Societal actors produce public value for their own reasons, and are guided by their own preferences and priorities (Bourgon 2011 in Van der Steen *et al.* 2015). Citizens can undertake this independently, as well as through self-organised networks and cooperatives. It is important to note that this is still acknowledged as a role for government, but that it is a departure from other models in that societal actors are primarily responsible for producing value via a bottom-up relationship (Bovaird 2007; Pestoff 2009; Sørensen & Torfing 2016). This type of value production happens within the bounds of government responsibility, as self-organising citizens still have to follow the law and act according to norms and standards (Sørensen & Torfing 2016). Self-reliance is not an equivalent of a "laissez-faire" approach to government. The key point of this perspective is that the dynamics that produce public value start within society and that government relates to that; for example, do nothing, let go, block, facilitate, attempt to "organise" more self-organisation (Bekkers 2007; Boons 2008; Boonstra & Boelens 2011; Portugali 2000; Stoker 2006 in Van der Steen *et al.* 2018:392).

The four governance perspectives, as alluded to, in the preceding discussion, emphasise different answers to questions of what defines good governance and what it means to be a good public leader. They are significant to help address the type of role, purpose and function of a public leader when dealing with the onslaught of cybersecurity issues and the impact on citizens and society.

It follows then, that good governance is an ideal which may seem difficult to achieve in its totality. However, to ensure sustainable human development and enhance the quality of life of citizens, action must be taken to work towards this imperative. The right to information is one of the methods by which success may be achieved towards good governance. Right to information is a basic requisite of good governance and the key to strengthening participatory democracy and ushering in people-centred governance. It also increases the level of transparency and accountability in the administrative and management machinery of government and is a powerful mechanism to both citizens and the public sector. Being cognisant of cyber-security in managing information is therefore, fundamental to good governance.

Given that access to information can empower the poor and the weaker sections of society to demand and obtain information about public policies and actions, leading to their welfare, it requires people-centred governance which is conscious of cyber issues. "Without good governance, no amount of developmental schemes can improve the quality of life of the citizens. Good governance constitutes four important elements: transparency, accountability, predictability and participation. The more citizens are able to access government functions, the greater the responsiveness of the government system to the communities' needs" (Shamshad 2009:576).

Information integration and good governance

Managing information integration and governance thereof is of strategic importance because if you harness information effectively, it can present new opportunities on various levels and improve decision-making for the sustainable future. Government, the public sphere and citizens are in need of information as a strategic resource which makes information governance a necessity. Maximising the value of information while ensuring compliance with regulatory obligations, managing risks and protecting security; are desired outcomes for good governance. Sound information integration and governance therefore provides five important capabilities necessary for good governance, as highlighted by Hulme (2012:103). These are:

- Delivery of trusted information for greater insights and improved decision-making regarding service delivery agenda;
- Elimination of wastage of expensive resources associated with the cost of managing automated information;
- Protection of information through cost-effective technology platforms;
- Aligning of public institutions' key strategies through provision of timely information linked to government's broader vision; and
- Ensuring fulfilment of fiduciary responsibilities, legal and other mandates (Hulme 2012:103).

The above aspects would in effect, ensure that information is protected and secured. The authors are of the view that the above discussion emphasises the 'new' dimension of public administration practices in the context of good governance imperatives relating to information management.

eGovernance and cybersecurity

eGovernance concerns the use of information and communication technologies such as the Internet, Wide Area Networks, mobile phones and other forms of engagement in order to deliver services to citizens, businesses, and government. A further definition is that of the transformation of the public sector's internal and external relationship through "enabled operations, information technology and forms of communication to optimise government's quest for service delivery while invoking participation and governance" (Sangita and Dash 2008:141). eGovernance then refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and Mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a "variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information or more efficient government management and governance. The benefits can be less corruption, increased transparency, greater convenience, revenue growth and cost reductions" (Malick and Murthy 2001:238). The authors further concede that new means of involving citizens through wider access, knowledge about available systems and services, communication channels and the degree of involvement including information security are considered the greatest challenges facing the administration, technology providers and the citizenry in the cyberage. By introducing cybercentric measures in e-governance, a more reflective approach could bring about positive changes and measures in how information is managed and governed while improving service delivery in the 21st century.

Relationship between Public Administration, New Public Management and Cybersecurity

In the 21st century and beyond, the prerequisites of good governance are operationalised with rapid automation and technology. In order to achieve the ideals of NPM, technology upgrades, incorporating modem techniques of management to ensure effectiveness and efficiency, capacity building of public institutions (including training of public sector leaders and officials), with transparency and openness are deemed essential aspects of good governance (Minocha 1998:280).

Since e-governance has been heralded as a transformational improvement in the quality, efficiency and effectiveness of governance, it stands to reason that a governance strategy driven by information and communication must be developed and applied to give effect to openness, transparency and accountability as normative guidelines of the Constitution of the Republic of South Africa, 1996 (*Constitution of the Republic of South Africa* 1996). It can therefore be said, that e-governance is a distinct dimension of NPM that has gained considerable prominence since the 1990s. Ongoing demands generated by political leadership, growing capacity building needs and perceived citizens' needs have contributed tremendously to the need for information technology innovation and governance.

