Submitted via email
NIP2050Phase2@dpw.gov.za

8 December 2022

Re: National Infrastructure Plan 2050 Phase 2 (21 October 2022)

To:
Ms Patrica De Lille, MP
Minister of Public Works and Infrastructure

Thank you for the opportunity to submit public comments on the National Infrastructure Plan 2050 Phase 2. We are research staff based at Research ICT Africa, a Pan-African Cape Town based think tank. We study the dynamics of cybersecurity in Africa. Dr. Scott Timcke is a Senior Research Associate with 15 years of academic research experience on states, markets and digital technology. He leads the AI Risk and Cybersecurity project. Mark Gaffley is an Attorney and Researcher working on the same project and is completing his PhD in law (Jurisprudence) at the University of Cape Town where his research explores AI ethics. He has 10 years experience practising law, having worked at a number of local and international technology companies.

Given our professional experience and research programs our comments are primarily addressed to elements of the Plan that intersect with issues of cybersecurity, cybercrime, digital economy and the governance of data flows. As digital technologies are 'distributed infrastructure' our comments do encompass issues related to road, rail, health, and educational infrastructure too. To a limited degree we offer secondary comments about the utility of the Plan furnishing more details about costing and accountability.

We applaud the authors of the National Infrastructure Plan for focusing on 'the dynamic industries of the future' through 'actionable steps and intermediate outcomes' (p6). Forward thinking like this can help ensure that citizens are not 'left behind' as new products, services, and advanced manufacturing technologies come to market the world over. We agree with the vision of the Plan that South Africans should be active participants in building the future too.

We provide 18 comments on the Plan, which follow the page break.

Data-Governance of Digital Infrastructure

1. There is value in remaking the digital economy so that citizens are included into a fairer system. The digital economy is characterised by super-profits while the routine operations of firms in this economy are core mechanisms for the widening of social inequality in the early 21st century.[1] The Plan does note that digital exclusion is associated with social inequality; however, as the rise of gig work well illustrates digital inclusion does not automatically alleviate social inequality.[2] RIA's research on the future of work in the Global South found that contractors participating in the gig economy lack staff support, basic employment benefits and have poor working conditions.[3] Moreover, workers' have limited privacy and agency over their data, are surveilled and have limited safety and security protections with no medical assistance being provided by private companies operating platform based services to e-delivery workers.[4] Indeed, the future of digital work looks very bleak when recognising the extent to which it is undergirded by precarity and relative deprivation.[5]

Without foregrounding issues of social and economic justice, the language of digital inclusion seems rather one-sided, as if it focuses more on the creation of customers for markets rather than the full development of the person as such. People are more than workers and consumers. To keep the digital economy from creating economic stratification, the Plan should consider the viability of concurrently advocating for a wealth tax, which if implemented appropriately could yield R143 billion.[6] Similarly the Plan can signal that there is value in the South African government supporting efforts in the international arena to undertake tax reform on data flows. Redistribution of the great wealth created by the digital economy can help ensure that everyone benefits from this transformation.[7]

---

[1] Onuoha, R., and Gillwald, A., (2022) Digital Taxation: Can it contribute to more just resource mobilisation in post-pandemic reconstruction?, January 2022, Research ICT Africa, https://researchictafrica.net/wp/wp-content/uploads/2022/02/Digital-Taxation-can-it-contribute-to-more-just-resource-mobilisation-in-post-pandemic-reconstruction.pdf

[2] Milkman, R., Elliott-Negri, L., Griesbach, K., and Reich, A. (2021). Gender, Class, and the Gig Economy: The Case of Platform-Based Food Delivery. *Contemporary Issues in Early Childhood*, *47*(3), 343–351. https://doi.org/10.1177/1463949116661126; Zhi Ming T., et al (2021) The ethical debate about the gig economy: A review and critical analysis, *Technology in Society*, 65 (May 2021) 101594, https://doi.org/10.1016/j.techsoc.2021.101594.

[3] Ahmed, S., Chinembiria, T., Moyo, M., and Gillwald, A. (2021). Future of Work in the global South (FOWIGS): Digital labour, New Opportunities and Challenges (working paper). December 2021. Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2021/12/Future-of-Work-in-the-global-South-FOWIGS-Working-Paper.pdf.

