Deloitte.

Connectivity Resilience Amidst COVID-19

A Telecommunications Thought Leadership Perspective

MAKING AN IMPACT THAT MATTERS since 1845

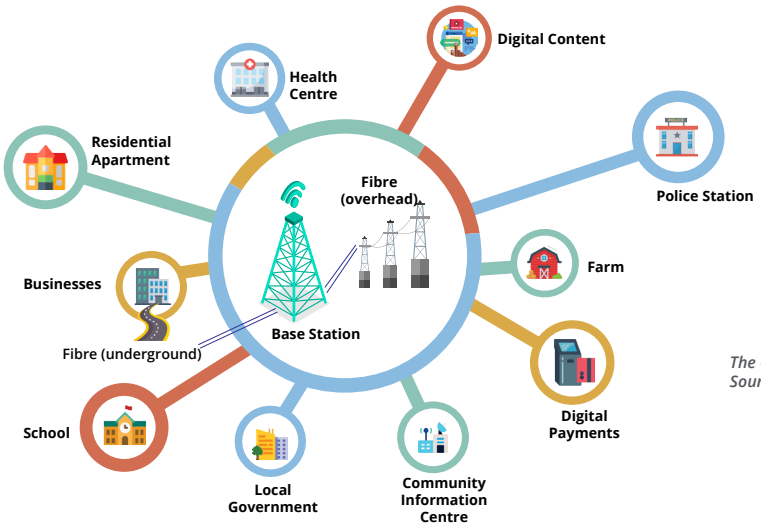
Connectivity Resilience in a VUCA world – Enhancing Communication Infrastructure amidst COVID-19

Internet service providers have seen **double-digit increases** in traffic with increased demand for **e-commerce, education and entertainment**

Volatility, Uncertainty, Complexity and Ambiguity – indeed, words that capture the stark reality of these times globally. The rapid spread of the pandemic COVID-19 to over one million confirmed cases and tens of thousands of lives lost across 212 countries, (WHO April, 2020) has impacted every aspect of our society, families, education, ways of work, public gatherings and individual daily routines. The world including business communities are in the process of re-defining a new and unprecedented normal where change is exceedingly rapid, old patterns are being upended overnight and social media is flooded with information both genuine and unverified throughout the communication networks. Within this context, many countries and organizations are struggling to define how to operate, how drastic emergency responses should be, and if protecting economic damage while saving lives via national lockdowns can be achieved simultaneously. There is an imperative to respond, recover and eventually thrive again.

The impact of the pandemic on communication and connectivity has been felt within the ecosystem surrounding the internet and communications technology, increasing demand and highlighting the need to leverage tools and innovative strategies to survive and thrive. As a ripple effect of the pandemic, significant increases in data consumption have been observed globally as entire populations shift to working and being educated from home due to social distancing. U.K. internet service providers have seen double-digit increases in traffic amidst the coronavirus lockdown with global streaming services such as Netflix and Disney+ cutting bandwidth usage to prevent network congestion (CNBC Markets). The educational sector has accelerated use of distance learning by necessity and home networks not designed for use cases such as simultaneous video conference calls are being tested, having to support heavy use for commerce, education and entertainment.

New e-commerce customers, the elderly and those who prefer in-store shopping, have taken to online retail services given the restriction of movement and may not migrate back to old patterns once the crisis is over. With the elimination of public gatherings and most sports leagues suspended, online entertainment options have seen rapid increase in demand. In addition, the streaming of religious services and conferences has increased both demand and frequency of live streaming. COVID-19 has accelerated the adoption of connectivity tools and forced networks to adjust to a new set of individual and enterprise user requirements.