It follows then, that the relationship between public administration and cybersecurity could be one of the most effective channels for protecting, accessing and dissemination of information and provide a customer-centric public service (Sapru and Sapru 2014:313–316). Malick and Murthy (2001:237) hold the view that unprecedented developments in information and communication technologies have opened new avenues for governance, thus introducing a new agenda, concepts and methodologies in the provision of information and services. Therefore, implementation by public institutions and public sector leaders requires more efficient government management of public service delivery. Minocha (1998:279) posits that the greater use of information technology and management techniques in revamping office-oriented systems with improved record-keeping, movement of files, space utilisation and adoption of other available automation has changed how public administration takes place in public institutions. Public offices have become more effective and efficient through the system of computerised information systems and innovative technologies. Reduction of excessive paperwork and the abolishment of unwarranted reports and returns have informed current terms of communication. Simplification and integration of office procedures, standardisation of job outputs and introduction of appraisals by technology-driven results helps boost efficiency levels. In other words, with the reliance on technology in recent years, public administration and service delivery have been affected by a new wave of security and information breaches that have resulted in a paradigm shift from the traditional citizenship-based model of public services, to a cybercentric citizens' approach (Brewer 2007: 550). How cybersecurity can be regulated through a multisector approach is an important aspect of cybergovernance in protecting the rights of cybercitizens. A key challenge for public administrators though, is to ensure that good governance and accountability principles are incorporated into citizenship-oriented systems.

The relationship between public administration and cybersecurity leads to the focus of cyber-enabled governance in the subsequent discussion.

Cyber-enabled governance and public administration

With the current information revolution, citizens must be empowered to assimilate information and make value-added decisions concerning service delivery matters that affect them. In the same light, public sector leaders and officials must be able to deliver on their given mandate. Malik and Murthy (2000:239) consider that good governance in public administration means provision of quality services to the citizens and stakeholders with diverse interests, administrative independence and managerial autonomy. Moreover, Kapur (2000:388) states that, an opportunity exists to craft a new vision for governance, obliterate outdated systems that have now turned into anachronisms in the new global scenario, and make innovation the 'life infusing force' in revitalising public sector organisations as a necessity in the information and cybersecurity age. With digital convergence, cyber-enabled governance entails developing awareness, creating access, generating feedback, sharing knowledge and implementing cybersecurity measures and cyberlaws as good governance perspectives in public administration (adopted from Rogers Okot Uma in Malik and Murthy 2000:241).

Another dimension of cyber-enabled governance in public administration is that of cyber- organising and cyberorganisations. In the context of public administration, social capital is the combination of resources where citizens engage with one another and with government in relation to service delivery matters. Through cybermeans, citizens are able to define their connection with organisations and themselves in a speedy manner. The form of social exchange poses important challenges, opportunities and questions for public administration, and what implications the role of cyberorganisations hold for the public administrator in a context dominated by technology (Brainard 2003:384). Communication via information is ostensibly devoid of face-to-face human interaction. Often people may not be looking for information in the form of data. Putnam (2000 in Brainard 2003:399) argues that organisational ties are eroding and that government should assume partial responsibility for revitalising them so that civic engagement and forms of social capital are not compromised in the cyberage. This discussion relates to both the social and political environment in which public administration takes place, and is explored further in the cybertoolkit under the recommendations put forward by the authors to this article.

Contextualising the 4IR and public administration

Nundkumar and Subban (2018:324) hold the view that the 4IR technologies create new forms of engagement. Caruso (2018 in Nundkumar and Subban 2018:324) further states that digitised information has become a strategic resource with the arrival of the 4IR, and is evolving at an exponential rate rather than a linear pace.

The 4IR has brought with it a range of technological advances and government is called upon to improve accountability and transparency, especially in the context of the public sector. In order to respond to the service delivery agenda with increased transparency and trust, government needs assistance. The rapid advances in technology relating to the 4IR could assist government (Van Heerden, Steenkamp and Van Heerden 2018:913–4). However, government has to deliver services smartly. Given the complexities of technology, the 4IR could assist government to effect improvements in service delivery (Van Heerden *et al.* 2018:923).

Developed and developing countries according to Shava and Hofisi (2017:204), are seemingly embracing the innovative technologies of the 4IR.

Trends in the 4IR can facilitate change in public administration, but they could also disrupt the engagement of citizens with public organisations thus compromising service delivery. According to Jarbandhan (2017:61) "the pressing question for policy-makers in the 4IR would be balancing state interventions to fulfil social needs without undermining the dynamism of the market system in times of rapidly developing technology".

The 4IR offers much to society from cheaper access to services to the dispersion of information at a rapid rate. It has also allowed for interconnectivity of devices and the cost-effective rendering of goods and services. However, the levels of interconnectivity allow for cybercriminals and syndicates to breach built-in security, and on occasion to misuse data or to even hold large organisations, individuals and governments to ransom. Consequently, it is important for governments to invest in securing their networks from cybercriminals. Investing in the design of state-of-the-art security systems is of paramount importance, so is the sharing of information on cyberthreats towards protecting information platforms. Data shows that cyber-attacks will continue to increase as technology rapidly becomes outdated in the 4IR; hence, striving to make cybercentric citizens more situationally aware of the information environment. Taking cognisance of the 4IR and ensuring a cybercentric approach both for citizens' protection and that of cybergovernance in leadership are fundamental prerequisites for good governance. The prospect of several systems competing for cybersecurity currently, indicates that it was possibly because cybertechnology remains one of the few areas attracting new government expenditure (Herrington and Aldrich 2013:301).

