South African – European Union Dialogue Facility

International Dialogue on

Strengthening Open Digital Governance in South Africa

Report on the

International Experience in Open Digital Governance

Luci Abrahams and Mark Burke

LINK Centre, University of the Witwatersrand

Prepared for the SA–EU Strategic Partnership Dialogue Facility

April 2022

Table of Contents

Abbreviations

AEPS	-	Aadhaar Enabled Payment System
AfCFTA	-	African Continental Free Trade Area
AI	-	Artificial intelligence
CBRA	-	Cross-border Regulatory Agency
CIDR	-	Central Identities Data Repository
CIO	-	Chief Information Officer
CoKP	-	Community of Knowledge and Practice
CPSI	-	Centre for Public Service Innovation
CSD	-	Central Supplier Database
CSIRT	-	Computer Security Incident Response Team
DCDT	-	Department of Communications and Digital Technologies
DGU	-	Digital Government Unit
DLT	-	Distributed Ledger Technologies
DSP	-	Digital Service Producer
DPSA	-	Department of Public Service and Administration
DSI	-	Department of Science and Innovation
EU	-	European Union
FDI	-	Foreign Direct Investment
GDPR	-	General Data Protection Regulation
GITOC	-	Government Information Technology Officers Council
GSMA	-	Groupe Speciale Mobile Association
ICT	-	Information and Communication Technologies
ID	-	Identity Document
IEEE	-	Institute of Electrical and Electronic Engineers
IGA	-	Internet Governance Alliance
ISOC	-	Internet Society
ITU	-	International Telecommunication Union
KYC	-	Know-Your-Customer
MoUs	-	Memorandums of Understanding
NIS	-	Network and Information Security
ODG	-	Open Digital Governance
OECD	-	Organisation for Economic Cooperation and Development
OES	-	Operators of Essential Services
OGP	-	Open Government Partnership
POPIA	-	Protection of Personal Information Act
SARS	-	South African Revenue Service

SEIAS	-	Socio-economic Impact Assessment System
SMYW	-	Small, Medium, Young and Women
UIDAI	-	Unique Identification Authority of India
UID	-	Unique Identity Number
UN/CEFACT	-	United Nations Centre for Trade Facilitation and Electronic Business

1. Introduction: Five Overarching Insights from International Experience

This paper on international experience in digital government explores five overarching insights through an overview of trends in the evolution to open digital governance (ODG), and a review of four case studies. Noting that South Africa is one focus of the dialogue and Denmark is the other, both countries can contribute to and benefit from the ongoing conversation on these overarching insights (which aggregate the many insights from the case studies), because they raise common issues for attention that are pertinent to all countries interested in strengthening ODG. Open digital governance can be explored from two perspectives: (i) using digital technologies, applications and processes to promote transparent and good governance, including open engagement and collaborative creation between citizens and government; and (ii) setting the policy, the legal and regulatory standards, and the institutional environment to achieve ODG. Both perspectives are included in the set of five overarching insights, noting the particular interest of the Department of Public Service and Administration (DPSA) and the Centre for Public Service Innovation (CPSI) in ODG, as well as the critical role to be played by the Government Information Technology Officers Council (GITOC) in achieving ODG.

Overarching Insight 1: A 21st century public service for 21st century citizens: Mission, leadership, and positioning of institutions responsible for public service innovation for open digital governance

Adopting and strengthening open governance requires a recognition that transparent and collaborative governance contributes to good governance and democracy. In the 21st century, citizens everywhere seek greater transparency from their governments, as a means of achieving the social and economic empowerment of all citizens. Using digital applications, governments can apply many layers of transparency and efficiency, in many aspects of governmental action, from single window applications designed to address the requirements of a segment of the population (traders), to education and health services and digital identity applications to meet the needs of the population as a whole. This requires a strong mission, in other words, a strongly embedded intention to achieve ODG no matter what obstacles and challenges might arise. It also requires highly committed, corruption-free, digital leadership.

Overarching Insight 2: Shifting to “digital-first”: Digital applications and data-driven public services for open digital governance

In all parts of the public service lie opportunities to introduce and exercise ODG. This requires the adoption of a “digital-first” approach for the public service as a whole. Digital-first means that the senior management of the public service must consider how digital applications can render the main services offered by their departments and agencies open, transparent and collaborative, in the interests of good governance and democracy. Digital-first also means that, where departments have already digitised their main services, they continually explore ways of strengthening openness, by enhancing service capability through continual digital innovation. Even more important, digital-first means that open governance is enabled by ensuring that citizens and residents of South Africa have access to all the

required information about government decisions, decision-making and the value created through public expenditure, in language and in formats that are easy to understand, and that they can participate in decision-making. While many digital applications are relatively costly, it is important to take note of the opportunities for low-cost, frugal innovation. Shifting to digital-first requires a mindset and culture change for the DPSA, the CPSI and the GITOC, and for the whole of government.

Overarching Insight 3: A 21st century public servant for a 21st century public service: Human capability for open digital governance

A major focus for strengthening ODG must be the strengthening of human capabilities, in terms of both understanding and advancing the rationale for openness, and understanding and advancing the capability to envision, design and operate digitally-enabled public service delivery, side by side with collaborative decision-making with citizens. The 21st century public service can work in tandem with other available sources of human capability, such as developers and start-ups in the tech hub and maker space ecosystem, augmenting the still limited digital capabilities in government.

Overarching Insight 4: Making open governance possible: Legislation, regulatory frameworks and standards for open digital governance

Open digital governance is only possible if the enabling legislative frameworks are enacted, if the appropriate regulatory decisions are made, and if the required standards are adopted. Many countries have adopted or are in the process of adopting legislation and regulations that will encourage ODG and mitigate the risks associated therewith, one of which is the European Union General Data Protection Regulation (GDPR). Organisations such as the International Telecommunication Union (ITU), the Internet Society (ISOC), the Institute of Electrical and Electronic Engineers (IEEE), the Wi-Fi Internet Governance Alliance and the Groupe Speciale Mobile Association (GSMA) are major players in the design of standards (GIP Digital Watch, no date) relevant to making ODG possible. At the national level, countries need the capacity to follow the progress of standards adoption and to understand the gaps in standards from the perspective of enabling ODG, particularly with respect to open standards for data sharing. Noting that open standards can apply to infrastructure, data, platforms and services, the DPSA, the CPSI and the GITOC could adopt the 5 core principles for open standards development (https://open-stand.org/resources/infographics/). Furthermore, the DPSA, the CPSI and the GITOC could build on existing standards for data sharing, such as the many standards referenced in the guidebook by the Open Data Institute (https://standards.theodi.org/introduction/what-are-open-standards-for-data/).

Overarching Insight 5: Public service innovation: Continually building a future orientation for open digital governance

In order to strengthen ODG, the state of knowledge in the DPSA, the CPSI and the GITOC must be extensive. This requires the creation of a few communities of knowledge and practice (CoKPs), in particular with attention to “digital-first”, human capability and standards. Furthermore, public service innovation must be designed as: (i) a platform; and (ii) a

research laboratory, with a research team constantly engaged in setting the future-oriented context required for public service innovation in general, and for ODG in particular.

In this paper on international experience relevant to ODG, the Aadhaar digital identity case study, the China single window for cross-border trade case study, the Malaysia smart schools case study and the Africa tech hubs case study offer a brief summative perspective, as the foundation for presenting the five overarching insights. Below we offer a tabular mapping of the case studies from international experience to the overarching insights.

A key idea emerging from the case studies, as relevant to the overarching insights, is that the DPSA needs to shift its gaze beyond setting public service rules and standards to having its major focus on public service innovation, including but not limited to ODG. It needs to set the future-oriented frame for the civil service and its operations, which needs continual resetting, as old challenges and new technologies present the opportunities for creating a contemporary public service, or what many refer to as modernisation, and which we can also refer to as innovation-oriented transformation. In so doing, the DPSA can make new rules and set new standards relevant to the transformed civil service administration and organisation. Even more important, it can shift from an overwhelmingly generic approach to its mandate, to include specialised approaches, where the DPSA, the CPSI and the GITOC engage with the specific nature of components of the public service and how they can each be transformed and therefore contribute to transformation in economy and society. There will be lessons that can be applied from one experience to another, where the DPSA is best suited to share those lessons because it looks across the public service as a whole. Nearly 20 years after the establishment of the CPSI, it is time to integrate the work of the DPSA and the work of the CPSI, so that the historical CPSI mandate can merge with the historical DPSA mandate and so that public service innovation can take centre stage. Like other departments who have shifted their identity and expressed that through a name change (the Department of Science and Innovation and the Department of Communications and Digital Technologies), the DPSA could become the Department of Public Service and Innovation (DPSI). Without a much more determined mission to create public service innovation, ODG will not be possible.

2. Evolution Towards Open Digital Governance

Contemporary societal challenges such as the climate emergency, the development of sustainable food systems, and the digital transformation of society, to name a few, are too complex and contested to enable centralised policy and regulation by governments alone for their resolution (Hajer & Wagenaar, 2003). Thus, governing arrangements that recognise the contribution of many actors to addressing these challenges need to move beyond the public–private divide in recognition of the limitations of traditional government by the state on its own (Kooiman, 2003). The notion of governance has come to the fore over the past three decades to signal the understanding that “sustained coordination and coherence among a wide variety of actors with different purposes and objectives such as political actors and institutions, corporate interests, civil society, and transnational organisations” are required to address societal challenges (Pierre, 2000, pp. 3–4). The governance approach assumes that

no single actor has the knowledge, information and resources to address complex and dynamic societal challenges (Kooiman, 2003).

The governance approach, as an institutional configuration to address societal challenges, cleared the path for the emergence of the ODG paradigm. Aided by the open data and open government movements, the ODG paradigm seeks to engineer a shift from governing arrangements and practice that are government-centric to ones that are citizen-centric. The origins of the Open Data movement can be traced to a gathering of Internet activists and thinkers in Sebastopol in December 2007, who proceeded to define the concept of open public data and established the principles to evaluate such data (Chignard, 2013). This approach to open data is premised on the notion that public data is a common property, and the movement encourages the sharing and use of such data as a common good. Open Data is a crucial catalyst towards Open Government, which is more accessible, responsive and accountable, and recognises the long-term benefits of improving citizen–government relations. The establishment of the Open Government Partnership (OGP) in 2011, working towards transforming how government serves its citizens, was a key milestone in the development of Open Government (https://www.opengovpartnership.org). Both Open Data and Open Government have contributed to the development of the ODG paradigm, given the focus on creating transparency, accountability and engagement.

A hallmark of the ODG paradigm is the degree and quality of the integration of citizens into political and service delivery processes through digital technologies, and transparency, participation and accountability are highly valued (OECD, 2016). As such, the paradigm places strong emphasis on co-production through which citizens collaborate with governmental institutions and entities to create public value (Meijer et al., 2019). In this paradigm, the role of data takes on critical significance through the provision of data by government to citizens and other actors (Kassen, 2022) to produce relevant information around shared value to address societal challenges (Meijer et al., 2019).

The proliferation of digital technologies in society and the extent to which they influence, shape and structure our everyday lives have significance implications for the way in which societies are governed. The contours of change are observed in the near ubiquitous access to the Internet (noting unequal access that nevertheless limits the extent to which large segments of societies can participate in the Information Society) that facilitates the emergence of networked and connected communities who are increasingly mobile and produce large volumes of digitised data. While many contributing factors trace the outline of these contours, the global character of contemporary society, its networked mode of organisation, and the accelerating pace of change are important to highlight, given the impact of these on governance and government.

Contemporary society is global in character; this would not have been possible without the proliferation of digital technologies throughout society. Globalisation is manifested through patterns of world-wide economic, financial, technological and ecological interdependence that continue to intensify (Held et al., 1999). The network mode of organisation activated by digital technologies has emerged as an integral feature of society, characterised by properties such as flexibility (ability to reconfigure in response to changing environments),

scalability (ability to expand and shrink with little disruption) and survivability (ability to operate in a wide range of configurations) (Castells, 2013). These properties, in turn, contribute to fragmentation and dispersion through high levels of connectivity and heterarchical social structures (Van Dijk, 2005). Finally, contemporary society is characterised by the accelerating pace of change (Rosa, 2013), linked to the speed of innovation and acceleration as a core rationale in computing so that this "accelerative logic flows into society" (Hassan, 2009, p. 159).

The administrative apparatus of bureaucratic government, the slow pace of policy and regulation, and siloed approaches to delivering services are at odds with these factors contributing to the qualitative changes emerging in society. Globalisation limits the extent to which governments can exercise full authority over rulemaking in their jurisdictions as they need to take account of international harmonisation and standardisation, for example in accounting for and capturing the value from cross-border trade in data. The network mode of organisation is increasingly becoming a feature of the way in which government is organised, given the limits of bureaucratic organisation to adapt and respond to complex challenges that span sectoral and service domains. The practice of policy and regulation is constantly in a state of catch-up as governments struggle to keep pace with technological innovation in society, such as in respect of regulating artificial intelligence (AI).