[4] Ibid.

[5] Standing, G. (2014). The Precariat. *Contexts*, 13(4), 10–12. https://doi.org/10.1177/1536504214558209.

[6] Chatterjee, Aroop., Czajka, L., and Gethin, A., (2021) A Wealth Tax for South Africa, Southern Centre for Inequality Studies, University of Witwatersrand, https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/scis/documents/WorldInequalityLab_WP2021_02_SouthAfrica_WealthTax_2b.pdf.

[7] Timcke, S. (2021). *Algorithms and The End of Politics*, Bristol: Bristol University Press.

2. There is scope for the Plan to acknowledge that there are different models of governance of data flows currently being debated in the international arena, and that selecting between these models shapes the relative ease of using digital infrastructure for inclusive economic reconstruction. The Plan would be strengthened by responding fundamentally to these kinds of issues by indicating which model of data flows South Africa supports. Indeed rather than a regulatory approach that looks at 'distributed infrastructure' and 4IR technologies (AI, machine learning, blockchain, drones and so on) as discrete entities, each with promises and pitfalls, there is value in developing a transversal digital policy that is far more comprehensive in nature. As the Plan illustrates on several occasions, this kind of digital policy coordination can work best when cutting across government departments and economic sectors. Accordingly, there is merit in formulating a high level of integrated planning, implementation, and public and private sector coordination as this can use distributed infrastructure to drive an equitable and competitive digital economy. Moreover, if new forms of digital infrastructure are governed by regulatory frameworks based on assumptions of static efficiency models traditionally used in telecommunications, then infrastructure, platforms and applications that can be complementary will appear to be in competition and then be treated as conflictual. These old models can stifle innovation thereby working against the vision of using infrastructure that the Plan promotes.

The AU Data Policy Framework – which Research ICT Africa consulted on – provides one model for the governance of data flows on distributed infrastrictrue.[8] The domestication of these principles for distributed infrastructure further allows for the standardisation and interoperability of cross border flows, especially in the context of operationalising the African Continental Free Trade Area, Digital Single Market as envisioned in the AU Digital Transformation Strategy for Agenda 2063. With a digital single market in Africa, South Africans have an arena to trade goods and services.

3. The Plan can provide reinforcement for regulatory institutions to ensure that the digital economy is not dominated by a select few. In a report commissioned by the National Planning Commision, Research ICT Africa argued that "without adequate preparation, South Africa will not be able to adopt new production methodologies that will emerge as a result of advanced technology. In addition to the correct regulations, data governance, infrastructure and skills to embark on the development of the 4IR or to evolve towards a more digitally-advanced economy, it is equally crucial to enable innovative public–private interplays at various levels of government.."[9] The same sentiment applies to discussion of pricing, new entrants, and lowering demand side barriers. Research ICT Africa's extensive work in our *After Access* survey project has the evidentiary support for this line of reasoning.[10] On this note, while the Plan does discuss the shortcomings of Connect SA, presently there are too few details about swift

[8] AU Data Policy Framework, February 2022, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
[9] Gillwald, A. (2020) Digital Futures: South Africa's Digital Readiness for the 'Fourth Industrial Revolution', August 2020, https://researchictafrica.net/wp/wp-content/uploads/2021/01/021220_Digital-Futures_SAs-Digital-Readiness-for-4IR_01.pdf, p7.
[10] After Access Surveys, https://researchictafrica.net/data/after-access-surveys/

implementation of broadband extension. It is long past time that underserved South Africans deserve an infrastructure that allows them to participate as full citizens of the digital environment, and they deserve adaptable regulators who are willing and capable of adopting a 'whole of society' perspective to make this goal a reality.

Cyber-Security and Cyber-Risk

4. Cybersecurity of autonomous vehicle systems is essential to ensuring that infrastructure is safe for users. Section 2.3. Passenger Transport notes how new vehicle technology like autonomous vehicles 'will require adaptation to infrastructure in both transport and communications, operations (e.g. traffic signals), enforcement, regulation, and funding models' (p20-21). As 'the passenger transport sector is agile and adaptable to changing transport realities' (p26), we recommend that state commissioned engineering studies be conducted to ascertain whether autonomous vehicles may increase the wear and tear of road related infrastructure thereby decreasing the life-expectancy of infrastructure. Scenarios involving the use of technologies on the horizon can help with this kind of planning exercise.