The South African government has recently emphasised the 4IR and its impact on public administration practices in the public sphere. Information technology implementation, management and governance are key aspects for due consideration to not impede sustainable service delivery. With the onslaught of the 4IR and growing awareness of cybersecurity, government must initiate the necessary legal and administrative steps to encourage and provide citizens with efficient, responsive and accountable public governance through information technology-enabled systems. The provision and protection of information of cybercitizens against any form of attack is ostensibly a constitutional imperative and right of citizens. A challenge faced by modern public administration, is that while technology has the potential – in keeping with government's current focus on digital access into the deep and semi-rural areas – for hands-on participation, it is equally important that technology-led public administration initiatives (Rattan and Rattan 2008:889) are effectively put in place to address the improvement, governance and protection of information. The information technology revolution would effectively require good governance strategies for public administration delivery systems amidst the 4IR.

With the 4IR, comes a rapid spate of technologies. With the rise in technology fusion, there is the need for security measures. A new approach is required to regulate the space. Of concern, is that space could play a persuasive and dominant role and there are growing concerns that the current mechanisms to regulate activities are no longer fit for purpose. In the global revolution and cyberwar, attack is easier than defence (Eide and Kaspersen 2015).

Shava and Hofisi (2017:205–6) state that the opportunities, challenges and effects of the 4IR on the functioning of public administration includes disruption of societal values and restructuring of the economy; and digitalisation and changing of the world order. Finally, the role of the state in a technology-driven environment must take cognisance of the following:

- The desire for public institutions to balance the power of technology and business with rules, codes and standards for safety, inclusion and respect for humanity.
- The ability of the state to adapt to technological advances.
- The realisation that the state is not static.
- The maintenance of public trust and safety when devolving new technology.
- Using technology ethically, especially in a cyberworld.
- It is important for the state to preserve the public interest, by adopting agile leadership and embracing the advantages of the 4IR (World Economic Forum in Jarbandhan 2017:64).

Linking the 'new age' of cyber-resilience in public administration

If one of the main focus areas of public administration is among others, the general welfare of the citizens, it stands to reason that the necessary measures should be put in place by government to ensure that it places the citizen at the forefront of its service delivery agenda. The modern repertoire is that, government, the private sector and citizens must work together to provide a cyberdefence that is less about barriers and more about resilience (Feakin 2011 in Herrington *et al.* 2013:303). The authors further maintain that, in the electronic age, security, risk and resilience have been cross-bred and present new challenges for cyber-governance. Over the next two decades, the main driver of information and communication technology will be an even closer connectivity of the Web and the individuals known as cybercitizens. When 'digital tsunamis' occur, citizens will invariably hold government to account for the failure of infrastructure which it no longer may be able to control, yet various sectors of government do not fully comprehend the magnitude of this calamity on service delivery. This interface therefore, requires the protection of infrastructure which is fundamental for good service delivery, and calls for resilience of stakeholders in public administration practices. The author warns that the most alarming aspect of cyber-resilience is that it is a moving target to be factored in government's strategic plans. It is common knowledge that government projects and programmes have failed in the past not only because they were 'big-bang' solutions with poor capacity to embrace emerging technology, but also because the private sector moved at a faster pace than the public sector. The world of information and communication technology is accelerating at a rapid pace and the issues that confront government are growing in size and complexity. Therefore, government has to re-engineer its mindset in order to ensure that it is prepared to address the pace of the information revolution (Herrington *et al.* 2013:300–303). The World Economic Forum Report, (2019) states that strong cybersecurity has become fundamental to a resilient business.