How do governments respond to the need for embedding ODG in ways that recognise the critical role of a broad range of stakeholders and actors in addressing societal challenges, while at the same time governing the processes of internal digital transformation that are underway? In order to identify the opportunities and challenges available it is necessary to briefly review the development of digital government over the past few decades.

3. Emergence of Digital Government

The mechanisms to deploy ODG approaches have their foundations in digital government, since interactions between governments and their citizens are premised on the exchange of information and data; therefore, digital technologies that facilitate data acquisition, storage, processing and communication are core technologies for government (Van de Donk & Snellen, 1999). Digital technologies are characterised by a fundamental duality in that they simultaneously generate information that provides transparency to activities and produce information that reflects back on their activities so that they render events, objects and processes visible, marking the difference between "smart" and "dumb" (Zuboff, 2015). These technologies are likened to the brain and nervous system since they can replace human communication, thinking and calculation and are far more complex in their application, use and effect (Fountain, 2001). Digital technologies support the internal management, public management and regulation, and delivery of public services by enabling information services, contact services, transaction services and data transfer services (Bekkers & Homburg, 2005).

Digital government has evolved through successive stages, linked to the capabilities afforded by digital technologies. Limited transformation change took place in the period from 1950 to the late 1990s (Dunleavy et al., 2006). This period first saw the introduction of

mainframe computers with complex interfaces in the defence and science sectors, followed by the cheaper, more powerful ones with less complex interfaces in the 1960s to centralise large administrative operations around batch-processing locations. The 1960s also witnessed the widespread use of computers for holding financial information which contributed to greater systematisation and the improvement of government accounting systems. Once these systems started being networked to remote terminals, computers commenced penetrating a wider range of "front" office administrative settings, and only after the development of relational databases with structured query capabilities did some changes occur in how much was computerised and the way in which data was stored. Office automation processes remained extensively adapted to and fitted in administrative arrangements and pre-existing cultures of public sector agencies (Dunleavy et al., 2006).

Only after the advent of the Internet with its World Wide Web system of hyperlinks was access to information and transactions across different departments and tiers of government enabled. It represented a technological convergence of several different digital technologies and media, including IT, telecommunications and broadcasting, which enabled digitisation, integration and interactivity, and the emergence of digital government (Lips, 2020). It provided a major opportunity to break down silos in government and deliver services in a more integrated, citizen-centric and responsive manner by making use of integrated web portals and facilitating the integration of services provided in different policy domains. Digital technologies are a critical infrastructure that made possible the integration between the front office and multiple, separated back offices in different government entities, contributing towards the ongoing shift towards citizen-centric public service delivery (Lips, 2020). The process evolved from a focus on technology in government to e-government and, at present, to digital governance (Janowski, 2015). The concept of digital government, first coined by the US National Science Foundation (Scholl, 2008), is defined as "the introduction, application and use of digital technologies and data in government and its external relationships (including citizens, businesses, civil society and international organizations) and the democratic, governmental and managerial implications" (Lips, 2020, p. 9).

Digital-era changes have triggered several shifts that coalesce around three themes (Dunleavy et al., 2006). The first is a process of reintegration that involves the increased use of shared services and simplifying delivery chains and joined-up governance. The second is holism that focuses on the re-organisation of services around the citizen, supported by data warehousing, simplified and integrated processes, and the co-production of services. The third is digitisation incorporating the concept of "digital by default" with fully online strategies for delivery, combining automated processes and isocratic administration.

4. Digital Technologies for Data-led Digital Governance

The nature of the capabilities that emerge in digital government environments is influenced by technological innovation and the types of technologies emerging. General purpose technologies are typically interdependent, interconnected and mutually reinforcing, with significant potential for disrupting the status quo (UN, 2018). The key characteristics of these technologies are that they are pervasive (spreading to most sectors), continually improving,

and innovation-spawning. Two key technologies that have a significant impact on government's data-enabled capabilities are briefly discussed below.

Artificial intelligence (AI) is founded on the notion that machines can be used to simulate human intelligence by understanding how multiple facts interconnect to form knowledge that can be represented in machine understandable form, including reasoning and learning processes that enhance the knowledge of a system (Franceschetti, 2018). The growth in the field is driven by the large volumes of data available, the diminishing cost of storage, and faster data processing speeds. The capabilities afforded through AI are centred on improved or augmented human decision-making and the design of solutions for complex problems. AI is used in many different sectors of the public service, including healthcare, transportation, predicting energy consumption, and monitoring pollution (OECD, 2019a). Some of the major risks related to AI include privacy invasion and surveillance, algorithmic bias, lack of transparency, adverse impacts on employment, and inequality (Franceschetti, 2018).

Big data refers to the process of examining very large data sets to uncover hidden patterns and unknown correlations that are so complex that traditional data processing application software is unable to deal with them (Engin & Treleaven, 2019). It concerns the volume of data generated, the variety thereof, the velocity at which it is created, and the veracity and value of the data. The drivers contributing to the development of the technologies supporting big data include the increasing proliferation of smart devices, sensors and connected networks that have boosted data generation, increased storage capacity and processing speeds, and improvements in data analytics through data science. The capabilities associated with big data include improved decision-support, analytical and predictive capacity, and the surfacing of hidden patterns and relationship. Big data is increasingly supporting a number of public sector domains, including smart city applications (Bibri, 2019), policymaking (Giest, 2017), and patient behaviour monitoring (Chui et al., 2019). The key concerns related to big data are linked to privacy, transparency and accountability, and data governance and regulation.

5. Digital Government Drivers, Barriers and Enablers

A range of factors serve as drivers for the development of digital transformation, including political and social, economic, and technological factors (Barcevičius, 2019). From a political and social perspective, the proliferation of digital technologies in the private sector and society more broadly exerts isomorphic pressures arising from efforts to keep up with digital transformation in business, the demand for improved services from government, and calls for increased transparency and participation in the political process. Economic factors refer to the attainment of objectives related to the realisation of benefits such as internal efficiency, effectiveness and rationalisation in government. Technological factors are those that stimulate new demand and expectations for innovative public service delivery, such as increasing capacity for connectivity and the processing, analysis and storage of data.

Technological, organisational and legal factors serve as constraints to the effective development of digital government (Barcevičius, 2019). Aging and outdated IT infrastructure, legacy systems and a lack of interoperability limit the pace at which digital government

evolves. There is a high degree of risk associated with the introduction of large-scale technology projects and the associated costs involved in the replacement of legacy systems and new digital infrastructure, technologies, systems, datasets and applications (Lips, 2020). On the organisational front, vertical and horizontal fragmentation present significant barriers (Barcevičius, 2019). Addressing these constraints requires management of a wide range of organisational and cultural changes in service relationships with citizens to provide new digital government services in more citizen-centric and integrated ways (Lips, 2020). Furthermore, new digital capabilities are required to address the integration and use of rapidly evolving technologies (UN, 2020), and these new capabilities require the re-skilling and up-skilling of public servants involved in digital government service provision (Lips, 2020). Privacy, data and cybersecurity concerns may also hinder digitalisation (Barcevičius, 2019), with laws and regulations made prior to the increased use of digital technologies hindering its deployment (Lips, 2020).

Enablers must be oriented towards addressing these barriers by focusing on the establishment of an appropriate and conducive policy, legal and regulatory regime; digital capabilities and skills in the public sector; and an environment that fosters innovation in the public sector (Dener et al., 2021). Strong and sustained political leadership and a comprehensive plan for digital government with a clear vision that enables inter-governmental coordination and collaboration are vital ingredients (Ingram & Dooley, 2021). The use of digital technology in identification systems is regarded as a necessary condition for digital government and a service relationship with citizens. The number of countries that have introduced digital identification stands at 161 (Dener et al., 2021), reinforcing the need for robust privacy and data protection and cybersecurity.

6. Digital Leadership through Policy, Strategy, Regulation and Institutional Arrangements

While significant progress towards digital government has been made over the past decade, several challenges remain, including (Dener et al., 2021):

> (a) the growing concern by governments about cybersecurity and by people about data privacy and protection; (b) the need to provide multiple channels for service delivery so that citizens have a choice of service access, particularly those who do not have adequate connectivity, devices, or literacy; and (c) limited government financial and human resources for developing and implementing digital government policies.

Effective policy, strategy and regulation are required to address these challenges.

6.1. Exercising Digital Leadership through Policy

Policy and its implementation are necessary to address societal problems and should lead to the interventions aiming to solve identified challenges. Policymaking refers to the ongoing process which recognises problems, formulates alternative courses of action, effects and implements chosen policy interventions, and evaluates the outcomes thereof (Dunn, 2018).

Digital technologies have also impacted the policy domain through the explosive growth in data and computational power that have contributed to the development of new approaches, concepts, instruments and methods needed to deal with societal problems. Developments such as open data, computational methods of processing data, simulation and visualisation are influencing the field of policymaking (Janssen et al., 2015). In the case of digital government policy, policymaking refers to the tools used to promote system-wide digital transformation through establishing the key enablers such as interoperability, digital identity, shared services and data infrastructures as the foundations on which it is built (OECD, 2019b). It incorporates the hard and soft instruments that policymakers can leverage to enable this change from strategy to implementation and delivery (OECD, 2021).

Based on the extensive work undertaken by the Organisation for Economic Cooperation and Development (OECD), the focus of government policy should incorporate the attainment of six dimensions (OECD, 2020). First, government policy should promote a *"digital by design"* approach in which digital is considered mandatory and the mobilisation of new and existing technologies is prioritised towards an omnichannel approach to service delivery. Second, policy should enable a *data-driven* public sector that recognises data as a strategic asset within the framework of a coherent and comprehensive data model and governance arrangements that exploit the value of data while at the same time protecting the data rights of citizens. Third, policy should facilitate the development of *government as a platform* premised on the development of an ecosystem for the delivery of high-quality services at scale. Fourth, policy should promote an *"open by default"* approach that ensures government data and policymaking processes are available and open to stakeholders to engage with to enable co-creation, cooperation and collaboration with different stakeholder groups. Fifth, it is necessary to ensure a *user-driven approach* in terms of which citizens and their needs are placed at the centre of policy and service design, development, delivery and monitoring. Finally, governments should adopt a proactive approach in which the needs of citizens are anticipated and responded to rapidly.

6.2. Exercising Digital Leadership through Strategy

Digital government strategy should provide a vision, with clearly defined goals and milestones, taking into account how stakeholders and their activities are incorporated (OECD, 2021). Two major approaches have been identified to setting strategy. Some countries have established an autonomous digital government strategy, which is set out in a single document, while others have opted for embedding their strategic priorities in different documents related to the digital economy and society, or public sector reform strategies. Either way, the digital government strategy should have strong linkages with other strategies and must be backed by measures and mechanisms that ensure strong coherence and effectiveness in the design and implementation of priorities.

Since 2015, 174 digital government entities have approved strategies with action plans to support the digital transformation of the public sector (Dener et al., 2021). Strategies should be clear on the problems to be addressed and the solutions proposed; indicate how government will manage financing and resourcing projects, activities and services; provide guidance on interoperability, network capability and institutional design; set out approaches

to be adopted in the management of digital technology projects; provide a framework for dealing with data; and indicate how citizens and stakeholders will be engaged (Sandoval-Almazán et al., 2017). Strategy typologies that prioritise different areas of focus include integration strategies focusing on the expansion of the range of digital services; network strategies that prioritise cooperation for digital service provision; access strategies that highlight the provision of access to citizens; and transformation strategies that concentrate on leveraging digital technology for catalytic change in government (Wirtz & Daiser, 2015). The implementation of the strategy requires a continual process of developing partnerships and alliances to influence key stakeholders, creating awareness of available resources and capabilities, drawing on support from the highest levels of government, establishing enabling legal frameworks, and creating the institutional frameworks that provide continuity and legitimacy (OECD, 2021).

The European Data Strategy (EC, 2020) recognises the central significance of data to digital transformation as the basis for new products and services, productivity and efficiency gains, and for enabling improved policymaking and upgrading of government services, and hopes that the strategy will become a model for other nations to follow. The purpose of this strategy is to create a single European data space in which fit-for-purpose legislation and governance will provide the framework for ensuring the availability of data with investments in standards, tools, and infrastructures and capabilities for data handling. The main pillars of the strategy rely on cross-sectoral measures for data access and use; enablers that include investments in data and capabilities for hosting, processing and using data; building competencies; and creating a common European data space in strategic sectors in manufacturing, health, financial services, energy, agriculture, public administration and skills.