Additionally, there are a number of ethical considerations relating to the use and deployment of autonomous vehicle systems that will require intentional engagement with local AI ethics researchers particularly as regards to issues of legal liability and responsibility, and discrimination, for the actions of such systems (i.e. determining whether to protect the vehicle occupant or a pedestrian in an unavoidable collision). Key to this is that autonomous vehicle systems may be designed in foreign jurisdictions using populations that do not reflect the demographics of South Africa for their training data, including not accounting for, or recognising, black people.[11] This can result in racial discrimination from systems. Moreover, South Africa could become a test ground for training autonomous vehicle systems to recognise populations that foreign jurisdictions do not readily have access to, as China is currently doing with facial recognition software used for surveillance in Zimbabwe.[12] These considerations are important given the Plan's recognition that 40% of road related deaths in South Africa are pedestrians (p32). A final consideration is that autonomous vehicle systems are not immune to cyber attack. Therefore cybersecurity standards must be implemented to realise the goal of safe and secure transport for all users.[13]

---

[11] Simonite, T. (2022) The Best Algorithms Struggle to Recognize Black Faces Equally. 22 July 2019. Wired, https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

[12] Chutel, L. (2018) China is exporting facial recognition software to Africa, expanding its vast database. 25 May 2018. Quartz, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity. See also Jili, B. (2022) The Rise of Chinese Surveillance Technology in Africa (part 1 of 6). 31 May 2022. Electronic Privacy Information Center, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/.

[13] Eliot, L. (2021) Serious Concerns That AI Self-Driving Cars Cybersecurity Will Be A Hacker Leak Like an Open Sieve. 25 August 2021. Forbes, https://www.forbes.com/sites/lanceeliot/2021/08/25/serious-concerns-that-ai-self-driving-cars-cybersecurity-will-be-a-hacker-leak-like-an-open-sieve/?sh=f402e96477fb

5. There is a need for clarity on technical and social standards. 'A global standard suited to South African conditions' is a vague statement that does not specify what technical standards will be adhered to or what specific ISO Protocols are intended to serve as a benchmark. On the social front, clearly digital infrastructure will serve to uplift communities who stand to benefit from it. As a word of caution, however, as indicated (p4-5), those areas that are not connected to universal-broadband run the risk of being shut out of the digital economy. Moreover, it is important that accessibility includes assurances that costs of access to digital services are not prohibitive or exclusionary. If used appropriately, digital infrastructure may serve to alleviate burdens on transport and road infrastructure (where, for example, workers are able to work from home and learners can access resources via online learning). This would also assist learning facilities in alleviating their infrastructural capacity burdens as learners can access online educational content without having to go to facilities (p42).

Compliance with the Protection of Personal Information Act

6. Policing solutions discussed in the Plan need elaboration to demonstrate how they work within the Human Rights paradigm and constitutional order. The plan has numerous references to state policing including:

I. 'infrastructure at critical border crossings' (p25) and 'strong state policing will secure the country's rail and road assets in partnership with local stakeholders' (p25);
II. 'the number of arrests and successful prosecutions of people involved in the theft of metals must rise each quarter' (p66); and
III. 'strategies to protect infrastructure to include drones and remote sensing-technology, CCTV etc' (p69).

These statements raise a number of ethical and human rights issues. First, where predictive policing software is deployed to realise crime prevention aspirations, police need to be cognisant of the training data used in these systems. Crime data are unique in that the end uses of datasets (police) control the data inputs (police reporting), which entails that crime data is filtered and has the propensity to reaffirm historical prejudices.[14] As an example, in the United States drug arrests continue to occur in predominantly poor and non-white areas owing to the reliance on historical data that continues to flag the same areas of cities as high risk.[15] This may be particularly prejudicial in South Africa with its history of racial discrimination under Apartheid having skewed datasets.