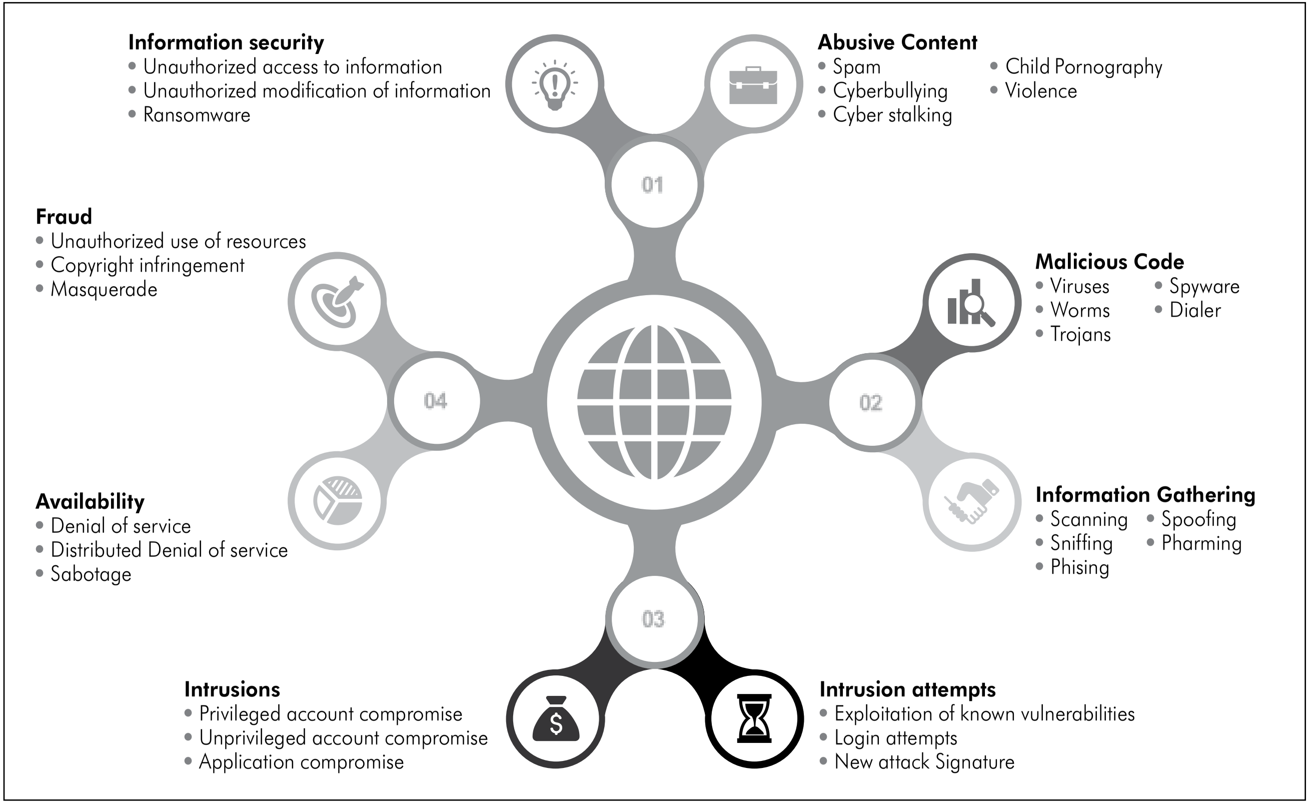
Data protection and security information management

Data and information protection, authentication and privacy issues including citizen (consumer) protection is a prerequisite for the information society and for building confidence in the management and governance of information. A culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all relevant stakeholders. Given the immediacy of cybersecurity issues, "it is important to enhance security measures and ensure protection of data and privacy is upheld. In the context of public administration, one must take into account social and economic development-oriented aspects of the information society" (Gazette, World summit on Information Society 2004:296).

The compilation and analysis of data protection and information governance is no easy task. In promoting new forms of citizen involvement, government can promote citizen co-creation in the arena of cybersecurity. In so doing, cybercitizens are protected and government will find that people would want to be part of the solution, especially for problems that directly affect them (Sapru and Sapru 2014:328–329). Rattan and Rattan (2008:901) list aspects of cyberstalking, cyberharassment, cyberterrorism, cyberdefamation, misuse of online transactions, misappropriation of information, information invasion and privacy issues as some of the serious violations that warrant the need for installing robust cybersecurity awareness for the protection of cybercitizens and creating a platform for technology-based good governance principles and practice in sustaining service delivery. Rattan and Rattan (2008:902) state categorically that, the liability of internet service providers must be strictly monitored regarding the service that is provided by them.

Figure 1 captures the related cybersecurity threats that South Africa potentially faces. They include information security breaches, abusive content, fraud, malicious coding, illegal information gathering, intrusions, etc.

Figure 1: Cybersecurity-related threats in South Africa



Source: (Department of Telecommunications and Postal Services 2017)

RECOMMENDATIONS

Some recommendations are put forward to address cybersecurity amidst good governance.

Effective cybersecurity governance should be underscored by a risk-based approach, according to Nundkumar and Subban (2018:324).

Authors Phahlamohlaka, Jansen van Vuuren and Coetzee, (2011:7) suggest the following recommendations in creating an awareness of cybersecurity:

- National public awareness and education campaign to promote cybersecurity;
- National strategy that touches all sectors and encourages widespread buy-in;
- Framework for research and development strategies on cybersecurity;
- Strategy to expand and train the workforce, including attracting and retaining updated cybersecurity measures;
- Expertise in government among public sector leaders and officials;
- Process between government and the private sector to assist in preventing, detecting and responding to cyberincidents;
- Mechanisms for cybersecurity-related information sharing that address concerns about privacy matters; and
- A Cybersecurity Awareness Toolkit (CyberSAT).

The Table presented in the discussion that follows highlights determinants of power elements associated with cybersecurity awareness. While the toolkit is based on policy elements from the South African environment and can be related to power issues, the kit could be easily adopted for cybersecurity awareness, suggests Phahlamohlaka *et al.* (2011:7).

Ramlackan, Subban and McArthur (2016:64) suggest that given the instantaneous nature of information, and that information is an essential part of any organisation, the confidentiality in information security is undisputed, making the CyberSat an essential platform for addressing cybersecurity threats and vulnerabilities.