6.3. Leading Open Digital Governance through Legislation and Regulation

The creation of large volumes of data arising from rapid technological innovation and the speed at which it can be generated, accessed, analysed and shared in contemporary society poses a host of legislative and regulatory challenges for government. The most significant of these are privacy protection, data protection and cybersecurity. The extent to which data can be used to improve the lives of people depends on the dissemination and exchange thereof, which, in turn, requires trust in the systems, regulations and institutions that underpin the security of data collection, processing and sharing (World Bank, 2021).

Three generations of digital rights relevant to digital government can be distinguished (OECD, 2021). The first generation consists of the groups of fundamental and essential rights such as personal data protection, cybersecurity and digital inclusion. The second generation of digital rights arises from the rapid adoption of technologies and comprises rights such as digital identity, transparency and open data. The third generation has reference to digitally mature government environments in which rights are linked to omnichannel and proactive service delivery, the ethical use of data and AI, and data ownership and management.

Data policy and governance aid in compliance with regulatory and legal requirements through data management and protection, information security, and the introduction of

principles and guidance related to data interoperability, standards and quality (EC, 2020b). The EU has made a proposal for a Data Act (EC, 2022) to ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data in a manner that is consistent with the rules for processing person data, including the GDPR and the ePrivacy Regulation, currently the subject of legislative negotiation.

The protection of privacy, and the use of data protection as the instrument to do so, has been given a significant boost with the landmark adoption of the GDPR in 2016, which took effect in 2018. The GDPR is considered the gold standard for data protection in the world, with many countries having modelled their legislation on this regulation (Kuner et al., 2020). The regulation is based on OECD principles for the fair processing of personal data, including transparency, data quality, accountability, and use and collection limitation (Custers et al., 2019). The GDPR is regarded as a regulatory floor for a widening range of policies in health, AI, transport, energy, competition and law enforcement, and has established a new governance structure with independent national data protection authorities as enforcers at its centre (EC, 2019). A critique of the GDPR is that it is focused on achieving procedural fairness rather than substantive fairness (Custers et al., 2019).

Countering cyber threats that can undermine the cyber–physical systems that integrate digital technologies and physical systems is a necessary condition for data governance, privacy protection, and the maintenance of trust in digital transformation. New categories of vulnerability arise with the integration of cyber–physical systems, including interception, replacement or removal of information from communication channels through the capture and disruption of computer systems or network operations. Cybersecurity incorporates data security, cryptography, software and hardware security, network and systems security, privacy, and other risks and issues. It comprises a body of knowledge about technology, processes and practices related to computers, data sources and networks (Möller, 2020). The Network and Information Security (NIS) Directive is aimed at achieving a high level of cybersecurity in Europe by establishing, among others, the NIS Cooperation Group and the network of Computer Security Incident Response Teams (CSIRTs) with the purpose of the exchange of information and cooperation related to measures and incidents (Negreiro, 2021). The implementation of risk management and reporting obligations for Operators of Essential Services (OES) and Digital Service Producers (DSPs) is one of the three pillars of the NIS Directive. Following the adoption of a new EU cybersecurity strategy (EC, 2020a), a proposal was submitted for the implementation of a revised directive (NIS 2) to replace the first one.

6.4. Standards and Interoperability as Central to Open Digital Governance

Standards are normative non-binding frameworks that provide common guidance on implementation approaches for adopting digital technologies in support of digital government (OECD, 2021). The existence of standards and interoperable systems is necessary to enable the data flows in government (OECD, 2019b). Interoperability is enabled by four layers (EC, 2017). It consists of legal interoperability, which refers to harmonised legal frameworks, policies and strategies; organisational interoperability, which comprises the way in which public administrations align business processes for mutually beneficial goals and

information exchange; semantic interoperability, which refers to the vocabularies and schemata to describe data exchanges providing the meaning of data elements and the relationship between them; and technical interoperability, which covers the applications and infrastructures linking systems and services.

A wide range of technical approaches to the implementation of interoperability across systems is observed, noting that these approaches are influenced by a country's context, governance structures and public administration traditions (Toomere et al., 2022). Countries such as the United Kingdom (UK) and Australia, for example, follow an application programming interface-first (API-first) based approach. Norway has introduced state-of-the-art systems, based on cloud, utilising a microservices-based architecture, while South Korea has used a centralised method for hosting and exchanging data. There is an increasing movement towards API-based interoperability systems which is likely to be accompanied by a shift away from a centralised data exchange with decentralised data storage approach to a decentralised data exchange approach (Toomere et al., 2022).

6.5. Design Features for Institutional Arrangements and Capabilities

Institutional arrangements describe the formal and informal ways of organising to govern and coordinate the implementation of digital government strategies and service transformation. These working arrangements influence government's agility, innovativeness and responsiveness to changes internally and externally. The most mature and advanced institutional arrangements are those in which an organisation in charge is at the centre of government, often in the prime minister's office or through a line ministry, and can itself either be a public sector agency, unit, office or directorate (OECD, 2021).

Notably, from 2011 onwards, an increasing number of governments have introduced specialised Digital Government Units (DGUs), as an example of policy transfer from countries such as the United States, Australia, Canada and the UK (Clark, 2020). These are dedicated in-house units of digital expertise operating at the centre of government that have adopted agile, user-centric approaches and rely on open standards and platform-based approaches. These teams are often led by private sector executives that bring new capabilities, skills and expertise (Mergel, 2019). Dedicated central government units have been established among 63 government entities, with 42 institutions connected to either the president's office, the prime minister's office or the ministry of information and communication technology (ICT) (Dener et al., 2021). These institutions are empowered to lead, initiate, design, allocate, implement and coordinate digital government policies and projects (OECD, 2021).

A central feature of a holistic approach to digital government development is the alignment of institutions, organisations, people, technology and data to bring about the intended change (UN, 2020). Digital skills and expertise are core factors in the advancement of digital government and to render coordination functions, advisory responsibility and in enabling decision-making (OECD, 2021). One hundred and forty-five countries have appointed a Chief Information Officer (CIO) or equivalent and several countries have appointed a network of CIO focal points within strategic institutions (UN, 2020). This role is deemed to be

the highest-ranking administrative officer responsible for overseeing public sector digital transformation and the implementation of digital technology projects (OECD, 2021).

7. Case Synopsis

The rationale for selecting these case studies is that they highlight a few of the issues that should be considered when government transitions to ODG, particularly as this relates to transparent, accountable and responsive engagement with citizens. Aadhaar demonstrates the significance of digital identity systems in socio-economic inclusion; the Customs Single Window case focuses on the role of platforms in mediating economic interactions among a diversity of stakeholders; the Smart School example illustrates the importance of building skills and capacities for young people and the parent community to engage in governance; and the Tech Hub and Maker Spaces case highlights the role that civil society organisations play in supporting applications and systems development through frugal innovation.

Figure 7.1 Case synopsis relevant to open digital governance

	Aadhaar, India	Customs Single Window, China	Smart Schools, Malaysia	Tech Hubs and Maker Spaces, Africa
Rationale	• Significance of identity as the basis for citizen social and economic inclusion	• Role of platforms in mediating economic interactions among many stakeholders	• Importance of building the skills and capacities of young people to engage in governance	• The role of civil society organisations in contributing to applications and systems development through frugal innovation
Overarching insights	• Strong mission to create impact through digital-first mega-projects	• Mission orientation and effective leadership in multi-stakeholder contexts through legislation, regulation and standards	• A strong mission orientation matched by a strong future orientation to build a 21st century economy and society	• Access to digital skills and resources to augment the capacity of the public service
Digital innovation	• Interoperability through open scale-out architecture	• DLT for inter-agency information sharing and cross-border information exchange	• Use of low-cost media and dynamic software applications	• Role of entrepreneurship in developing applications, platforms and solutions to solve problems
Skills and capabilities	• Mix of tech industry skills and public sector knowledge	• Mix of technical engineering skills and collaboration skills	• Mix of digital skills and 21st century skills	• Harnessing the skills of technopreneurs
Policy and regulation	• The risks associated with a “build first, legislate later” approach	• The role of regtech and suptech in regulation	• Policy and regulation mitigate risk of harmful content and cyberbullying	• Policy to enable explicit engagement and transactions capability with tech hubs and maker spaces
Implementation ideas	• Re-examine the concept of identity in digital service delivery	• Opportunities for platform-based governance	• Learners and parents as significant stakeholders in ODG	• Development of open governance applications

Each of the case studies presents a specific insight of relevance to South Africa. These insights are framed as overarching insights. The case of Aadhaar illustrates the coalescing of all stakeholders around a strong mission with political support for a challenging mega-project. The Customs Single Window case demonstrates the need for effective leadership in a multi-stakeholder context, supported by appropriate legal frameworks. The Smart School case demonstrates the orientation towards the future with the goal of being a 21st century innovation-based economy and society, and the Tech Hubs and Maker Spaces case notes the importance of finding ways to augment the capacity of the public service.

The digital innovations highlighted in the case studies include achieving interoperability through open scale-out architecture in the case of Aadhaar, the use of distributed ledge technology (DLT) to support inter-agency information sharing and cross-border information exchange in the case of the Customs Single Window, the use of low-cost media and dynamic software applications in the Smart School case, and the role of entrepreneurship oriented towards problem-solving in developing applications, platforms and solutions in the Tech Hubs and Maker Spaces case.

The cases highlight the importance of a mix of tech industry skills together with public sector knowledge, technical engineering and collaboration skills, digital and 21st century skills, and leveraging the skills of technopreneurs.

On the policy and regulatory front, the cases highlighted the risks associated with a "build first, legislate later" approach (Aadhaar), the potential role for regulatory and supervisory technologies in regulation (Customs Single Window), the importance of mitigating risks associated with harmful content and cyberbullying among young people (Smart Schools), and the need for policies that explicitly support transactions with Tech Hubs and Maker Spaces.

Finally, the cases noted several implementation ideas relevant to South Africa. Since identity is essential for service delivery relationships between citizens and government, it is important to re-examine what identity means and how it is operationalised in a digital context, as shown in the Aadhaar case study. The Customs Single Window case study highlighted the potential of platform-based governance, while the Smart Schools case noted the importance of learners and parents in ODG in the education environment. The Tech Hub and Maker Spaces case emphasised the potential role for these types of institutions in the development of open governance applications.

8. Case 1: Creating Digital Identity for All – Aadhaar, India

8.1. Relevance to South Africa

Open digital governance requires attention to technological changes that undergird and shape the expression of citizen–government relations, and the potential for shifting power relations that this may entail. Identity, as the basis for an individual's ability to interact with government, is essential in this regard. The identity of a person forms the basis for the recognition and establishment of credentials through which they can assert their rights and discharge their duties in contemporary society (World Bank, 2019). Identity is the foundation of citizen–government relations and serves as the basis for citizen access to services (Lips, 2010). The widespread proliferation of digital technologies throughout society and in government has also influenced approaches to the management of identity by government. The use of digital technologies in identity management has contributed to the emergence of digital identity, which refers to the set of digital data representing a person (Laurent et al., 2015) and is composed of information that is stored and transmitted in digital form (Sullivan, 2013).

The digital identification system established in India through the Aadhaar programme is the largest such undertaking in the world with 1.2 billion unique numbers, covering about 95% of the country's population (Gelb & Mukherjee, 2019), amounting to 16% of the world's population (Misra, 2019). This scale of enrolment was achieved over a period of ten years (Rao & Nair, 2019). The need for the establishment of a national identification system has its motivation in efforts to support inclusion and improved public service delivery, including through reducing fraud and corruption (Sen, 2019).

The establishment of the Unique Identification Authority of India (UIDAI) under the Ministry of Electronics and Information Technology in January 2009 with the mandate to create unique identities for all Indian residents was a key milestone in the rollout of the programme (Anand, 2021). Prior to the establishment of the programme, various identity documents (IDs) existed, such as the electoral identity card, the income tax PAN card, and the ration card, but these were limited in their coverage and unable to serve the entire population, with each created to serve a specific purpose requiring different sets of documents and verification processes (Sen, 2019). Under Aadhaar, a 12-digit unique identity number (UID) is issued to every resident by the UIDAI and is linked to their demographic information (name, address, date of birth and gender) and their biometric information (photograph, ten fingerprints and two iris scans), which is stored on a Central Identities Data Repository (CIDR) (Sen, 2019). Aadhaar is not a card; rather, the proof of identity is the number itself, which can be verified by any authorised body so that no physical identity proof is required (Misra, 2019).

8.2. Insights for South Africa

The Aadhaar number enables the bearer to engage in multiple transactions, rather than have multiple cards or forms of identification for each transaction. The overarching insights from the Aadhaar programme are the incredibly *strong mission orientation to achieve success on a digital innovation mega-project*, the significant digital capability unleashed with respect to the project, the digital leadership exercised and the capacity established for success, and the need for enabling policy and regulation upfront. Where these features are in place, the chances of success are increased. The weaknesses, risks and concerns expressed in the discussion on this case study will require understanding and attention, noting that innovation often brings inherent risks and requires risk mitigation measures. Related insights include an appropriate level of digital leadership and a platform design enabling value-added services and products. As a digital project in operation for more than ten years from inception, there is much to study, learn and understand in terms of strengths and weaknesses.