The Connected Community. Source: Deloitte Insights

New Ways of Working and Disaster Recovery

Organizations need to adopt resiliency strategies across the domains of People, Processes and Technology and continuously update their threat response strategies in an evolving, globally-connected operating environment. The first step should be a review of disaster recovery and business resilience plans, and then a comprehensive playbook developed on how people, processes and technology will operate in the event of single or multiple crises. Once the emergency has been contained and response delivered, a plan to leverage the new trends and shift in industry landscape is the next crucial step for all leading organizations to adapt to the future.

Expanded capacity may be needed to cope with the increased need for communication and digital tools, and further strategies to ensure the quality of service with new demand patterns observed. Autonomous processes must be emphasized with the increased use of cognitive technologies such as Robotic Process Automation (RPA) to reduce manual tasks such as configuration of transmission equipment or analysis and adjustment of customer capacity. Remote monitoring and configurations systems should be leveraged requiring less human intervention.

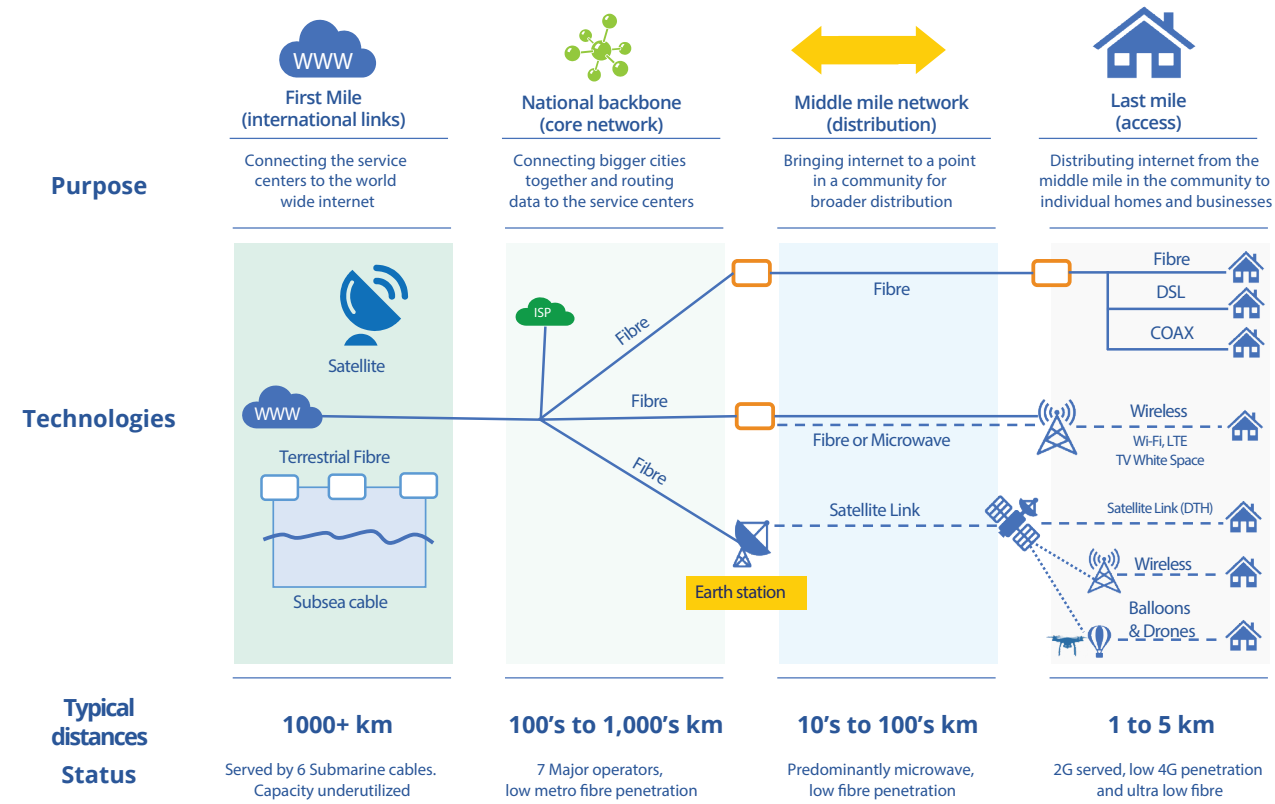
Recommendations to enhance Resilience for Communication/Connectivity Providers and Enabling Environment Stakeholders across domains: People, Process, Technology (PPT)