Cyberterrorism

Laraque (2016 in Shava and Hofisi 2017:211) notes that, "although new technologies appear to have been embraced by governments globally, as agents for social and economic change they have paved the way to global terrorism and cyberattacks". The authors further hold the view that, these effects of cyberattacks as raised in the article pose serious threats to the functioning of public administrations as governments are incurring huge costs in counter-terrorism security measures to ensure the safety of their citizens.

A proposed generic model to address terrorism in this context is that of a cyberterrorism life-cycle model. In addressing some of the critical aspects of

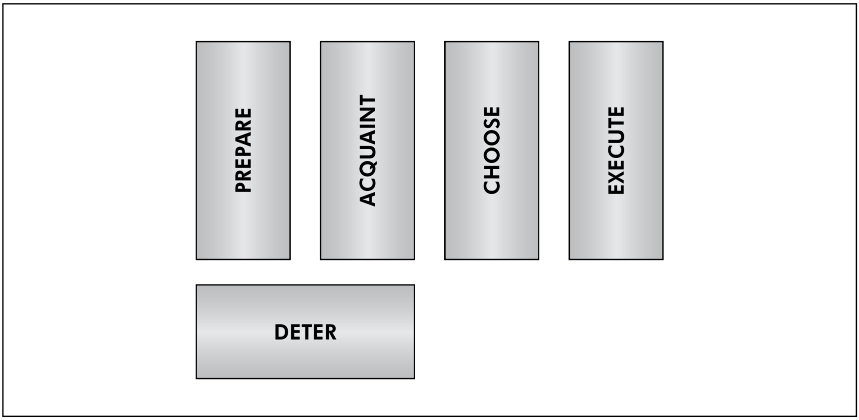
Table 1: The CyberSecurity Awareness Toolkit (CyberSAT)

Philosophical position		Determinants				
Policy elements		Economic	Political	Military	Social	Information
Structures in support of cybersecurity	Cybersecurity breaches will happen regardless of structures established	Establish commercial and financial response structures	Establish a national security level institutional arrangement on cybersecurity	Establish military security	Build confidence in response and capacity of established institutions	Let the public trust in security of communication management and systems
Reduction of cybersecurity threats and vulnerabilities	Threats and vulnerabilities exist but reduction thereof is key goal of good governance practice	Develop various economic breaches monitoring tools and techniques	Send regular political signals that cyber security is a priority	Develop monitoring tools and techniques on ongoing basis	Effectively communicate benefits of paying attention to threats and vulnerabilities	Effectively communicate cyber security as priority
Cooperation and coordination between government and private sector	Partnerships and cooperation across all sectors and society are critical	Build confidence that continued ICT use is competitive advantage than liability	Build public confidence that political leadership will take care of personal information	Create reasonable civil-military interactions within broader government framework	Clear lines of accountability and expected behaviours to contribute trust and confidence building	Build confidence in the public that political leadership will take care of personal information protection

Philosophical position		Determinants				
Policy elements		Economic	Political	Military	Social	Information
International cooperation on cybersecurity	No country can do it alone	International partnerships and shared global spaces are necessary tools	Leaders need to develop relationships that extend across borders	Define standards of conduct in cyberspace	Establish reasonable precautions in relation to balancing secrecy and information sharing are necessary	Promote information sharing
Capacity building and culture of cybersecurity	Focus internally and on basics. Insider threats are more than external threats	Focus on public education and awareness	Behaviour of individual users is the single most important part of cybersecurity battle	Behaviour of individual users is the single most important part of cybersecurity battle	Behaviour of individual users is the single most important part of cybersecurity battle	Focus on public education and awareness
Compliance with technical and operational cybersecurity standards	Actively Participate in creation of international standards	Define standards of conduct in cyberspace	Articulate coordinated national information and communications infrastructure objectives	Define standards of conduct in cyberspace	Define standards of conduct and governance of cyberspace	Articulate coordinated national information and communications infrastructure objectives

Source: (Adapted from Phahlamohlaka et al. 2011:8)

Figure 2: CyberTerrorism Life-Cycle Model



Source: (Veerasamy *et al.* 2012:2)