[14] Timcke, S. (2020). The One Dimensionality of Econometric Data, *Triple-C*, 18(1): 429-443.
[15] Adams, R. Pienaar, G. Gastrow, M. Gaffley, M. et al. (2021) Human Rights and the Fourth Industrial Revolution in South Africa. HSRC Press. https://www.hsrcpress.ac.za/books/human-rights-and-the-fourth-industrial-revolution-in-south-africa, p47.

Second, there is danger in turning the success of crime prevention into something that is measurable through the number of arrests made, particularly when predictive policing systems are used. This method tends to quantify policing and turn it into a tool to increase productivity and efficiency, rather than to address underlying criminogenic factors.[16]

Finally, increased use of surveillance technologies through drones and remote-sensing technologies may deepen South Africa's discriminatory divide if, for example, these surveillance technologies are deployed in affluent predominantly white communities and racially profile black people.[17] These realistic scenarios stress the need for regulatory frameworks that ensure human oversight and determination in the use of such technologies.

7. All references to data in the Plan needs to emphasise the importance of compliance with the Protection of Personal Information Act 4 of 2013 (POPIA). All points relating to data in the Plan should minimally ensure alignment with and compliance to POPIA. Indeed, it is worrying that no mention whatsoever was made of POPIA, including the need for compliance with industry specific code of conducts (if applicable) and appropriate privacy safeguards when data is referenced in the Plan. Indeed, the Plan provides that digital data will be leveraged to enable continuous improvement and an entity will be identified that will be responsible for collecting, analysing and curating data (p26) where compliance with POPIA should be mandated. To emphasise the need for securing personal and sensitive information a recent report on the education sector[18] found that the majority of technologies put children at risk or directly violate children's privacy and other rights, for purposes unrelated to their education. Similar risks exist for health infrastructure and references in the Plan to ICT systems containing patient records (see p52) and e-health systems (p53) need safeguards in place for dealing with patient information and strict compliance with POPIA.

[16] Ibid, p48.
[17] Ibid, p49-50.
[18] Human Rights Watch (2022). Online Learning Products Enabled Surveillance of Children. 12 July 2022. Human Rights Watch, https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children. Here 163 technologies used for educational purposes across 49 countries, including South Africa, were assessed for possible rights violations.

8. More emphasis on the gatekeeping role of the public procurement professional (especially in light of increased digitisation) is required. As procurement processes become increasingly digitised and more artificial intelligence (AI) based solutions are implemented, it becomes important for those involved in decision making develop technical expertise to:

I. understand the nature of these technologies;
II. assess their suitability as solutions for South African challenges;[19]
III. detail how decisions on procuring AI based technologies are made; and
IV. consider social concerns such as fairness, accountability, transparency and the ethics of AI usage and deployment prior to deployment.[20]

The Plan is noticeably silent on AI, its use and deployment in infrastructure and the risks, opportunities and challenges the technology will present. Moreover, for 'decision-making [to] be accountable and institutions effective' (p viii), it is important to note that automated decision making processes (either by AI or assisted by machine learning processes) may run the risk of perpetuating discriminatory practices. This stresses the need to ensure algorithmic accountability in the public sector.[21]

9. More information is required to evaluate data governance in public private partnerships (PPPs). There are a number of factors that the Plan fails to address or consider when it details PPPs as solutions. When PPPs are formed (p vii, p 15) it will be important for policy makers to consider any potential ramifications of outsourcing government services to private entities, particularly with regard to the collection and use of data, obtaining prior informed consent prior to collecting data, and the safeguards in place for collection, use and storage of any personal or sensitive information. As an example, vulnerable groups were subjected to predatory practices in South Africa where the government outsourced grant payments to private third-party service providers (PSPs).[22] It therefore remains critical to recognise that digitisation and outsourcing to the private sector can create new avenues for exploitation.[23] Moreover, policy and regulatory frameworks that are supportive of PPPs (p16) must be sufficiently clear on