8.3. Digital Innovation and Technologies

One of the key design features of Aadhaar is the de-linking of the question of identity from that of a person's nationality so that all residents can be enrolled (Sen, 2019). This means that an applicant does not have to prove Indian citizenship when enrolled in the programme. Applicants must provide proof of residence for at least 182 days in the previous year since proving nationality could cause significant delay and exclusion. This approach can be described as an "identity-first" approach since it merely establishes identity that incorporates a minimal data collection process which makes the rapid scaling up of enrolment possible (Sen, 2019).

The system offers extensive interoperability as a universal identity gateway for all an individual's interactions with a diversity of state and private bodies (Rao & Nair, 2019). The system is designed as a digital platform with an hour-glass architecture (Singh, 2019). This design incorporates a simple and easy-to-use solution comprising the Aadhaar unique number for every individual and authentication services linked to this number as the waist,

while enabling innovation above and below. Importantly, UIDAI opted for an open scale-out architecture, rather than a scale-up design that relies on specific technologies from one vendor. The open scale-out architecture relies on standard off-the-shelf hardware from multiple vendors to avoid lock-in and the use of open-source technologies, unless there is no other option. The development of the system focused on controlling the software, digital spine and certification, and incentivised the ecosystem to provide IT products and services through the creation of a government-oriented market.

Enrolment is undertaken by registrars and enrolment agencies, enabling individuals to apply at enrolment centres where the required demographic and biometric information is provided (Misra, 2019). Registrars are UIDAI partners who usually outsource enrolment to UIDAI-certified agencies with enrolment centres or mobile camps (Sen, 2019). The information is then encrypted and transferred to the CIDR, through a Secure File Transfer Protocol where connectivity is available, or it is transferred on portable hard disks by post where the infrastructure poses challenges. The incoming data is checked for duplicates at the CIDR through a process of deduplication, after which a 12-digit Aadhaar number is randomly generated (Misra, 2019). An authorised body can cross-check an individual's identity at any time or place using different methods, including service delivery agencies using the Aadhaar authentication system for matching the number and the individual's demographic attributes; a one-time-password delivered to the individual's mobile number or email address; or using the biometrics, either iris or fingerprint (Misra, 2019).

Aadhaar has had a significant influence on inclusion, particularly financial inclusion and communication, linked to the opening of bank accounts and mobile phone subscriptions. People can use Aadhaar as a means of identification to open bank accounts. It enables banks and customers to fulfil know-your-customer (KYC) requirements (Gelb & Mukherjee, 2019) and has, together with schemes like the Prime Minister's People's Bank scheme, contributed to 80% of Indians holding bank accounts by April 2018 (Misra, 2019). Mobile phone subscriptions have increased from 17 per 100 inhabitants to 85 in 2016, approaching universal access, including a growing share of smartphones and Internet-enabled devices (Gelb & Mukherjee, 2019). The implementation of the Aadhaar Enabled Payment System (AEPS) encourages digital payment across banks with the rollout of the United Payment Interface enabling instant payments and money transfers between banks using the Aadhaar number linked to the bank account (Misra, 2019). A digital locker that serves as an online repository of documents that can be shared by individuals has been rolled out by the government; this digital locker links the Aadhaar number to the repository containing, for example, health records, drivers' licences and college mark sheets (Misra, 2019). Multiple schemes incorporating the public distribution of goods and government services make use of the Aadhaar authentication. The programme cost is one of the lowest in the world, with US$1.16 per enrolment made possible by a number of factors, including the absence of a smart card (Sen, 2019). Notwithstanding the aforementioned achievements, concerns have been growing about the forms of surveillance enabled by Aadhaar as an example of a socio-technical arrangement and how this might shape power relations between the citizen and the state (Henne, 2019).

8.4. Digital Skills and Capabilities

A mix of people from the public and private sectors were brought on board to implement the project, ensuring a balance of people with knowledge of the government ecosystem and technical expertise related to technological innovation (Misra, 2019). In addition to the founder, Nandan Nilekani, who started the technology company Infosys, others from India's technology sector included Pramod Varma as chief architect from Infosys; Viral Shah, co-inventor of the Julia programming language; Shankar Maruwada, CEO of Marketics; and Sanjay Swamy, CEO of mCheck. The negotiated status of Nilekani as that of a cabinet minister provided the impetus for him to drive an expedited agenda and hire private sector staff (Anand, 2021). The Aadhaar team was kept between 200 and 300, with much of the work outsourced and support obtained from other government departments. The UIDAI entered into Memorandums of Understanding (MoUs) with registrars, government departments and private organisations to establish the implementation infrastructure that made such a large-scale process possible (Rao & Nair, 2019).

8.5. Policy and Regulatory Issues

India's approach to the implementation of Aadhaar has been described as "build first and legislate later", with proponents arguing that it was the only way to move forward in the country (Gelb & Mukherjee, 2019). The UIDAI was established through executive order, rather than enabling legislation. Aadhaar was implemented in the absence of a framework for data protection and privacy regulation (Sen, 2019). A consultation paper on a Legal Framework for Data Protection and Security and Privacy Norms was issued in July 2010 and argued for a law beyond the mandate of Aadhaar covering e-governance issues and data sharing and privacy from third parties (Misra, 2019). The project continued without legislative foundations until the adoption of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (Aadhaar Act) in March 2016 and its publication in the *Gazette* of India in July and September 2016 (Bhandari & Sane, 2019). Since the passing of the Aadhaar Act, several regulations have been issued by the UIDAI related to regulating different aspects of the programme, including the process of enrolment; the generation of Aadhaar numbers and their delivery to residents; the updating of information; the appointment of registrars and enrolling agencies; the omission and deactivation of Aadhaar numbers; grievance redressal; the different modes of authentication; the specification of an information security policy that emphasises confidentiality, prescribes the security obligations of service providers and personnel, and provides for audit and inspection; and how identity information associated with the Aadhaar number holder can be shared with third parties (Bhandari & Sane, 2019). In a critical assessment of the legislative framework, Bhandari and Sane (2019) identified several weaknesses, including the delegation of policy matters and essential legislative functions to the UIDAI with wide discretion, the potential conflicts of interest arising from the UIDAI's dual role as administrator and regulator, the failure to provide specifics for grievance redress, and the uncertainty related to remedial measures.

8.6. Practical Ideas for South Africa

South Africa needs to re-examine the idea of identity, and express more clearly, in policy terms and in practice, how it understands identity. This is a conceptual issue where digital identity is quite different from analogue identity; it has little to do with a digitised card, and more to do with how a person establishes their identity for the purposes of living, acting and transacting in the world.

9. Case 2: Creating Enabling Platforms – The Digital Single Window for Cross-border Trade, China

9.1. Rationale

Open digital governance can be made possible through the design and operation of digital platforms, on a small scale or on a large scale. Platforms enable multiple government departments and citizens and residents to interact with each other, with ease and convenience, and with openness and transparency. One example of an area in which ODG can be of significant economic benefit to South Africa and South Africans is cross-border trade. See, for example, the discussion on the AU-NEPAD blog with respect to the benefits for women traders (https://www.nepad.org/blog/harnessing-emerging-technologies-enhance-cross-border-trade-systems-women-africa). We note that this is an exemplar case and that platforms can be designed as applicable to many digital governance contexts.

With respect to this case study, the digital single window is a platform that enables many entities to share information and data, and to enhance the efficiency of cross-border trade, noting that South Africa's global trade was estimated at ZAR3,2 trillion in 2021, of which 43% was imports and 57% was exports (tralac, 2021). This case study is relevant to the role of the DPSA, the CPSI and the GITOC in building ODG, because it illustrates how government platforms can benefit economic players, including small and micro-enterprises and large businesses. It offers a demonstration of the insight that the DPSA needs to shift its gaze beyond rules, to mainstreaming innovation in public service delivery through the use of platforms. The DPSA can also engage in fostering or facilitating an appropriate rule-based environment for the new innovative solutions, such as platforms. The digital single window for cross-border trade is just one context in which such a platform can be used. Another area for a single window application would be local government services, as part of smart city development, where ODG is necessary. The case study is therefore an exemplar of cross-governmental collaboration, a necessary dimension of ODG. It is also an exemplar of government–trader collaboration, noting that platforms can also be designed for government–citizen interaction.

9.2. Insights for South African Open Digital Governance

The overarching insights relevant to the South African public service are the following.

A 21st century public service requires mission, leadership and positioning: The case of China is interesting because it uses the digital single window to enhance trade with many countries in Asia and globally. This offers useful insights for South Africa with respect to

enhancing its trade with other African countries and globally. This is particularly important, given the commencement of the African Continental Free Trade Area (AfCFTA) in 2022, an as yet untested arrangement, which will require all African countries to employ innovative means for effective trade facilitation, revenue collection and cross-border security, including the digital transformation of customs administration. The open governance component of this endeavour relates to the need for extensive information to be made available to traders, particularly small, medium, young and women (SMYW) traders, who seek to engage in trade in the SADC region and on the continent, while traders can also express their needs and requirements. As South Africa is already engaged in the establishment of a digital single window as part of its customs modernisation programme, led by the South African Revenue Service (SARS), the DPSA, the CPSI and the GITOC can learn from the China/SARS experience, envisioning the design of platforms for public service innovation and ODG in other spheres of responsibility.

Digital skills and capabilities: Building platforms for public service innovation and ODG presents the opportunity for learning while innovating, and shared learning. Where the DPSA, the CPSI or the GITOC identifies an opportunity for creating a public service platform, it may consider that there are limited digital skills and capabilities in government to create such a platform. Typically, platforms will be designed by tech companies or tech start-ups, but the everyday operation of these platforms, including data analytics, would ideally be done by data analysts employed as public servants and those public servants who have domain-specific knowledge. This presents an opportunity for public servants to learn new skills and adaptiveness.

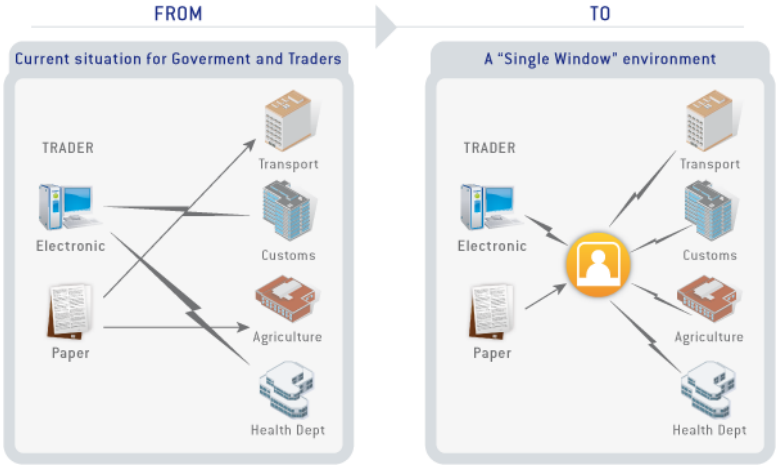
Legislation, regulatory frameworks and standards: The DPSA is responsible for the organisation and administration of the civil service, including standards-setting for the public service. Historically it has focused on quality of service standards, human resource-related standards, and public service ICT standards. While standards-setting will remain important, the DPSA must lift its gaze to consider other important public service standards, such as standards for efficiency, standards for good governance, standards that would facilitate innovation, and standards for open governance. Open governance is a component part of good governance and can be enabled by the design of digital platforms, noting that a shift to digital government is also a shift to creating forms of “government as a platform”. Building open governance, as a component of platform government, will require standards-setting.

9.3. Digital Innovation and Technologies: Overview of the Single Window Application

The digital single window is a recommendation of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), aimed at creating more efficient trade and more efficient trade analytics (see UNECE Recommendation 33 and the explanatory diagram from the UN Trade Facilitation Implementation Guide website at Figure 9.1 below).

Figure 9.1 Transitioning to a digital single window

(UNECE Recommendation 33)



Source: UN (no date)

China's single window model enables access to its platform for its own government agencies, the government agencies of trading partners, and foreign traders. Figure 9.2 below illustrates the structure of China's single window, a platform on which the many agencies responsible for trade, both Chinese agencies and those of China's trading partners, participate in border management and customs administration.

Figure 9.2: China's single window

Key: GACC – General Administration of Customs of the People's Republic of China; MPS – Ministry of Public Security MOT – Ministry of Transport; STA – State Tax Administration; SAFE – State Administration of Foreign Exchange

Source: World Customs Organisation (2019)

The single window enables inter-agency information sharing, port law enforcement and other basic services required for cross-border e-commerce, cross-border information exchange and data analytics services, with all agencies acting collaboratively. Twenty-five ministries and commissions, including cross-border regulatory agencies (CBRAs), participated in the design and implementation of the single window. Tasks included the design of business

norms, technical frameworks, specifications and standards to coordinate the functions of the China Single Window (World Customs Organisation, 2019).