	Immediate Steps RESPOND	Medium Term (6 months) RECOVER	Long Term (6 -12 months) THRIVE
PEOPLE	• Provide healthcare options for tes ting, information and rapid response to staff supporting critical services • Protection guidelines should be followed and tools /equipment such as sanitizers, gloves and masks provided. • Provide accommodation for staff and safe transportation to enhance social distancing efforts. • Ensuring IDs and mobility of key personnel in concert with local and state government agencies	• Invest in primary and backup structure for key skills and function alities. Train teams of Telco and NOC engineers to be cross functional and eliminate key man risks. • Review awareness of emergency and business continuity plans and per form test runs at random to ensure preparedness. • Foster awareness and enforce laws against willful or ignorant damage of Critical National Infrastructure	• Continuous training of people in key skills and digital fluency • Establish crisis response teams and annual training
PROCESS	• Review of Critical Operational Pro cesses, Dependencies and Single Points of Failure. • Creation and continuous updates of Resilience, Disaster Recovery and Business Continuity Plans. • Review of emergency protocols in line with best practice healthcare recom mendations from Governments, WHO and National Disease Control Agen cies and prioritizing critical support functions.	• Automate Business Processes and reduce manual/physical points of intervention. • Invest in competent connectivity network/fiber route maintenance providers with guaranteed SLAs and proven timelines for fault and con nectivity restoration. • Investing in international/local insurance for business continuity and disaster recovery. • Debrief and publish lessons learned during and after the emergency for improved safety & security locally and globally.	• Improve Power resilience and supply strategy for on-site storage and back up power • Increase redundancy of systems where possible for increased fault tolerance. • Continuously update knowledgebase and lessons learned after the emer gency for improved safety and securi ty locally and globally.
TECH	• Ensure Primary and Backup Data centers for safekeeping of data and critical system/information back up. Leverage cloud options for immedi ate deployment. • Enhance remote working culture with Digital Fluency Training • Utilize remote/virtual collaboration tools and platforms	• Investment in resiliency/redundancy across communication and fiber net works (First mile, middle and last mile) by ISPs and Network Opera tors. • Enhance Automation of business processes leveraging technology tools such as Robotic Process Automation, Artificial Intelligence (AI) and Digital Fluency Training. • Leverage remote configuration, mon itoring and troubleshooting tools and systems requiring less human inter vention for fixes/emergency opera tion	• Continuous Investment in resiliency • Review data resilience, security and critical system / information back up. • Industry focus on more “Plug and Play” devices with reduced need for configurations. • Increased satellite coverage to reach the unserved/underserved areas; efficient use of spectrum as well as TV whitespace to deploy broadband

Nigeria's Telecommunications Sector - Driving Critical National Services

The recently launched Nigerian National Broadband Plan (NNBP) 2020-2025 recommends the Federal Government declares Telecoms assets as Critical National Infrastructure (CNI) and assign security agencies to ensure its protection from willful or ignorant damage. The digital economy is driven by high-speed internet connectivity "broadband"; as such the NNBP recommends the creation of a national database of Telecoms infrastructure; stakeholder awareness summits and further highlight penalties in the Nigerian Cybercrime Act for damage of Telecoms infrastructure. Deloitte supported the Presidential Committee on Nigerian National Broadband Planning to draft and compile the committee's 2020-2025 plan and Implementation Roadmap.

President Buhari has stated the importance of Telecoms as CNI and tasked all agencies, including the Federal Ministry of Communications and Digital Economy led by the Honourable Minister Dr. Isa Ali Ibrahim Pantami, to proceed with these efforts to secure Nigeria's communications infrastructure.