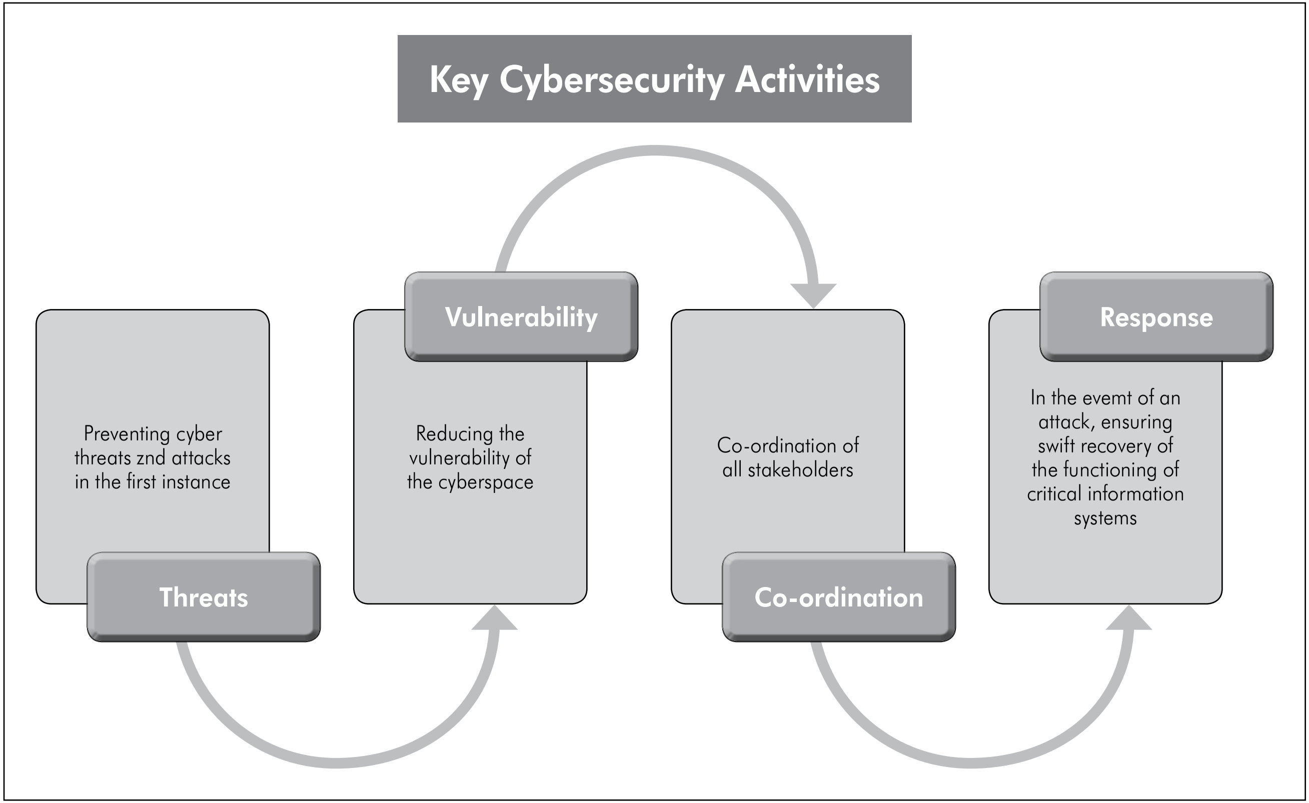
cyberterrorism, five important steps must be considered in cybergovernance. These are Prepare, Acquaint, Choose, Execute and Deter (Ericksson and Penker in Veerasamy, Grobler and Von Solms 2012:2) in order to address and combat attacks online, as is outlined in Figure 2 that illustrates the CyberTerrorism Life-Cycle Model.

The authors submit that cyberterrorism (overt) has emerged as a new threat in information technology and information governance as opposed to cybercrimes (covert), and can be termed a convergence of terrorism and cyberspace. The model allows for the identification of future areas of research and development regarding emerging methods of attack and deterrence (Veerasamy *et al.* 2012:2).

THE FUTURE OF PUBLIC ADMINISTRATION IN THE CYBERAGE

One of the considered and greatest challenges facing new forms of information technologies is the notion of privacy. The right to privacy of individuals is a significant Constitutional imperative of Chapter 2 of the Bill of Rights of the *Constitution of the Republic of South Africa*, 1996. Despite that, tracking and sharing of information is a crucial part of the new connectivity in the cyberage (Schwab 2016). Giving credence to good governance perspectives, the future of public administration in the cyberage poses interesting – yet challenging aspects for public organisations, government and citizens in their engagement with one another. In order to revitalise their role in governance matters, public administrators must reimagine themselves from being agents of regulation and control to becoming agents of

Figure 3: Government's role in cybersecurity


Key Cybersecurity Activities
Threats
Preventing cyber threats znd attacks in the first instance
Vulnerability
Reducing the vulnerability of the cyberspace
Co-ordination
Co-ordination of all stakeholders
Response
In the evemt of an attack, ensuring swift recovery of the functioning of critical information systems

Source: (Department of Telecommunications and Postal Services 2017) the social bond (Vigoda & Golembiewski 2001 in Brainard 2003:401). In other words, public administrators must learn to be co-facilitators of social capital, and participate in the shared reality with citizens through cyberorganising so that they are able to effectively fulfil their roles and responsibilities in various institutional settings. Another perspective for the future of public administration practice is that the current systems of cybergovernance and cyber-resilience warrants collective human accountability because in the future state of public administration, the state demands increased transparency from the citizens. However, the state is also required to significantly increase its accountability and transparency to the citizens (Herrington and Aldrich 2013:308). Figure 3 captures the role of government in cybersecurity.

It is clearly evident that government will have to invest in creating and 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 in Sutherland 2017:1–3). These activities range from identifying cyberthreats, reducing vulnerabilities within cyberspace, coordinating with all stakeholders and responding to the threats effectively and efficiently.