The China Single Window offers a model to support the trade integration objectives of African countries, at the sub-regional level of SADC or SACU, and at the continental level through the AfCFTA. SARS is already working on the design and implementation of the single window for South African trade and customs modernisation. These efforts are complemented by a broader digital transition on the African continent, including the digital transformation of the trade finance systems, noting significant evolution in Africa's payments platforms and gateways (see Figure 9.3 below).

Figure 9.3 Platformisation for the cross-border trade and e-commerce environment

Source: Briter Bridges (2022a)

The single window is an integrated platform that uses DLT and non-distributed ledger technologies, in a tech development ecosystem. This ecosystem includes technological infrastructure and protocols that enable simultaneous access by multiple government entities, as well as validation of trading data and required record updates, thus promoting high levels of compliance with applicable regulations and the payment of border taxes, while creating an efficient trade environment. We are not concerned here with a detailed breakdown of the underlying technologies. The point is that where a government department or entity undertakes a digital innovation or digital transformation exercise, it is either (i) highly likely that digital advancement is taking place in other parts of the same ecosystem; or (ii) it is necessary that the relevant government department or agency should constantly be studying and reviewing the digital transformation signals and trends in its domain of operation, in order to leverage the opportunities available for its own transformation to greater efficiency and greater openness. In this case, the signals and trends indicate that

platform-based government is desirable in some spheres of governmental operation. Furthermore, platform-based government offers opportunities for open governance because there is such a vast amount of data that can be shared for the benefit of citizens in general, and in this case for SMYW traders in particular. Furthermore, platforms enable information-sharing in both directions, from government to citizen and from citizen to government.

9.4. Digital Skills and Capabilities Relevant to Platform-based Governance

In the case of the China single window for international trade facilitation, this mega undertaking required new skills and new mindsets, much of this acquired during the course of the project. In particular, skills and capabilities are required for technical engineering of the platform including DLT and AI applications design, as well as for understanding the operation of the new business models, content development and data analytics, and for the appropriate design of policy, law and regulation, as well as compliance with laws and regulations. Introducing digital platforms for more effective public service delivery, enhanced by open governance, requires public service administrators to focus on intentional skills building exercises, in collaboration with the line departments, whether this relates to the specific case of customs modernisation, or to the more general need to build platform-based open governance.

The DPSA is concerned with building public service skills, noting also its promotion of these efforts through the National School of Government. Similarly, the GITOC is concerned with having access to high quality digital skills for building digital government. Furthermore, the Department of Communications and Digital Technologies (DCDT) is concerned with building digital skills for the country, including the public service, as set out in the National Digital and Future Skills Strategy adopted by Cabinet in 2020. Such skills and capabilities can best be built during the course of work on a particular large or mega-project, because there is a real requirement to learn new skills and to adopt new mindsets. These departments and government entities can learn from observing the customs modernisation platform environment at SARS, while also learning from other country case studies, such as the China single window case.

9.5. Policy and Regulation for Open Digital Trade Governance

Government agencies and traders (importers and exporters) need to interact with each other to facilitate compliance with trade regulations and to ensure the payment of applicable customs duties and fees. Laws and regulations must be developed for the implementation of the platform, clarifying which of the many agencies will be the lead agency and setting out the regulatory environment for open governance. The following statement is important in this regard (Jiang, Zhang & Jin, 2021, p. 140):

> The [five-year] plans are conducive to creating a benign and *open* e-commerce environment. The plans propose to optimize the governance environment of e-commerce, emphasizing the need to strengthen the construction of e-commerce information infrastructure, and t*o implement effective supervision based on internet technology regulations and law*. The development of e-commerce needs to reinforce industry guidance and create a healthy and *open environment*. The development of e-commerce also needs to abide by the basic principles of equal emphasis on competition and co-

> ordination, adhere to the promotion of fair market competition and *open development*, prevent and suppress monopolistic and vicious competition, and establish an *open, fair and honest market* order through supervision. (Our additions in brackets and our emphasis.)

Regulatory issues that are prominent when focusing on platform-based government, noting again that platforms are particularly enabling of open governance, include personal data protection, because there will be huge volumes of personal data, and cybersecurity regulation, because there is significant risk of cyber-attack. Furthermore, in the trade environment specifically, where financial regulations and regulatory compliance need attention, regulatory technologies (regtech) and supervisory technologies (suptech) can be introduced to effectively reduce e-commerce and financial risk. In the case of cross-border trade and e-commerce, new fintech solutions are being used, giving even more reason to use automated and standardised regulatory approaches enabled by technology, since the quantity of data is too vast for humans to manage. While this applies in the cross-border e-commerce and trade environment, it is relevant in all platform-based environments.

9.6. Practical Ideas for South Africa

The DPSA will need to (i) consider the opportunities for platform-based government in the public service in line with its mandate to focus on the administration and organisation of the civil service; and (ii) shift from a purely generic approach to the administration and organisation of the civil service to an approach that understands the particular dynamics of the particular segments of the civil service. This is made as a practical suggestion because the need to strengthen ODG requires the DPSA, the CPSI and the GITOC to look for the specific opportunities where such openness and such governance can benefit South Africans and the South African economy.

10. Case 3: Digital Bilingualism and 21st Century Skills – Malaysia Smart Schools

10.1. Rationale

Open digital governance requires young citizens to have the skills and capacities to engage with government, in relation to politics and elections, policy and development practice, health and employment, and general public service advancement. In the 21st century, open governance requires a combination of digital skills and 21st century skills, often referred to as digital bilingualism. In this respect, it is necessary to give attention to the transition to and operation of smart schools, in which teachers and learners prepare each other for work and life in a digitally enabled society. Twentieth century education systems are highly bureaucratised to the extent that many, including in South Africa, do not encourage openness, collaboration and innovation. These systemic weaknesses mean that teachers follow a rubric set by administrators and learners follow a rubric set by teachers and administrators, limiting knowledge-sharing to a narrowly defined curriculum with an emphasis on minimum requirements, rather than opening up knowledge-sharing for effectively operating in the world of work and in life. Furthermore, there is limited actual teaching and learning with dynamic or interactive software applications.

10.2. Insights for South African Open Digital Governance

The overarching insights relevant to the South African public service are the following.

A strong 21st century mission orientation: In the case of Malaysia, the mission has been enduring for 25 years. When engaged in a mission, such as the transformation of a major embedded system, in this case, studying an education system, then every moment, every day, every week, every year is precious and novel approaches must be consistently introduced and nurtured in order to achieve success. In cases where a purely or mainly technological approach is taken, unmatched by human creativity and human ingenuity, then system change will be slow, costly, inefficient and unattractive to the participants. System change is as much about institutional culture change as it is about technological change. In relation to this case study, the dialogue can reflect on the techno–human impetus of change.

The 21st century mission orientation must be matched by an equally strong future orientation, in the sense that the goals and objectives are achieved. In the case of Malaysia, the mission is to build a 21st century workforce with strong innovation-based capacity. In the case of ODG in South Africa, this relates to the importance of enabling future generations of young South Africans to participate effectively in political, social, economic and institutional governance.

10.3. Smart School Innovations and Technologies

The early stages of the development of Malaysian smart schools (in the early 2000s) saw the use of TV, VCRs and radio to access educational content (El-Halawany & Huwail, 2008). This is important because it introduces the importance of frugal innovation in a social context. Since a major focus of public services is precisely those social contexts that are poorly resourced, the introduction of relatively low-cost media for educational content is a breakthrough in thinking about education. Furthermore, it would be necessary to interpret educational content more broadly than curriculum content, or textbook-related content. This is the mindset shift that Malaysia made when introducing such practical technologies in schools.

In their analysis of Malaysian smart schools, El-Halawany and Huwail (2008, p. 122) state that “ICT in education has become tools and enablers to make learning more interesting, motivating, stimulating and meaningful to students”. We can add an important dimension to this, namely, the availability of dynamic software applications, for example, Excel, Geometer’s Sketchpad and GeoGebra for mathematics teaching and learning. These visual tools enable the learner to observe the dynamic nature of change in variables, equations, graphs and shapes (amongst others) and therefore to understand the nature of mathematics and engage with mathematics as something useful in the real world, in their world.

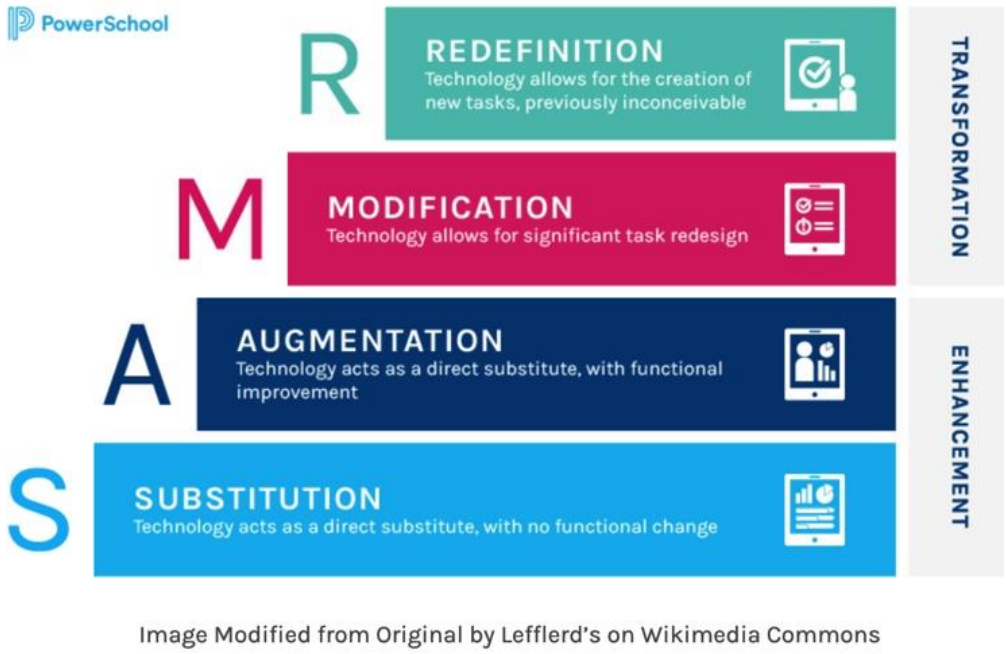
Equally important is the range of dynamic software available for language learning, meaning that learners can learn the required South African languages, including those that are not their home language, with greater speed and success than when always requiring a teacher to be present. These examples of dynamic maths software and language learning software,

and the availability of software for many other subjects, points to the opportunity for introducing digital bilingualism at an early age, in other words, whatever the specific task is eg. language learning, learners can also learn about the digital tools and approaches that enable such language learning. The learner learns the language and acquires knowledge of the digital tools required to continue learning and improving.

10.4. Smart School Pedagogy, Digital Skills and Capabilities

Puentedura (2006) observes that the levels of integration of digital technologies into educational process and practice can be viewed at four levels, namely simple substitution of the textbook; augmentation of the learning process; modification of teaching, learning and assessment; and redefinition including learning in new ways, as below:

Figure 10.1 SAMR model relevant to digital innovation in schools

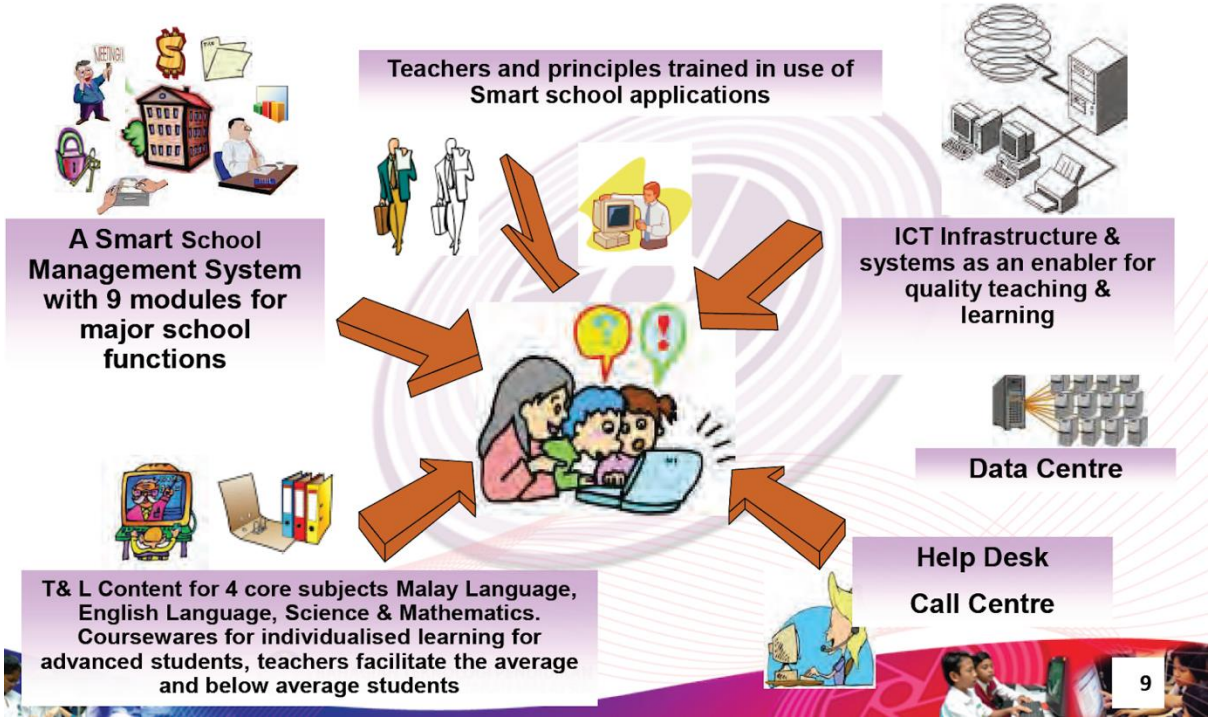


Source: PowerSchool (no date)

The SAMR model shows that teaching and learning can and should operate at all four levels, and should not operate only at the level of substitution. Trends in digitally-enabled education show another key requirement, namely to give attention to skills that complement digital skills, expressed as 21st century skills (Van Laar et al., 2017). These include seven core skills (technical, information management, communication, collaboration, creativity, critical thinking and problem solving) and five contextual skills (ethical awareness, cultural awareness, flexibility, self-direction and lifelong learning). In the case of Malaysia, they reinterpreted this as "technology and media literacy … learning and innovation skills … life and career skills" (KPM, no date, slide 14).