Broadband Architecture Framework. Source: World Bank/Nigerian National Broadband Plan 2020-2025

Further priority initiatives recommended in the NNBP that will promote long term resiliency of connectivity infrastructure include establishing a coordinating body for fibre builds to prevent overlaps and improve coverage. This body would also ensure standard Right-of-Way charges nationwide that will encourage additional fibre builds of primary and back-up routes. A one-stop shop for faster base station permitting and acquisition is recommended to accelerate coverage and improve quality of service. Co-ordinated government funding of national and regional backbone infrastructure and schemes to ensure last mile access in public institutions such as schools, hospitals and government agencies are all key long term initiatives that will improve the resiliency of the nation's communications infrastructure.

Connectivity Infrastructure and Resilience Costs

Telecoms infrastructure is highly capital-intensive requiring fibre optics, base stations, transmission equipment and specialized engineers for installation and maintenance. The NNBP estimates $5 Billion will be needed over the next five (5) years to support the target of providing broadband connectivity to 70% (penetration) of the population by 2025. With approximately 54,000kms of fibre currently deployed nationally in Nigeria, network deployments to reach customers run into millions of dollars annually, however, the additional cost of insuring and building resilience into telecommunications networks is critical and not optional despite the high costs.

Traditional and new threats to Connectivity

Traditional threats to connectivity are a challenge that all providers face daily such as fibre cuts, vandalism, community disturbances and infrastructure damage due to poorly supervised road construction. In February 2020, Airtel Nigeria stated they experienced over 1,000 fibre cuts from July 2019 to Jan 2020 seriously affecting call quality.

On the submarine (First mile) segment, the West Africa Cable System (WACS) and South Atlantic 3 (SAT3) cables linking Europe to Nigeria and further on to South Africa, experienced service disruptions in January and recently March 2020, impacting 12 African countries including Ghana, Nigeria, Cameroun, Ivory Coast and South Africa. The effects included prolonged internet outages across the region, affecting the ability to download or upload information. Restoration on other providers and insurance provisions on the international cables were required to effect repairs and return regular service. Given the national implications, organizations should ensure provision for such repairs and maintenance with global/local insurance companies for business continuity and disaster recovery. Connectivity providers need to deploy more resilient infrastructure immediately as businesses now recognize the criticality of moving services online given the high and increasing demand for digital services

In efforts to curb the pandemic, threat responses include social distancing with organizations requiring isolation of people, communities and cities to stop the viral spread while a vaccine is developed. These necessary lockdown measures have affected workforces, and thus, lack of mobility is a threat to the ability to maintain connectivity infrastructure. In addition to traditional emergency personnel, technology personnel such as Telecoms engineers, maintenance crews, mobile network managers and operators must be allowed free passage to ensure communication links are stable, uptime is maintained, and capacity is not compromised.

These evolving threats must be addressed by organizations via a holistic approach to people, process and technology that ensures zero key man risks balanced with a focus on staff protection and safety.

Power and its impact on connectivity.

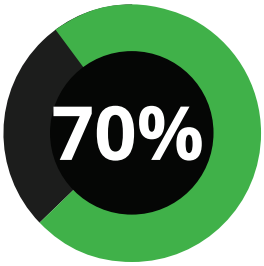
A key underpinning factor to stable connectivity and communications is reliable power. In May 2015 when Nigeria was rocked by the fuel shortage crisis with widespread diesel scarcity, major Telcos who rely on diesel generators rather than the unreliable national electricity grid, issued warnings that lack of diesel to power their infrastructure posed a significant threat to the quality of service and ability to operate their networks. With fuel reserves running low, there was a high risk of potential call drops, internet outages and at worst case a full shutdown if power disruptions continued. Additionally, some local radio stations had to end overnight broadcasts due to the fuel crisis.