[19] Nagitta, P. O., Mugurusi, G., Obicci, P. A., Awuor, E., (2022). Human-centred artificial intelligence for the public sector: The gate keeping role of the public procurement professional. *Procedia Computer Science* 200, 1084-1092. https://doi.org/10.1016/j.procs.2022.01.308.
[20] Gaffly, M., Adams, R., and Shyllon, O. (2022). Artificial Intelligence, African Insight. A Research Summary of the Ethical and Human Rights Implications of AI in Africa. HSRC & Meta AI and Ethics Human Rights Research Project for Africa - Synthesis Report, https://africanaiethics.com/wp-content/uploads/2022/02/Artificial-Intelligence-African-Insight-Report.pdf.
[21] See Ada Lovelace Institute, AI Now Institute and Open Government Partnership. (2021) Algorithmic Accountability for the Public Sector, https://www.opengovpartnership.org/wp-content/uploads/2021/08/algorithmic-accountability-public-sector.pdf
[22] See *Minister of Social Development of the Republic of South Africa and others v NET1 Applied Technologies South Africa (Pty) Ltd and Others*. See also South African Human Rights Commission (SAHRC) (2017). Human Rights Impact of Unsecured Lending and Debt Collection Practices in SOuth Africa. SAHRC, https://www.sahrc.org.za/home/21/files/SAHRC%20BHR%20RA%203%20-v3.pdf.
[23] Gaffley, M. (2021) AI and Data in South Africa's Finance Sector: Towards Financial Inclusion. Policy Action Network, https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData9_FinServices_V1_Elec.pdf.

what the private sector can and cannot do with any data it collects, as well as inappropriate functions of any software private companies may deploy in providing solutions from PPPs.

Cyber-Crime and Digitization Systems

10. The Plan lacks a basic discussion of cybersecurity elements of important sensitive information systems. This consideration should be at the forefront of policy-makers' minds if the state wishes to create a population registry, or build e-health and e-education services that will be accessed by many people. Given that the authors stress corruption, what systems will the state use to protect citizens and their information from internally assessed breaches, hacks, and leaks? Additionally what steps will the state take to uphold rights to privacy, and particularly the sharing of sensitive data? In short, the state needs to demonstrate that it can be trusted as good stewards of citizens' data. Introducing and updating modules in cybersecurity at the National School of Government courses can help build this trust.

Further, keeping (transnational) cybercrime in mind, all municipal trading services need to adhere to cybersecurity protocols that exceed global minimum standards. We are greatly alarmed by the lack of any mention about the cybersecurity needs for South Africa's critical infrastructure including nuclear power plants, related power facilities, and water facilities. Funding and training for Computer Security Incident Response Teams (CSIRTs) ought to be accounted for in the Plan. Similarly funding must be allocated for municipal trading services and providers to become certified in and comply with cybersecurity best practices including having robust monitoring and protection mechanisms in place to ensure the integrity of critical infrastructure. Independent verification of certification and compliance is valuable as the South Africa government moves to the operator licence model for municipal trading services. Furthermore, the Plan should consider the vulnerabilities inherent in using IoT solutions in critical infrastructure (e.g. water as a precious resource), which may become key targets for potential cyber attacks. Indeed, power and water utilities are already being targeted by governments and cybercriminals in other jurisdictions.[24]

[24] Magill, J. (2022) U.S. Water Supply System Being Targeted By Cybercriminals. 25 July 2021, https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=7facf3bb28e7. See also Clark, R. M., Panguluri, S., Nelson, T. D., and Wyman, R. P. (2016) Protecting Drinking Water Utilities From Cyber Threats. Idaho National Laboratory. https://www.osti.gov/pages/servlets/purl/1372266. See further Macola, I. G. (2020) The five worst cyberattacks against the power industry since 2014. 2 April 2020. Power Technology, https://www.power-technology.com/analysis/the-five-worst-cyberattacks-against-the-power-industry-since2014/.

11. Encourage and fund the further digitization of documentation for freight services. Systems have already been purchased by Transnet for railways, port, and pipeline networks,[25] and we encourage the deployment of similar systems to increase efficiency and use, providing of course that there is due attention given to cybersecurity. Processing and control systems in logistics are vital to help achieve the target of '[moving] 50 million tonnes of freight and 100 million passengers from road to rail' (p34).