CONCLUSION

In theorising and deconstructing cybersecurity and cybergovernance as key elements, the quest for enhancing service delivery and the future of public administration must be considered. In an era of growing interdependence and collaborative engagement, information management in a technology-driven world is for effective decision-making, strategic management and service delivery. Equally important, is shaping the mindset of government and cybercitizens alike in embracing the evolving cyberenvironment. Sovereignty, as is contextually understood within the physical domain is easy to police; however, in cyberspace, sovereignty as it is traditionally understood becomes a blurred concept. Knowledge, competence and commitment are vital aspects that could inform new approaches and nuances, giving credence to cybercrisis or risk management and the governance of cybersecurity systems becoming a fundamental imperative in the information revolution era. The formidable question is: who controls and directs the governance of information in the current decade and beyond? Finally, the authors highlight the need for further research into cybersecurity and protection of cybercitizens in the context of good cybergovernance, calling for greater accountability. The role of government has now come into sharp focus in addressing the challenge of cybersecurity. This is exacerbated by poorly trained public servants who do not have a deep enough grasp of the challenges of risks posed by cybercriminals, cyberterrorists and the like. It is therefore incumbent on government to train and develop senior managers on cyber-related matters, to educate the public on being cybersmart and to implement cyberpolicies (which are already developed or which are currently being developed) so as to protect itself and society at large from cybercriminals.

REFERENCES

Alford, J. 2009. *Engaging public sector clients: From service-delivery to co-production*. Hampshire, UK: Palgrave Macmillan.

Argyriades, D. 2003. Values for public service: lessons learned from recent trends and the Millennium Summit. *International Review of Administrative Sciences.* 69(4):521–533.

Ansell, C. and Gash, A. 2007. Collaborative Governance in Theory and Practice. *Journal of Public Administration Research and Theory.* 18:543–561.

Bekkers, V. (Ed). 2007. *Governance and the democratic deficit: Assessing the democratic legitimacy of governance practices*. Aldershot, UK: Ashgate Publishing, Ltd.

Boons, F. 2008. Self-organization and sustainability: The emergence of a regional industrial economy. Emergence: *Complexity and Organization*. 10(2):41–48.

Boonstra, B. and Boelens, L. 2011. Self-organization in urban development: Towards a new perspective on spatial planning. *Urban Research & Practice*. 4:99–122.

Botha, A.C. and Van WoutLeenen, L. 2019. A comparison of Chat Applications in terms of security and privacy. Paper presented at conference. University of Coimbra, University of Coimbra, Portugal.

Bourgon, J. 2011. *A new synthesis of public administration: Serving in the 21st century* (Queen's Policy Studies). Montreal, Québec, Canada: McGill-Queen's University Press.

Bovaird, T. 2007. Beyond engagement and participation: User and community co-production of public services. *Public Administration Review.* 67:846–869.

Brainard, L.A. 2003. Citizen organising in cyberspace. Illustrations from health care and implications for public administration. *American Review of Public Administration.* 33(4):384–406.

Brewer, B. 2007. Citizen or customer? Complaints handling in the public sector. *International Review of Administrative Sciences.* 73(4):549–556.

Christensen, T. and Laegreid, P. 2007. The Whole of Government Approach to Public Sector Reform. *Public Administration Review*. 67(6):1059–1066.

De Graaf, G. and Van Asperen, V.H. 2016. The art of good governance: how images from the past provide inspiration for modern practice. *International Review of Administrative Sciences.* 84(2):405–420.

Dentchev, N.A. and Heene, A. 2004. Managing reputation of restructuring corporations: Send the right signal to the right stakeholder. *Journal of Public Affairs*. 4:56–72.

Department of Telecommunications and Postal Services. 2017. Cybersecurity Briefing to the Portfolio Committee, 28 February 2017. Available at: **https://pmg.org.za/files/170228Presentation_Cybersecurity.pptx**. (Accessed on 15 November 2019).

Eide, E.B. and Kaspersen, A. 2015. The dark side of the 4IR – and how to avoid it. World Economic Forum. Available at: www.weforum.org (Accessed on 5 November 2019).

Ferlie, E., Lynn Jr, L.L. and Pollitt, C. 2007. *The Oxford Handbook of Public Management*. Oxford: Oxford University Press.

Gazette. 2004. World Summit on the Information Society. Geneva 2003 – Tunis 2005. The *International Journal for Communication Studies.* 66(3–4):291–302.

Hartley, J. 2005. Innovation in governance and public services: Past and present. *Public Money and Management*. 25(1):27–34.

Herrington, L. and Aldrich, R. 2013. The future of cyber-resilience in an age of global complexity. *Politics.* 33(4):299–310.

Hulme, T. 2012. Information governance: Sharing the IBM approach. *Business Information Review.* 29(2):99–104.

Jarbandhan, D.B. 2017. Principles for Public Sector Leadership in the 4IR. Critical considerations. *Administratio Publica*. 25(4):60–72.

Kapur, J.C. 2000. IT and good governance. *Indian Journal of Public Administration.* 386–395.

Kaur, N. and Sitlhou, L. 2017. "Governance of Development Assistance: Issues and Challenges". Available at: http://ic-sd.org/wp-content/uploads/sites/4/2016/06/Development_Assistance_-_Full_Paper.pdf (Accessed on 23 February 2019).