In line with this, Telcos need to ensure resilience of critical operations, power supply networks and emergency energy resources as well as Data Center and Network Operating Center (NOC) processes and staffing to ensure their enterprise and individual customers maintain internet, voice access and can carry out critical transactions. Some base stations are exploring the use of Solar Power to reduce dependency on the grid/fuel and increase emergency backup time provided by traditional inverters and UPS systems. Improvements in reliable power delivery via the national grid (GenCos, DisCos and the Transmission network) would significantly reduce the cost of Telecoms operations in the country, allowing operators to invest in further resilience measures such as fibre between base station towers to dramatically improve call quality and reduce reliance on weather susceptible microwave radios.

Connectivity Support and Maintenance Resources (People, Process, Technology)

In terms of the people and resourcing to managing connectivity, Network engineers

The NNBP estimates **$5 Billion** will be needed over the next five (5) years to support the target of providing broadband connectivity to



(penetration) of the population by 2025.

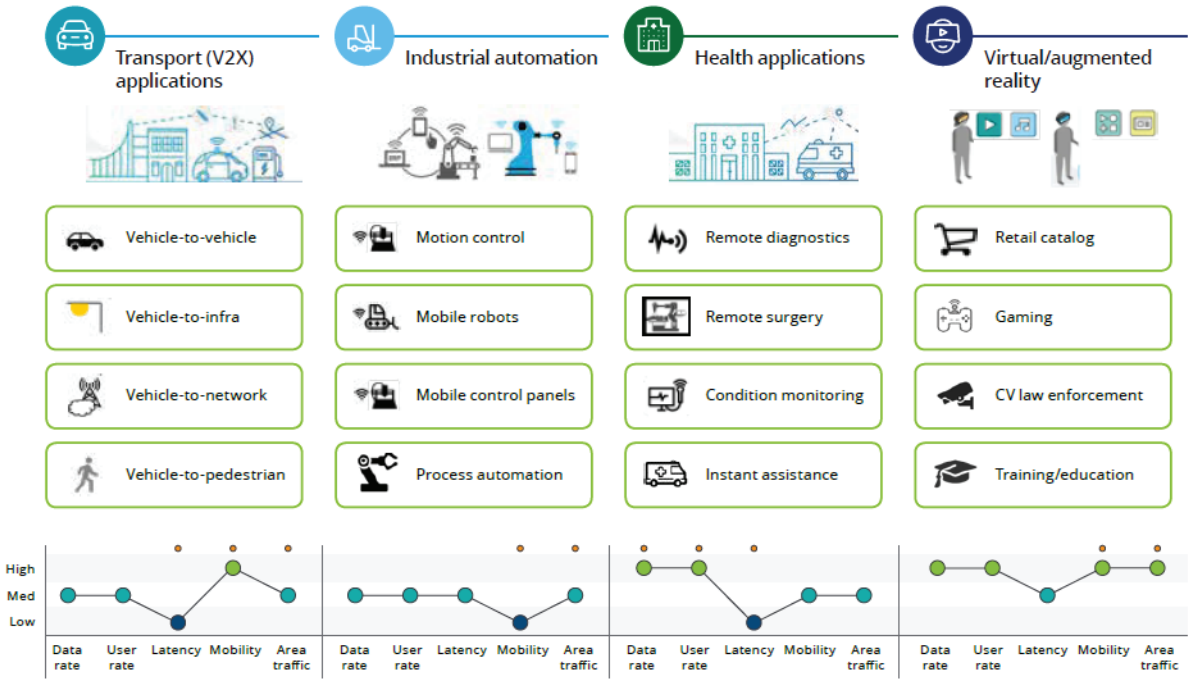
and infrastructure maintenance staff provide critical communication support to systems that enable emergency responders to communicate. IT engineers support essential networks of businesses across every industry and ensure mission-critical applications run smoothly enabling productivity and commerce. As such, critical skilled resources should be proactively supported, with secure transportation, healthcare and 24/7 accommodation options made available to staff providing critical connectivity services.