Retrofitting Municipal Trading Services

12. Municipal trading services 'separating-at-source and recycling programmes' (p26) could be complemented by sorting critical materials from waste. Not only can sortion fulfil the aspirations of a digital circular economy, but recycling programs can preserve critical materials that are key inputs for digital infrastructure. In this regard, it is positive to note that the Plan has considered how stolen metals may be fed into recycling programs. More research is needed for how legitimate and stolen materials can be identified in recycling programs. This is important in light of the Plan's recognition that the circular economy is essential for the employment and income of very vulnerable workers such as waste-pickers. Moreover, the Plan can support R&D into the construction of automated waste centres which can recycle and redirect materials from landfills to advanced manufacturing. The Plan indicates that more than half of municipal landfills do not comply with regulatory standards, waste collection is not reliable [and that this] leads to waste accumulation and health hazards (p13). Finally, with an eye on 2050, it will be important for the Plan to consider growing amounts of electronic waste or e-waste (computers, phones, their components, batteries etc) and the legislative measures that have been put in place to deal with safe disposal of such waste.[26]

13. The Plan should emphasise the need for better enforcement elements for levying and efficient collection of municipal rates and taxes to strengthen the process. The Plan indicates that customers owed municipalities R232 billion and that municipalities have struggled to collect all the revenue that is due to them (p8-9). This indicates the need to prioritise enforcement mechanisms in situations where customers do not pay their rates and taxes, as opposed to focusing on the efficiency of collection mechanisms. Practically, the system may work better with increased efficiency, but this focus possibly appears to prioritise addressing the symptom (collection) rather than the cause (non-payment).

[25] IT Web (2022) Transnet maps digital journey with Huawei, 17 November 2022, https://www.itweb.co.za/content/kYbe97Xb149qAWpG.
[26] Zali, M. (2021) New electronic waste management regulations will take effect in November. 18 October 2021. Mail & Guardian, https://mg.co.za/environment/2021-10-18-new-electronic-waste-management-regulations-will-take-effect-in-november/.

14. Where possible upgrades to existing infrastructure should provide for smart solutions. The Plan mentions the periodic upgrading of buildings, roofs and equipment (water, sanitation, electricity, safety and access infrastructure etc) as well as government's attempts to provide for water savings on government buildings programmes (as indicated in SIP 28 PV) (p43-46). The Plan does not explicitly mention turning to 'smart' or 'digital' solutions for these upgrades or savings processes. Smart solutions may have higher installation costs, but are likely to drive down maintenance costs and increase efficiencies in the long run.

Planning and Public Accountability

15. There is utility in providing more itemization details about programs; presently the plan is too sparse for citizens to properly evaluate. We do appreciate how the Plan acknowledges that it is not a comprehensive master plan, but we do think the DPWI could provide more specific information about programs, spending plans, and lines of accountability. Thickening the plan can help citizens reasonably find all the necessary information in one place. This means they do not have to navigate the labyrinth of multiple state documents. The provision of more details in the plan itself allows citizens to evaluate prospects of success and give them the information to make investment decisions. Furnishing these details is especially important as the plan asks for the private sector to spend 20% of GDP on infrastructure, or roughly R1463 billion.

16. There could be greater clarity on the timelines for spending and budget allocations. Presently the plan is silent about when spending will occur. Citizens do not know whether the target is to spend 1% of GDP (benchmarked to 2022) each year until 2050. Or whether the bulk of the spending will occur in the next five years. Or whether some sectors take priority when it comes to spending. Altogether more details and charts about spending plans would be helpful. Furthermore, the plan could better identify which state agencies are responsible for each component, and their anticipated budgetary allocation. In addition to giving citizens a leading indicator of forthcoming budgets, without open budgeting citizens cannot assess the fiscal feasibility of any endeavour outlined in the plan. The plan needs to include fiscal scoring and blue paper appendices. In line with the plan explicitly stating that 'new thinking is required,' we recommend that the authors revisit all 'will be' and 'must be' language and replace it with specifics about budgetary allocations, commissioned reports on progress undertaken by independent bodies not associated with the state, parliamentary testimony, and specific programs. Specifics allow for accountability.