Malaysia and South Africa have adopted the paradigm of 21st century skills. Malaysia argues that "[w]e are examining our education system to create a curriculum where people learn how to learn so they can continue their education throughout the rest of their lives. The measure of success in 2020 will be the number and quality of people who can add value to information" (KPM, no date, citing Mohamad, 1996). This statement reflects on the importance of pedagogical thinking, the *how* to learn, rather than simply the *what* to learn. In other words, technologies must enable the how, not only the what. The Malaysian smart schools project was founded on an understanding of digital pedagogy that saw the need for "different skills" for a "different economy", acquired through "different learning". Figure 10.2 below illustrates the redesign of schools, with multiple inputs, with digital infrastructure as an enabler, but not the only focus. Of these inputs, one of the most important is the training in smart school applications. It is the applications that enable change. It is also the applications that will create opportunities for ODG in schools, where teachers, parents and learners can become "communities of education" through the use of online parent–teacher engagements (reinventing the old meeting), school blogs and other media for open dialogue.

Figure 10.2 The importance of applications and school redesign



Source: KPM (no date), slide 9

10.5. Smart School Policy and Regulatory Issues

The move to digitally enabled teaching and learning raises the same risks and concerns as in other areas of digital adoption, namely the protection of personal data and cybersecurity risks. In the case of schools, it also raises risks of exposure to harmful content and cyberbullying. While all these issues can be addressed at the level of the education department, it is possible to put a set of model guidelines in place for the civil service, which

the education department can build on with respect to education, and that other departments can build on with respect to their mandates.

More importantly, the way to manage the protection of personal data and cybersecurity is not to avoid going digital; instead, it is to manage going digital through effective policy innovation and regulation. The European Union GDPR seeks to encourage digitalisation in its domain and introduces regulation in order to make digitalisation possible and sustainable. Similarly, the Protection of Personal Information Act (POPIA) of South Africa is aimed at protecting those who engage in the digital economy.

10.6. Practical Ideas for South Africa

The DPSA and the CPSI can partner with departments to consider opportunities for ODG, on the understanding that ODG can only evolve if there is digital innovation in public services. For example, if you are not creating smart schools, you cannot create ODG, as there would be no digital medium available for learner and parent interaction with teachers and with school management. Imagine a basic education system in which parents can communicate online with education district authorities, such as maths subject advisors. That would require a very different mindset and a different set of relationships amongst the stakeholders, with a shift to seeing learners and parents as the major stakeholders in ODG, not as the recipients of education. Furthermore, such culture change is very long-term and multi-generational. Intensifying the work on public service innovation in education and the related requirements for ODG can benefit successive generations even more than the current generation, but that means we must start now.

11. Case 4: Building Software (Applications, Platforms, Services) for Open Digital Governance – Relationships with Tech Hubs and Maker Spaces

11.1. Rationale

Open digital governance requires a sizeable and continually evolving tech ecosystem which uses the innovative capabilities of developers and programmers, and of tech start-ups and new tech entrepreneurs, in addition to the resources and capabilities of the more conventional hi-tech firms. We highlight three reasons why this is a requirement: (i) technopreneurs are mostly young and have powerful ideas about the future that they wish to co-create; (ii) technopreneurs are keen to produce open source software because they are continually creating new applications; and (iii) technopreneurs are often in a position to offer frugal innovation approaches, which is not common with conventional hi-tech firms. Budgeting for applications for ODG will take place in the context of major financial constraints since the public sector already spends over R30 billon per annum on ICT-related goods and services. Incorporating technopreneurs, their tech start-ups and tech hubs in the design and delivery of ODG is therefore important for managing the risk of weaknesses in the tech development ecosystem.

11.2. Insights from African Tech Hubs for Open Digital Governance

The overarching insights relevant to the South African public service arising from this African tech hubs case study are the following.

Taking a digital-first approach: Tech hubs and maker spaces are at the forefront of digital innovation on our continent and in South Africa, and they offer the opportunity for a digital-first approach to fostering ODG. In other words, when seeking an approach to advancing governance, it is generally useful to consider whether a digital solution would be appropriate. In particular, a digital-first approach to governance would require attention to open data models (open to developers) and the related matters of personal data protection.

Digital skills and human capability: Tech hubs and maker spaces offer a pool of digital skills and entrepreneurial capability that are well suited to the kind of open social innovation required in the sphere of public service governance.

Future orientation: Tech hubs and maker spaces have a strong future, problem-solving orientation and a forward-looking culture and practice, which would be beneficial to government efforts to foster and strengthen ODG.

11.3. Digital Technologies and Innovation Spaces

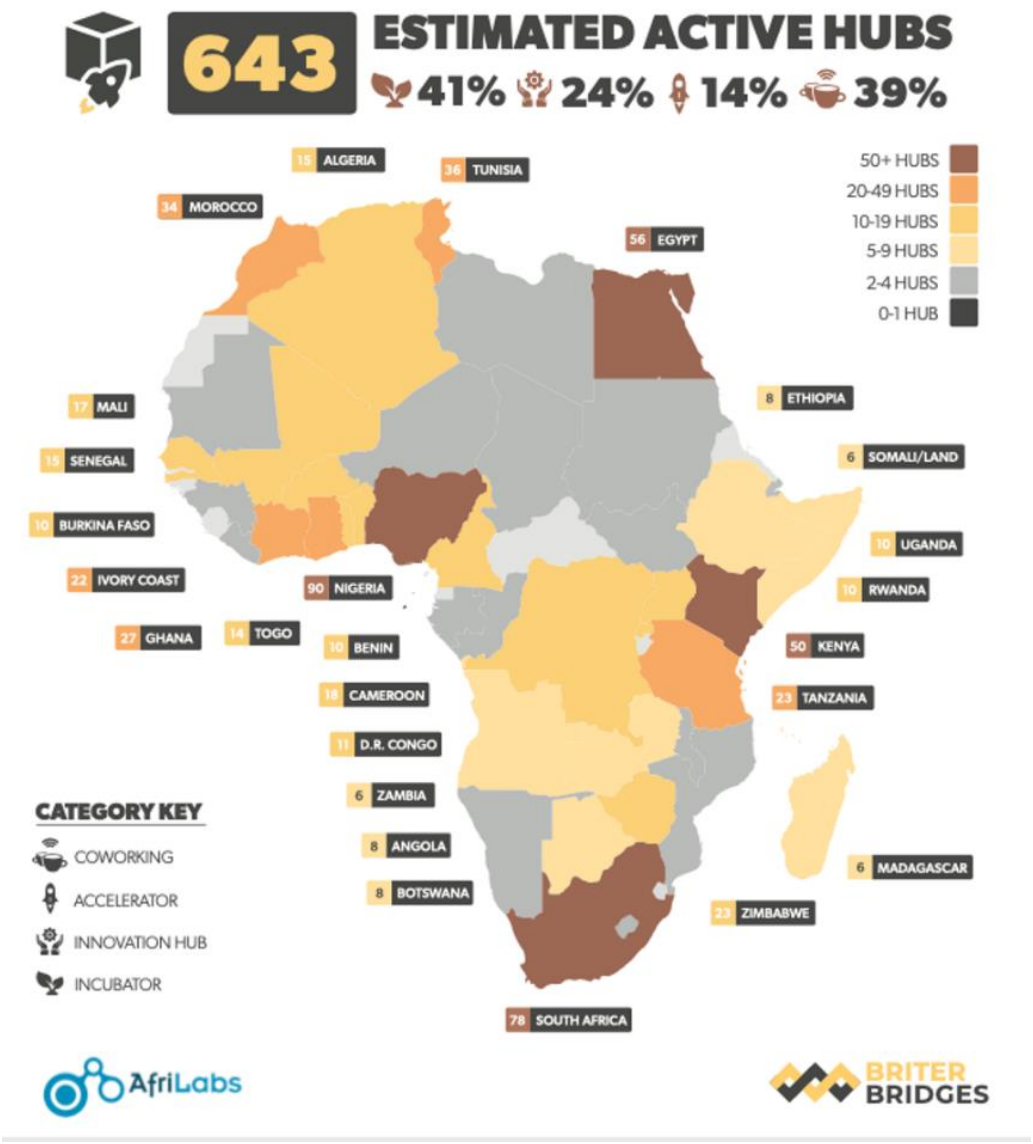
In 2019/2020, more than 643 active tech hubs in Africa were hosting more than 4,265 tech start-ups, with investment of USD453,7 million (see Figure 11.1 and Figure 11.2 below). Some of the hubs are collaborative working spaces (where technopreneurs and small tech-enabled businesses gather and share space and knowledge), some are incubators (designed to foster tech start-ups), some are accelerators (designed to enable tech start-ups to move from being fledgling businesses to sustainable operations), and some are innovation hubs (designed to aggregate digital and related innovation capacity). Many tech hubs include maker spaces, also referred to as FabLabs (fabrication laboratories) or TechShops, where small and micro-scale digitally-enabled manufacturing takes place, using technologies such as 3D-printers and liquid 3D-printers, computer-aided design (CAD) software, computer numeric control (CNC) laser-cutters, and other digital technologies that create a physical artefact or product for sale (Kraemer-Mbula & Armstrong, 2017, pp. 5–6). In some cases, maker spaces are standalone innovation spaces. A few tech hubs incorporate all of the above forms of innovation space.

In South Africa, in 2019/2020, more than 78 tech hubs were hosting more than 700 start-ups with investment of approximately USD241 million, more than half the total investment for the 26 countries mapped in the Briter Bridges (2022b) report. Data from this report and from other research (Abrahams, 2021; Adesida et al., 2021) indicates that South Africa has a relatively large and maturing tech hub ecosystem with which all spheres of government can engage. In the past 15 years, tech hubs have emerged as a common phenomenon in a large number of countries globally, meeting the demand for hi-tech innovation for corporate clients, as well as quality low-cost innovation for social services. An example of the latter is the Pelebox smartlocker designed by Technovera, which is located at the Tshimologong

Digital Innovation Precinct in Johannesburg (see https://www.pelebox.com/locker.html). The Internet-based smart locker design enables patients to collect repeats of their chronic medication in under two minutes, avoiding queues.

With respect to emerging technologies and their beneficial use, Nigeria offers a number of powerful examples. Adesida et al. (2021) reference various reports and publications that provide data that Nigeria is a major tech hub and tech start-up environment. In 2021, start-ups from the ed-tech and e-health sectors participated in the Nigeria–UK Tech Hub iNOVO accelerator programme, promoting digital solutions relevant to communities during the COVID-19 pandemic, and with value beyond the pandemic (Jackson, 2021). With regard to social services, the ed-tech companies are Afrilearn (curriculum-relevant video lessons combined with gamified exam practice), DigiLearns (an AI-based mobile adaptive learning tool that operates via SMS or USSD and offers ease of access); and Schoola (multilingual, gamified learning solution that uses AI for content generation). The e-health start-ups are Gleeworld Pharmacy (a telepharmacy and medication delivery platform), Pharmaserv Health Project (a platform that enables healthcare providers to procure essential medicines efficiently), and Wellvis (which provides telemedicine consultations on a pay-as-need basis) (see https://disrupt-africa.com/2021/03/08/10-nigerian-tech-startups-selected-for-inovo-accelerator/). These are just a few examples of socially-oriented innovation in a sustainable and growing tech hub ecosystem.