Business Process Automation

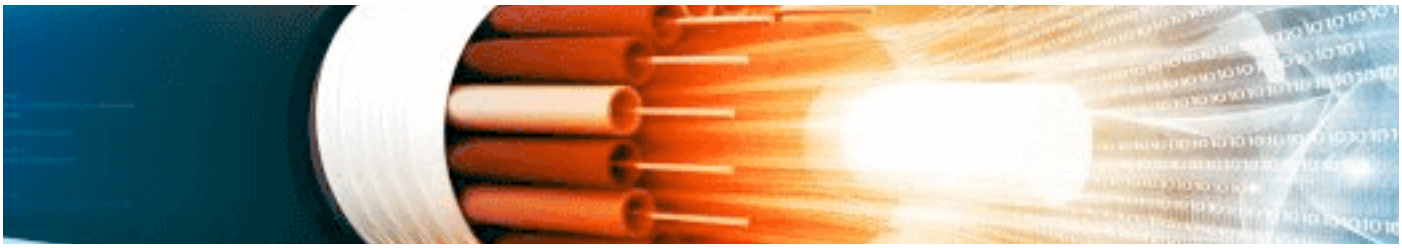
Business processes will need to shift from manual to fully automated systems and leverage technologies like Robotic Process Automation, Artificial Intelligence for monitoring networks and rule-based/advanced decision making. Leveraging exponential technologies that enable remote control, configuration, monitoring and trouble-shooting of telecoms equipment will be vital in supporting the management of field equipment remotely, minimizing the need for physical intervention and improving staff safety.

As networks continue to expand in geographic reach, business process automation reduces the reliance on physical staffing presence in various regions, thus lowering the cost of operations and allowing faster scalability. Leveraging exponential technologies also has the benefit of reducing manual errors and increasing efficiency of repetitive tasks which may need to be performed across a wide array of network equipment.

Globally, telecoms operators are investing in new technology with varied applications across industries including transportation, manufacturing, healthcare, retail, education and more. To stay competitive this highlights the need for investments in infrastructure to deliver these services locally and for the government to protect such investments as CNI.



Global Telecommunications Organizations are Investing in New Technology. Source: Deloitte Future of Connectivity



A Telecommunications Industry Leaders' Perspective – Funke Opeke CEO MainOne: Connectivity Resilience amidst COVID-19

Funke Opeke
CEO of Main One Cable Company Nigeria Limited

Deloitte interviewed Funke Opeke, a Telecommunications Leader, CEO of Main One Cable Company Nigeria Limited and most recently the Chairperson of the Presidential Committee for the Nigerian National Broadband Plan 2020-2025, to share an industry perspective on best practice in maintaining connectivity amidst the Volatility, Uncertainty, Complexity and Ambiguity (VUCA) environment created by the COVID-19 pandemic. Excerpts from the discussion are captured below and provide insights into the necessary steps connectivity leaders must take to ensure resiliency in their operations across people, process and technology domains.

In your own words, can you share the potential impact of COVID-19 on connectivity in a partial or full lockdown scenario?

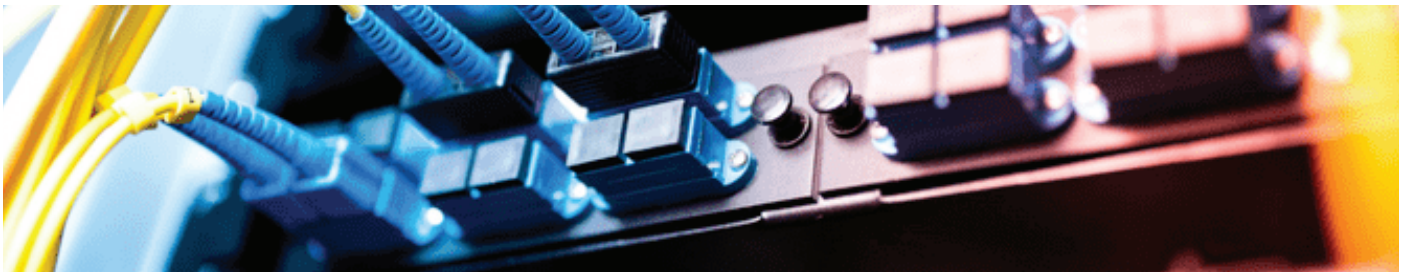
We have seen an overall increase in demand for connectivity services in the past few weeks.