Klijn, E.H. and Koppenjan, J.F. 2000. Public management and policy networks: Foundations of a network approach to governance. *Public Management an International Journal of Research and Theory*. 2:135–158.

Malick, M.H and Murthy, A.V.K. 2001. The challenge of E-Governance. *Indian Journal of Public Administration.* XLVII(2):238–253.

Minocha, A.P. 1998. Good governance: New Public Management perspective. *The Indian Journal of Public Administration.* 271–280.

Nundkumar, A and Subban, M. 2018. Embracing the 4IR: Risk-based perspectives of the South African TVET College Sector. *Journal of Contemporary Management.* Special Edition: 4IR. 15:305–328.

Okot-Uma, R.W.O. (n.d.). Electronic Governance: Reinventing Good Governance. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.6576&rep=rep1&type=pdf. (Accessed on 06 November 2019).

Osborne, D. and Gaebler, T. 1992. *Reinventing Government. How the entrepreneural spirit is transforming government.* Reading, MA: Addison-Wesley.

Pestoff, V. 2006. Citizens and co-production of welfare services: Childcare in eight European countries. *Public Management Review*. 8:503–519.

Pestoff, V. 2009. Towards a paradigm of democratic participation: Citizen participation and co-production of personal social services in Sweden. *Annals of Public and Cooperative Economics*. 80:197–224.

Phahlamohlaka, L.J., Jansen van Vuuren, J.C. and Coetzee, A.J. 2011. Cyber Security Awareness Toolkit for National Security: An Approach to South Africa's Cybersecurity Policy Implementation. 1–11.

Proceedings of the first IFIP TC9/TC11. South African Cyber Security Awareness Workshop (SACSAW) Gaborone. Botswana. Available at: http://hdl.handle.net/10204/5162 (Accessed on 25 January 2019).

Portugali, J. 2000. *Self-organization and the city*. London, England: Springer Science & Business Media.

Ramlackan, T., Subban, M. and McArthur, B. 2016. The relevance of South African Legislation on social media as a strategic disaster and crisis communications tool. *Journal of Information Warfare*. 15(1):60–74.

Rattan, J. and Rattan, V. 2008. Metamorphosis of Public Administration and Law in India: A critical assessment of the impact of IT and global competitiveness. *Indian Journal of Public Administration*. LIV(4):886–903.

Republic of South Africa. 1996. *Constitution of the Republic of South Africa*. Pretoria: Government Printers.

Republic of South Africa. 2015. The National Cyber Security Policy Framework. Pretoria: Government Printers.

Sangita, S.N. and Dash, B.C. 2008. Information communication technology, governance and service delivery in India: A critical review. *Indian Journal of Public Administration*. LIV(1):141–161.

Sapru, R.K. and Sapru, Y. 2014. Good governance through eGovernance with special reference to India. *Indian Journal of Public Administration*. LX(2):313–331.

Schwab, K. 2016. *The 4IR*, The World Economic Forum. Available at: http://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab (Accessed on 7 November 2019).

Shamshad, A. 2009. Right to information: Issues of administrative efficiency, public accountability and good governance in India. *Indian Journal of Public Administration*. IV(3):562–577.

Shava, E. and Hofisi, C. 2017. Challenges and opportunities for Public Administration in the 4IR. *African Journal of Public Affairs*. 9(9):203–215.

Sørensen, E. and Torfing, J. (Eds.). 2016. *Theories of democratic network governance*. London, England: Palgrave Macmillan UK.

Stoker, G. 2006. Public value management: A new narrative for networked governance? *The American Review of Public Administration*. 36:41–57.

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.

Van Heerden, Q., Steenkamp, A. and Van Heerden, M. 2018. Chaining the building blocks for blockchain implementations in South Africa's public sector. Steering the 4th Industrial Revolution. 29th SAIIEE Annual Conference Proceedings. 3886-1. 913–924.

Van der Steen, M., Van Twist, M.J.W. and Bressers, D. 2018. The Sedimentation of Public Values: How a Variety of Governance Perspectives Guide the Practical Actions of Civil Servants. *Review of Public Personnel Administration*. 38(4):387–414.

Veerasamy, N., Grobler, M. and Von Solms, S. 2012. Towards a cyberterrorism Life-Cycle (CLC) Model. Proceedings of the 4th workshop on ICT uses in Warfare and the Safeguarding of Peace, Sandton, Johannesburg. 1–10.

World Economic Forum. 2019. The cyber security guide for leaders in today's digital world. Shaping the future of cyber security and digital trust. World Economic Forum. 1–24.

Wyman, R. 2017. Consider the consequences: A powerful approach for reducing ICS cyber risk. *Cyber Security*. 1(1):1–17.

AUTHORS' CONTACT DETAILS

Professor Mogie Subban (corresponding author)
School of Management, Information Technology and Governance
University of KwaZulu-Natal
Cell: 082 373 4303
Email: subbanm@ukzn.ac.za

Professor D B Jarbandhan
School of Public Management, Governance and Public Policy
Affiliation: University of Johannesburg
Cell: 083 647 2580
Email: vainj@uj.ac.za