Additionally, there is a need to be cautious about 'Debt Capture.' The Plan puts a target of the public sector spending 10% of GDP, roughly R730 billion on infrastructure. Great caution should be exercised if any portion of this spending is funded by loans. Already the state has a debt of approximately R2260 billion.

17. The Plan needs to acknowledge that government departments and state agencies are accountable to Parliament. Presently the plan does not stipulate (or indicate specific funding for) the need to furnish reports to parliament. Nor does the report indicate line item funding for independent authorities to proactively investigate the use of funds in building infrastructure.

18. As infrastructure spending is notorious for fraud and waste, it is advisable that the Plan allocate spending for prevention, investigation and prosecution of civil servants and contractors who abuse funds. Coordinating oversight can be supported by a publically open and searchable database that shows transparent contracts, contractors, projects and expenditures. This database could be supported by data analytic tools so that prudent public monitoring can deter and blunt inevitable waste. It is useful to have oversight models be included in infrastructure legislation.

Thank you for the opportunity to comment on Phase 2 of the National Infrastructure Plan 2050. Like the DPWI we are eager to see how South Africans will build and use infrastructure to develop and explore their talents to further enrich the world. Adequate foundations can better position people to participate in collective life to make the next iteration of the South African project a success.

Dr. Scott Timcke
Senior Research Associate
Research ICT Africa
stimcke@researchictafrica.net

Mr. Mark Gaffley
Researcher and Project Manager: AI
Research ICT Africa
mgaffley@researchictafrica.net

Organisational Profile

Research ICT Africa (RIA) is an African think tank that has operated for over a decade to fill a strategic gap in the development of a sustainable information society and digital economy. It has done so by building the multidisciplinary research capacity needed to inform evidence-based policy and effective regulation Africa. RIA's dynamic and evolving research agenda examines the uneven distribution of the benefits and harms of the intensifying global processes of digitalisation and datafication.

On this basis, we seek to provide alternative policy and regulatory strategies that produce different outcomes that will address digital inequality in Africa and enable data justice. Through rigorous research and analysis RIA seeks to build an African knowledge base in support of digital equality and data justice, and to monitor and review developments on the continent.

Our public-interest research on the digital economy and society responds to national, regional and continental needs. It provides relevant stakeholders with the information and analysis required to develop flexible and adaptive policies and regulation to deal with an increasingly complex and dynamic digital environment.

RIA contributes to the gathering and analysis of data and indicators to establish a repository of knowledge for furthering research and digital governance and to enable greater African participation in global governance. RIA hosts an African network, which extends across the continent and further collaborates and leverages its activities through national, regional and continental partnerships.

On the basis of our research and extensive practical policy and regulatory experience, RIA offers technical assistance and advisory services to multilateral agencies, governments and regulatory agencies across the continent. It also offers regulatory executive training and post-graduate education through the University of Cape Town's Nelson Mandela School of Public Governance.

RIA has been commissioned to undertake research, technical assistance and capacity building for multilateral agencies such the African Development Bank, the World Bank and the European Bank for Reconstruction and Development, the International Telecommunications Union (ITU), the Commonwealth Telecommunications Organisation (CTO), United National Conference on Trade and Development (UNCTAD) and UNDESA. We have provided technical assistance to the Government of Mauritius, Namibia and South Africa, including Treasury, the Department of Communications, Department of Trade and Industry, the Competition Commission and ICASA.

RIA participates actively in global fora such as the Internet Governance Forum, the UN Secretary General's Digital Cooperation Roadmap and the Global Partnership on Artificial Intelligence.

RIA also enjoys high levels of credibility amongst donors and has established a reputation for excellence, delivery and accountability. We have built enduring relationships with donors including the Canadian International Development Research Council (IDRC), the Swedish International Development and Cooperation Agency (SIDA), Open Society Foundation, Mozzila and the Shuttleworth Foundation.

RIA's research, which arises from a public interest agenda, is made available in the public domain, and individuals and entities from public, private sector and civil society are encouraged to use it for teaching, further research or to enable them to participate more effectively in national, regional and global digital policy formulation and governance.