For a lot of businesses, customers need to initiate transactions online while, their staff need to access critical servers to work remotely, so connectivity requirements have increased.

On the retail side also, customers need to shop and work from home, so there is increased usage on networks as well. We have also seen a decline in some areas, for example, small businesses accessing the Internet from the office have now abandoned that for home usage, this is however a very small percentage of the traffic.

With new threats like COVID-19, what will be the impact on connectivity infrastructure and how prepared is your organization? What steps is your organization taking to prepare for the lockdown?

To be honest, we were incredibly well prepared with our Business Continuity plans. Better prepared than I imagined. Majority of our staff have tools to work from home, and with our flexi work practices already in place, we immediately ensured they started doing so. For our critical infrastructure which requires physical presence and oversight, we quickly identified critical staff to cover major locations. We made arrangements to isolate and house those staff in short let flats close to the infrastructure and provided catering services. Finally, we made arrangements for their security and rite of passage from the apartment to the office through the Security Agencies.



What are some resiliency efforts you have put in place in the past and are there others you are considering with the current outbreak of COVID-19? Does this modify/ alter your existing disaster preparedness and business continuity plans?
We have redundant equipment and diverse network routes at the core of our network and data centre infrastructure. We also monitor our sites pro-actively and have out-of-band management access to our devices so staff can access them remotely from home to address any issues. We factor this in when we build our infrastructure, so there are no plans to alter what we already have in place now as it is serving us well.

What traditional threats to connectivity have you experienced, and how have they helped (or differed) in preparation for this pandemic? e.g. Fibre cuts, Vandalism, Community disturbance, Natural disasters
Fibre cuts are the big one. However, with the lockdown also comes restrictions or stoppage of construction activity, so we hope that risk will be reduced. Also, some vandalism, but again we hope the restrictions in movement will slow that down. On average, we have between 5 and 10 cuts every month on our network and many more on partner networks to which we are interconnected.

Given the challenges in the country and with the current outbreak of COVID-19, are you expecting this to cause any downtime to your network? Please share the reasons for your answer
No. Our network is resilient, and we do not expect downtime as a result of COVID-19.

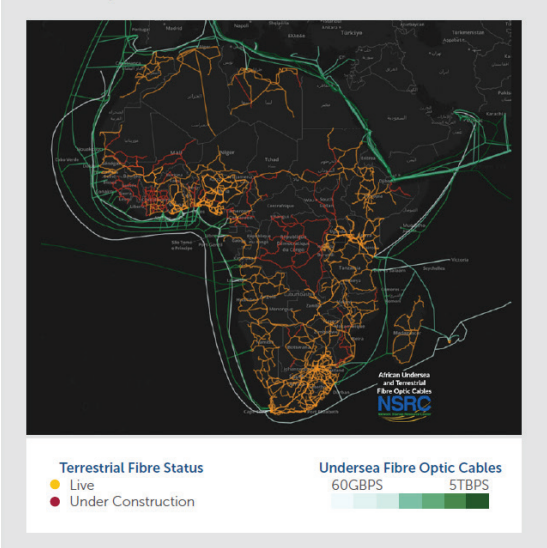
Please share your thoughts on the cost of investing in infrastructure resilience and is there an even higher cost to not protecting your network? E.g., what is the cost of repairing a fibre cut vs cost of having a fibre repair contract or value of a secondary route vs the risk of a single link and network outage?
The cost of resilience is sometimes double the initial cost because you may need 1:1 back up. Sometimes, it is less e.g. 40% - 60% additional. For us, all of our infrastructure is protected, we keep critical spares, and we also sign maintenance agreements with OEMs and service providers. As a B-to-B service provider, we guarantee service levels to our customers and the only way to ensure that is to build the resiliency within.