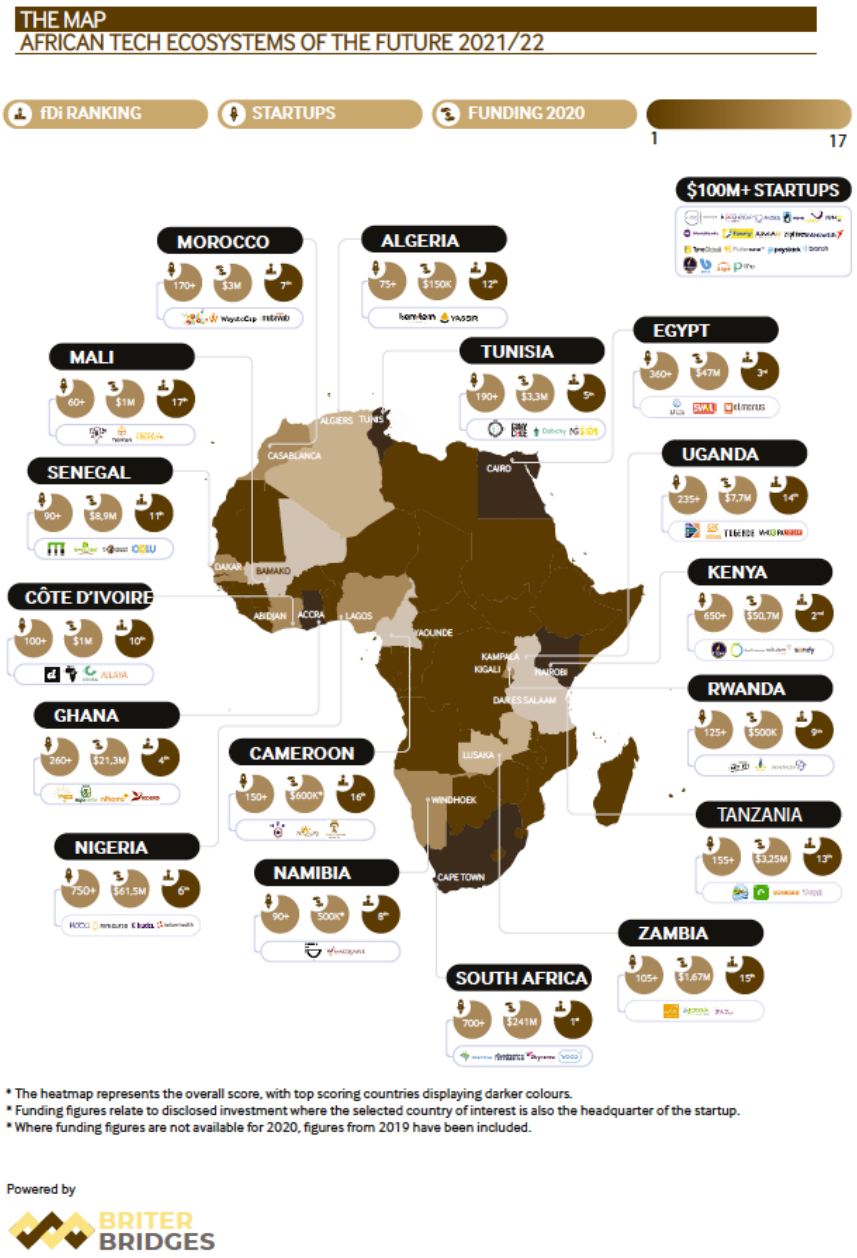
Figure 11.1: 643 African tech hubs



Source: AfriLabs and Briter Bridges (2019, p. 6)

The map below, Figure 11.2, shows the levels of funding to African tech hubs today, illustrating significant opportunities to increase the size of funding and revenue into this landscape, in ways that produce innovative services. With regard to the subject of this SA–EU dialogue, such services can also include applications, platforms and other solutions to strengthen ODG.

Figure 11.2 Funding levels and insights into the African tech hub ecosystem



Source: Briter Bridges (2022b)

African tech hubs, and tech hubs more widely, have demonstrated frugality at two levels: (i) in relation to the relatively low costs associated with the design of the innovation spaces, enabling them to keep the costs of use low for the technopreneur community; and (ii) tech hub community members often provide their services at a lower cost to clients than does the corporate sector. While clients should always be required to pay fair prices for services at tech hubs, the main challenge of tech hubs and their hosted start-ups today is that they need more clients. Government and society can benefit significantly from being clients to tech hubs, recognising their value and pushing forward the demand and supply relationship, to mutual benefit.

While South Africa ranks highest on the overall index for African tech ecosystems of the future (Briter Bridges, 2022b, p. 33), it can learn from Morocco with respect to tech hub connectivity; from Cairo, Egypt with respect to foreign direct investment (FDI) strategy; from Tunisia and Namibia with respect to cost-effectiveness (including frugality); from Kenya, Ghana and Tunisia with respect to human capital and lifestyle; and from Nigeria, Kenya and Egypt with respect to start-up status; amongst others.

Governments can connect into this tech hub ecosystem (at country level and at continental level) in order to make their particular problems, challenges and requirements top of mind, and to focus the innovation potential of tech hubs and their hosted start-ups on applications relevant to ODG. Since digital technologies, particularly AI-enabled solutions, are suitable for collecting extensive data, they lend themselves well to designing applications that enable users to contribute to successive versions of these applications, with continual improvement. Connecting into the tech hub ecosystem requires the client organisation to design open data approaches, even if this means partially open data models, with the data being open to the developers. This is necessary for designing and building applications or platforms with data analytics capabilities, including health analytics, trade analytics, modelling and other data science capabilities. It is important to note that cybersecurity and personal data protection matters are important in relation to any of these innovations and ventures where there is a risk to humans greater than what they would ordinarily experience. Hence, specific cybersecurity and data protection measures, such as data anonymisation, must be incorporated into open data models, applications, platform and services design.

11.4. Digital Skills and Capabilities

One of the main value propositions of African tech hubs is their ability to harness the skills of technopreneurs in ways that increase the size of the pool of human resources with respect to digital skills and to aggregate the capabilities at easy-to-reach innovation spaces. They provide an environment in which clients for digital innovation can find a match between skills, technologies, digital innovation and entrepreneurial capabilities, on the one hand, and their particular problem or need for solutions, on the other hand. They represent a sizeable talent pool for African countries, relevant to creating their own start-ups, but more importantly, relevant to making a significant contribution to digital innovation for social and economic impact. The significant value of tech hubs is that they provide powerful spaces for knowledge sharing and collaborative innovation (Abrahams, 2021), meaning that technopreneurs and developers team up to achieve the goals set by clients.

11.5. Policy and Regulatory Issues Relevant to Tech Hubs and Tech Start-ups

The digital innovation space can be supported by policies, such as the Digital Economy Blueprint: Powering Kenya's Transformation (Republic of Kenya, 2019); the National Digital Economy Policy and Strategy 2020–2030: For a Digital Nigeria (Federal Ministry of Communications and Digital Economy, 2019); and the National Digital and Future Skills Strategy: Originality, Agility, Critical Thinking and Problem-Solving for Digital Inclusion (Republic of South Africa, 2020). These policies provide the context in which tech hubs are understood to have transformative agency. However, greater attention must be given to

other components of the policy and regulatory environment by government and by regulatory entities, including attention to (i) measures to support tech hubs and their hosted start-ups in respect of compliance with legislation and regulation, such as that for personal data protection, tax compliance and other legal requirements; and (ii) of particular importance to the DPSA, actions to amend the National Treasury Regulations in order to do business with tech hubs and/or their hosted start-ups. While private and commercial firms operate within their own guidelines with respect to doing business with tech hubs or tech start-ups, National Treasury Regulations would, for example, require a tech start-up to have a Central Supplier Database (CSD) number and report in order to do business. This requirement could be amended to require the government department entering into a client relationship with a tech hub or tech start-up to assist the entity in getting registered, providing the relevant information and facilitation. Compliance and facilitation are equally important to creating the foundations for greater engagement between government bodies and tech hubs or tech start-ups. In other words, compliance can be fostered, rather than the absence of a particular document or documents being used to exclude participation or engagement. While this particular point is not exclusive to ODG, it is an important component of the ecosystem that would drive a shift to ODG.

11.6. Practical Ideas for South Africa

South Africa has more than 700 tech start-ups, located at more than 60 tech hubs and other spaces, and it has 153 Thusong Service Centres across its nine provinces (https://www.gov.za/about-government/contact-directory/thusong). The tech hubs offer distinct types of opportunities, different from the services orientation of Thusong Service Centres. Nevertheless, their different approaches present the opportunity for some level of pairing. For example, the Genesis YES tech hub (https://www.facebook.com/GenesisYouthHub/) in Louwville, Vredenburg, the Hopefield (satellite) Thusong Centre and the Langebaan Thusong Service Centre are in relatively close proximity to each other, less than 30km apart. Here lie opportunities for developers, technopreneurs, start-ups and tech hubs to provide open governance applications to citizens through these centres.

12. Insights for South Africa

The review of a few global trends in ODG and the international case studies presented offer a wide range of insights for South Africa, including but not limited to the five overarching insights presented in the introduction and in Figure 7.1.

From the perspective of being mission-driven and positioning institutions for public service innovation and ODG, it is apparent that digital government needs to take centre stage in policy and institutional configurations if the ambitions for ODG are to become a reality. Digital government should be embedded and mainstreamed in policies and strategies across the sectors and spheres of government, creating the foundation to achieve public service innovation and ODG. For instance, ODG could be integrated into the Socio-economic Impact Assessment System (SEIAS) used in South Africa as a criterion to assess the value of new

policy proposals, strategies and governmental programmes. In this way, ODG can become embedded in the practice of policy, strategy and programme development by government.

Furthermore, sustained and effective leadership is required to promote public service innovation and ODG across government. In particular, from the perspective of transforming to data-driven public services, the curation of data and the governance thereof must become a policy priority, through the creation of fit-for-purpose data governance frameworks that promote investment in data generation, standards, tools, infrastructures and capabilities. Such a leadership approach can harness the power of data for developmental purposes. From the perspective of fostering the required human capability for ODG, South Africa needs to accelerate its Implementation Programme for the National Digital and Future Skills Strategy. The focus here is on advancing digital and 21st century skills and capabilities in government side by side with capabilities in schools, communities and society at large so that ODG can take effect. From the perspective of an enabling legislative and regulatory environment, it is necessary to speed up the formulation and adoption of regulation fit for the digital society, including privacy protection, data protection and cybersecurity measures. From the perspective of a future orientation to ODG, it is necessary to anticipate the disruptive implications of general-purpose technologies, notably AI and Big Data. The whole of government, in particular the DPSA and the GITOC, must play a leading role in transitioning to ODG with an eye to benefits for economic growth and democracy, while simultaneously understanding and addressing the associated risks.

References

Abrahams, L. (2021, December 16). *Innovation and scaling by tech hubs and their hosted startups: Three South African cases*. Open AIR Working Paper 26. https://openair.africa/innovation-and-scaling-by-tech-hubs-and-their-hosted-startups-three-south-african-cases/

Adesida, O., Karuri-Sebina, G., & Thaver, K. (2021). Strengthening innovation ecosystems in Africa: Seeking out the systemic changes in the wake of COVID-19.

African Union Development Agency (AUDA-NEPAD). (2021, December 7). Harnessing emerging technologies to enhance cross-border trade systems for women in Africa. https://www.nepad.org/blog/harnessing-emerging-technologies-enhance-cross-border-trade-systems-women-africa

Afrilabs & Briter Bridges. (2019, October). *Building a conducive setting for innovators to thrive: A qualitative and quantitative study of a hundred hubs across Africa*. https://briterbridges.com/briterafrilabs2019

Anand, N. (2021). New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management. *Journal of Science Policy & Governance 18*(1). https://doi.org/10.38126/JSPG180101

Barcevičius, E., Cibaitė, G., Codagnone, C., Gineikytė, V., Klimavičiūtė, L., Liva, G., Matulevič, L., Misuraca, G., & Vanini, I. (2019). *Exploring digital government transformation in the EU*. European Union. http://doi.org/10.2760/17207

Bhandari, V., & Sane, R. (2019). A critique of the Aadhaar legal framework. *National Law School of India Review, 3*(4), 72–97. https://nlsir.com/wp-content/uploads/2020/07/Vrinda-Bhandari-_-Renuka-Sane.pdf

Bekkers, V., & Homburg, V. (2005). E-Government as an information ecology. In V. Bekkers & V. Homberg (Eds.). *The information ecology of e-government*. IOS Press.