How much have you invested in infrastructure resilience, spares, backups, capacity swap agreements (general range? If available)
Tens of Millions of USD.

Do you expect your Network Operations Centre to experience increased calls from customers during this period? Please state the reasons for your answer.
No. Indeed, we have fewer calls because things are stable for those who need the services. The smaller customers have generally shut down and gone home.

In times of peace or under threat, a nation's ability to communicate internally with its people, Government agencies, allies and opposition is critical.

African Undersea and Terrestrial Fiber Optic Cables



Source: World Bank Digital Moonshot for Africa/NSRC

Nigerian businesses have moved online. However, there is much more that businesses can do to invest in resiliency and outsource services to commercial data centres or Cloud solutions so that they can remain fully functional in situations like this

How do you describe the impact of the power sector in Nigeria on your connectivity service? Do you have other power sources/reserves and how long can you operate without power from the grid/ diesel shortage or in a lockdown scenario?

Our data centre has a direct connection to the National Grid through Eko Disco. This generally assures us of power availability greater than 90%. This is a critical part of achieving stability for us, and so we have invested in this situation. Beyond that, we have three weeks supply of diesel and arrangements with long term suppliers to replenish each time we go down by a third of our capacity.

Where will you recommend power improvements are made to support the stability and resiliency of your infrastructure?

Most of the power problems we see occur at customer locations. It affects businesses in general here and also limits employees' capacity to work from home. We need to solve the power problem for everyone. It is more of a distribution issue than a generation issue from what I understand

Please indicate any further comments, thoughts or recommendations for the nation regarding connectivity resilience and uptime during emergencies?

I think one of the key observations is how far Nigerian businesses have moved online. However, there is much more that businesses can do to invest in resiliency and outsource services to commercial data centres or Cloud solutions so that they can remain fully functional in situations like this. Some of our customers have not skipped a beat, and their businesses keep running 100% because they had implemented those plans ahead of the COVID-19 crisis.

With the increased demand for connectivity services and as organizations move to work from residences amidst reduced mobility operations, the importance of strategic planning and investing in connectivity resilience cannot be overstated. Given the global economic slowdown and forecasts that a quick recovery in oil prices is not anticipated, the telecommunication sector which currently contributes 10.6% to GDP (NCC, Q4 2019) will become even more critical for a post COVID-19 economic recovery plan.

Additionally sectors like healthcare, manufacturing, agriculture and more which can leverage on the digital economy for acceleration will support cross sector recovery to improve national economic growth. Thus, connectivity providers and organizations across all industries must review their technology strategy, business resilience and disaster recovery planning to ensure they are prepared now and for the unforeseen future.

Contacts

Yemi Saka
Partner, Consulting Leader, West Africa.
ysaka@deloitte.com.ng

Wole Oyeniran
Associate Director, Enterprise Technology & Performance, West Africa.
ooyeniran@deloitte.com.ng

Linda Quaynor
Partner, Strategy, Customer & Marketing, West Africa.
lquaynor@deloitte.com.ng

Roland Teye
Associate Director, Ghana Consulting Marketplace Leader.
rteye@deloitte.com.gh

Joseph Olofinsola
Partner, Human Capital, West Africa.
jolofinsola@deloitte.com.ng

Egomaron Jegede
Telecommunications and Infra-structure SME, West Africa.
ejegede@deloitte.com.ng

Bernard Orji
Partner, Core Business Operations, West Africa.
borji@deloitte.com.ng

Deloitte.