Bibri., S. (2019). The anatomy of the data-driven smart sustainable city: Instrumentation, datafication, computerization and related applications. *Journal of Big Data*, *6*(59). https://doi.org/10.1186/s40537-019-0221-4

Briter Bridges. (2022a, February 2). Payments landscape in Africa. https://briterbridges.com/stories/2022/1/20/product-insights-series-payments-landscape-in-africa

Briter Bridges. (2022b). *African tech ecosystems of the future 2021/22*. https://www.jengalab.org/en/2021/the-first-african-tech-ecosystems-of-the-future-2021-22-report-sheds-lights-on-the-continents-start-ups-and-techpreneurial-landscape/

Castells, M. (2013). *Communication power*. Oxford University Press.

Chignard, S. (2013, March 29). A brief history of open data. *Paris Innovation Review*. http://parisinnovationreview.com/articles-en/a-brief-history-of-open-data

Chui, K., Liu, R., Lytras, M., & Zhao, M. (2019). Big data and IoT solution for patient behaviour monitoring. *Behaviour & Information Technology*, *38*(9), 940–949. http://doi.org/10.1080/0144929X.2019.1584245

Clarke, A. (2020). Digital government units: What are they, and what do they mean for digital era public management renewal? *International Public Management Journal*, *23*(3), 358–379. http://doi/org/10.1080/10967494.2019.1686447

Custers, B., Sears, A., Dechesne, F., Georgieva, I., Tani, T., & Van der Hof., S. (2019). *EU personal data protection in policy and practice*. T.M.C. Asser Press.

Dener, C., Nii-Aponsah, H., Ghunney, L., & Johns, K. (2021). *GovTech Maturity Index: The state of public sector digital transformation*. International Development in Focus. World Bank. http://doi.org/10.1596/978-1-4648-1765-6 and https://www.worldbank.org/en/events/2021/09/16/govtech-maturity-index-the-state-of-digital-transformation-in-the-public-sector

Dunleavy, P., Margetts, M., Bastwo, S., & Tinkler, J. (2006). *Digital era governance: IT corporations, the state, and e-government*. Oxford University Press.

Dunn, W. (2018). *Public policy analysis: An integrated approach*. 6th Edition. Routledge.

El-Halawany, H., & Huwail, E. I. (2008). Malaysian smart schools: A fruitful case study for analysis to synopsize lessons applicable to the Egyptian context. *International Journal of Education and Development using Information and Communication Technology*, *4*(2), 117–143. http://ijedict.dec.uwi.edu/viewarticle.php?id=447

Engin, Z., & Treleaven, P. (2018). Algorithmic government: Automating public services and supporting civil servants in using data science technologies. *The Computer Journal*, *62*(3), 448–460. https://doi.org/10.1093/comjnl/bxy082

European Commission. (2017). New European Interoperability Framework: Promoting seamless services and data flows for European public administrations. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf

European Commission (EC). (2019). *Data protection rules as a trust-enabler in the EU and beyond – taking stock*. Communication from the Commission to the European Parliament and the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374&from=EN

European Commission (EC). (2020). *A European strategy for data*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

European Commission (EC). (2020a). The *EU's cybersecurity strategy for the digital decade*. Joint Communication to the European Parliament and the Council. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission (EC). (2020b). *Data governance and data policies at the European Commission*. https://ec.europa.eu/info/sites/default/files/summary-data-governance-data-policies_en.pdf

European Commission (EC). (2022). Proposal for a regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act). https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

Federal Ministry of Communications and Digital Economy. (2019, November). *National digital economy policy and strategy 2020–2030: For a Digital Nigeria*. https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file

Fountain, J. (2001). *Building the virtual state: Information technology and institutional change*. Brookings Institution Press.

Franceschetti, D. (2018). *Principles of robotics & artificial intelligen*ce. Grey House Publishing.

Gelb, A., & Mukherjee, A. (2019). *Building on digital ID for inclusive services: Lessons from India*. Centre for Global Development Note Sep 2019. https://www.cgdev.org/sites/default/files/building-digital-id-inclusive-services-lessons-india.pdf

Giest, S. (2017). Big data for policymaking. *Policy Science*, *50*, 367–382. http://doi.org/10.1007/s11077-017-9293-1

GIP Digital Watch. (no date). Digital standards. https://dig.watch/topics/digital-standards

Hajer, M., & Wagenaar, H. (2003). Introduction. In M. Hajer & H. Wagenaar (Eds.). *Deliberative policy analysis: Understanding governance in the networked societ*y. Cambridge University Press.

Hassan, R. (2009). *Empires of speed: Time and the acceleration of politics and society*. Brill.

Held, D., McGrew, A., Goldblatt, D., & Perraton, J. (1999). *Global transformations: Politics, economics and culture*. Stanford University Press.

Henne, K. (2019). Surveillance in the name of governance: Aadhaar as a fix for leaking systems in India. In B. Haggart, K. Henne, & N. Tusikov (Eds.) *Information, technology and control in a changing world*. International Political Economy Series. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-14540-8_11

Ingram, G., & Dooley, M. (2021). *Digital government: Foundations for global development and democracy*. Brookings Global Working Paper No. 163. https://www.brookings.edu/wp-content/uploads/2021/12/Digital-government.pdf

Jackson, T. (2021, March 8). 10 Nigerian tech startups selected for UK-Nigeria Tech Hub iNOVO accelerator. Disrupt Africa. https://disrupt-africa.com/2021/03/08/10-nigerian-tech-startups-selected-for-inovo-accelerator/

Janowski, T. (2015). Digital government evolution: From transformation to contextualisation. *Government Information Quarterly*, *32*(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Janssen, M., Wimmer, M., & Deljoo, A. (Eds.) (2015). *Policy practice and digital science: Integrating complex systems, social simulation and public administration in policy research*. Springer.

Jiang, Y., Zhang, L., & Jin, Y. (2021). China's e-commerce development and policy relevance. In M. Sweets (Ed.). *Adapting to the digital trade era: Challenges and opportunities*. World Trade Organisation. https://www.wto.org/english/res_e/booksp_e/10_adtera_chapter_06_e.pdf

Kassen, M. (2022). *Open data governance and its actors*. Palgrave Macmillan.

Kementerian Pendidikan Malaysia (KPM). (no date). The Malaysian smart schools: Developing 21st century skills. [JAET Presentation]. http://www.jaet.jp/katudou/seminar_ict/Malaysia.pdf

Kooiman, J. (2003). *Governing as governance*. Sage Publications.

Kraemer-Mbula, E., & Armstrong, C. (2017). *The maker movement in Gauteng Province, South Africa*. Open AIR Working Paper 6. Open African Innovation Research (Open AIR) network. https://openair.africa/the-maker-movement-in-gauteng-province-south-africa/

Kuner, C., Bygrave, L., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford.

Laurent, M., & Bouzefrane, S. (2015). *Digital identity management*. ISTE Press Ltd.

Lips, M. (2010). Rethinking citizen–government relations in the age of digital identity: Insights from research. *Information Polity*, *15*, 273–289. http://doi.org/10.3233/IP20100216

Lips, M. (2020). *Digital government: Managing public sector reform in the digital era*. Routledge.

Meijer, A., Lips, M., & Chen, K. (2019). Open governance: A new paradigm for understanding urban governance in an information age. *Frontiers in Sustainable Cities*, *1*(3). http://doi.org/10.3389/frsc.2019.00003

Mergel, I. (2019). Digital service teams in government. *Government Information Quarterly*, *36*(4). https://doi.org/10.1016/j.giq.2019.07.001

Misra, P. (2019). *Lessons from Aadhaar: Analog aspects of digital governance shouldn't be overlooked*. Pathways for Prosperity Commission Background Paper Series No. 19. Oxford. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-09/lessons_from_aadhaar.pdf

Möller, D. (2020). *Cybersecurity in digital transformation: Scope and applications*. Springer. https://doi.org/10.1007/978-3-030-60570-4

Negreiro, M. (2021). *The NIS2 Directive: A high common level of cybersecurity in the EU*. European Parliamentary Research Services. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

OECD. (2019a). *Hello, world: Artificial intelligence and its use in the public sector*. OECD Working Papers on Public Governance No. 36. https://www.oecd-ilibrary.org/docserver/726fd39d-en.pdf?expires=1645601868&id=id&accname=guest&checksum=9D7637FE492E04C762A928CC56A9D309

OECD. (2019b). *Digital Government Index: 2019 results*. OECD Public Governance Policy Papers No. 03. https://dx.doi.org/10.1787/4de9f5bb-en

OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*. OECD Public Governance Policy Papers No. 02. https://dx.doi.org/10.1787/f64fed2a-en

OECD. (2021). *The e-leaders handbook on the governance of digital government*. OECD Digital Government Studies. https://doi.org/10.1787/ac7f2531-en.

Pierre, J. (2000). Introduction: Understanding governance. In J. Pierre (Ed.). *Debating governance: Authority, steering and democracy*. Oxford University Press.

PowerSchool. (no date). SAMR model: A practical guide for K–12 classroom technology integration. https://www.powerschool.com/blog/samr-model-a-practical-guide-for-k-12-classroom-technology-integration/

Puentedura, R. (2006). Transformation, technology, and education. http://hippasus.com/resources/tte/puentedura_tte.pdf

Rao, U., & Nair, V. (2019). Adhaar: Governing with biometrics. *Journal of South Asian Studies*, *42*(3), 469–481. https://doi.org/10.1080/00856401.2019.1595343

Republic of Kenya. (2019). *Digital economy blueprint: Powering Kenya's transformation*. https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf

Republic of South Africa. (2020). *National digital and future skills strategy: Originality, agility, critical thinking and problem-solving for digital inclusion*. https://www.gov.za/sites/default/files/gcis_document/202009/43730gen513.pdf

Rosa, H. (2013). *Social acceleration: A new theory of modernity*. Columbia University Press.

Sandoval-Almazán, R., Luna-Reyes, L., Luna-Reyes, D., Gil-Garcia, R., Puron-Cid, G., & Picazo-Vela, S. (2017). *Building digital government strategies*: *Principles and practices*. Switzerland: Springer.

Scholl, H. (2008). Discipline or interdisciplinary studies domain: Challenges and promises in electronic government research. In H. Chen et al. (Eds.). *Digital government: E-government research, case studies and implementation*. Springer.

Sen, S. (2019). *A decade of Aadhaar: Lessons in implementing a foundational ID system*. Observer Research Foundation Issue Brief No. 292. https://www.orfonline.org/wp-content/uploads/2019/05/ORF_Issue_Brief_292_Aadhaar.pdf

Singh, R. (2019). Give me a database and I will raise the nation-state. *Journal of South Asian Studies*, *42*(3), 501–518. https://doi.org/10.1080/00856401.2019.1602810

Sullivan, C. (2013). Digital citizenship and the right to identity in Australia. *Federal Law Review*. https://ssrn.com/abstract=2379240

Toomere, T., Kamalanathan, S., Fruedenthal, M., Valdma, S., & McBride, K. (2022). *Digital government interoperability platform reference architecture*. Cybernetica. https://doi.org/10.13140/RG.2.2.35029.91368 and https://cyber.ee/uploads/Digital_Government_Interoperability_Platform_Reference_Architecture_4d2b8a83f6.pdf

Trade Law Centre (tralac). (2021). South Africa's 2021 global trade update. [Infographic].

United Nations (UN) (no date). *Trade facilitation implementation guide: The single window concept*. https://tfig.unece.org/contents/single-window-for-trade.htm

United Nations (UN). (2018). *World Economic and Social Survey 2018: Frontier technologies for sustainable development.* https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESS2018_es_en.pdf

United Nations (UN). (2020). *E-government survey 2020: Digital government in the decade of action for sustainable development*. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

Van Dijk, J. (2005). *The network society: Social aspects of new media*. 2nd Edition. Sage Publications.

Van de Donk, W., & Snellen, I. (1999). Towards a theory of public administration in an information age? In W. van de Donk & I. Snellen (Eds.). *Public administration in an information age*. IOS Press.

Van Laar, E., Van Deursen, A., Van Dijk, J., & De Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behaviour*, *72*, 577–588. http://dx.doi.org/10.1016/j.chb.2017.03.010

Wirtz, B., & Daiser, P. (2015). *E-government: Strategy, process, instruments*. Speyer.

World Bank. (2019). *Global ID coverage, barriers, and use by the numbers: An in-depth look at the 2017 ID4D-Findex Survey*. https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf

World Bank. (2021). *World Development Report 2021: Data for better lives*. https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

World Customs Organisation (WCO). (2019). *Case study: China international trade single window*. [Annex II to doc. PM0482E1]. http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/sw-initiatives/china/pm0482e1_annexii.pdf?la=en

Yeung, K. (2017). “Hypernudge”: Big Data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118–136. http://doi.org/10.1080/1369118X.2016.1186713

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospect of an information civilization. *Journal of Information Technology*, *30*, 75–89. https://doi.org/10.1057/jit.2015.5