**OPINION ARTICLE**

**Why the Internet's backbone needs urgent protection**

By Alpheus Mangale, SEACOM Group CEO

**JOHANNESBURG - In a world where the Internet powers everything from banking to healthcare, education, security, and even our social lives, we rarely stop to think about the invisible infrastructure keeping it all connected.**

While satellites and wireless networks offer some redundancy, subsea cables remain the backbone of global connectivity. Beneath our oceans, over 600 subsea cables – stretching over 1.4 million kilometres – carry [97% of the world's internet](https://www.mei.edu/blog/subsea-data-cables-security-shared-concern-global-north-and-south) traffic. These fibre-optic cables enable over $10 trillion in financial transactions daily and form the digital economy's backbone.

**A fragile digital backbone**

The demand for connectivity is skyrocketing, with the submarine cable market expected to grow from $18.28 billion in 2023 to [$33.29 billion by 2028](https://www.visualcapitalist.com/cp/charting-the-depths-the-world-of-subsea-cables/). However, this expansion hasn't been matched with the necessary security measures, leaving these critical networks increasingly vulnerable. We need to rethink how we protect this infrastructure before the cracks in our digital foundation become full-blown fractures.

1. Accidents and physical damage

Subsea cables might be engineered for durability but are far from invincible. Fishing trawlers, ship anchors, and dredging cause more than 70% of failures, making maritime activity the most significant threat. Natural disasters like earthquakes and underwater landslides also pose risks. A recent [rockslide near Côte d'Ivoire](https://www.internetsociety.org/resources/doc/2024/2024-west-africa-submarine-cable-outage-report/) severed four major cables, disrupting connectivity in 13 West African countries.

Geopolitical tensions further compound these risks. More cables don't necessarily mean better security. A single, well-placed cut can still wipe out internet access across entire regions, emphasizing the need for stronger protection measures.

1. The power shift in cable ownership

Telecom companies and international technology consortia controlled subsea cables for decades, ensuring balanced global connectivity. But today, global investments are led by a few global tech giants. Although these investments are welcome and answer a global need for the world, they must also be balanced with lesser dependency on them without the risk of domination of new subsea cable projects, which can lead to unprecedented control over global data flow.

While such investments have accelerated infrastructure expansion and improved capacity, they also raise uncomfortable questions: *1) Who controls the data flow? 2) Will nations become dependent on foreign tech giants for connectivity? 3) What happens if these companies prioritize their own services over broader public access?*

With little regulatory oversight, private corporations are shaping the future of global connectivity, determining who gets access, where cables are built, and under what conditions. If left unchecked, this power shift could reshape the Internet in unpredictable ways, making it essential for policymakers to act now.

**What needs to change?**

Strengthening the resilience of subsea cables requires a multi-layered approach, focusing on infrastructure planning, cybersecurity, and international cooperation.

1. Smarter infrastructure planning

Instead of relying on a few key cables, providers must route global internet traffic through multiple diverse pathways to avoid single points of failure. Strategic cable placement is also crucial – many cables run through politically sensitive or high-risk maritime zones, making them vulnerable to accidents and sabotage. Future deployments must prioritize safer, well-planned routes. Additionally, more substantial materials and AI-powered monitoring can help detect early signs of damage and prevent outages before they occur.

1. International cooperation and regulation

A lack of centralized oversight leaves subsea cables exposed to security gaps. Similar to treaties governing airspace and territorial waters, global agreements must set clear regulations for cable security, monitoring, and rapid response. Governments must ensure fair competition and prevent a handful of companies from dictating global connectivity. Collaboration between governments, telecom providers, and tech companies is essential. Protecting subsea cables isn't just a national issue; it's a global priority that requires public-private partnerships and coordinated action to safeguard the future of connectivity.

**Africa needs to act NOW!**

For Africa, the stakes are even higher. Subsea cable landings have proven their economic benefits, with some African nations seeing GDP per capita increase by 6.1% after new cable installations. Broadband penetration has also been linked to a 1.38% increase in GDP growth, proving that digital infrastructure is a key economic driver.

Although [seventy-four submarine cable systems](https://blog.telegeography.com/2025-africa-telecommunications-map) connect the continent, only 50 are currently active, with 24 still under construction. Many African nations, including Togo, Liberia, and Sierra Leone, rely on just one or two subsea cables, leaving them particularly vulnerable to internet blackouts that disrupt daily connectivity, hinder economic growth, and widen the digital divide.

The world's oceans hold critical concentration zones that amplify these tensions. The Strait of Malacca, an essential artery for global trade, processes 114 terabits of daily data traffic and has 14 cable crossings. In 2023 alone, the region reported eight security incidents, with an economic impact potential of up to $4.5 trillion. Similarly, the Suez Canal zone hosts 15 major cables accommodating daily financial flows of $3.2 trillion. Given its severe political risk rating and limited alternative routes, any disruption here would have catastrophic implications. With its seven strategic cables vital for Black Sea connectivity, the Turkish Straits faces a heavy Russian naval presence, which is actively monitored under NATO's protection plans, emphasizing the importance of securing these vital maritime routes.

The East Coast subsea cable system is incredibly fragile, with over 15 cables concentrated in the Red Sea – a concentration zone carrying more than 80% of Africa's internet traffic to Europe and Asia. This single point of failure poses a significant risk, emphasizing the urgent need for new routes, [improved redundancy](https://blog.cloudflare.com/fr-fr/undersea-cable-failures-cause-internet-disruptions-across-africa-march-14-2024?/), and stronger network protections to safeguard Africa's digital future.

As one of Africa's leading subsea cable operators, SEACOM has seen firsthand how fragile digital infrastructure can hold back entire economies. We advocate for more investment in African-owned and managed subsea infrastructure, regional redundancy to prevent single points of failure, and stronger regulatory frameworks to ensure fair access to connectivity. Without bold action, Africa risks becoming increasingly dependent on foreign-controlled internet infrastructure, leaving the continent with little say in how its data moves, who controls it, and what protections are in place.

We assume the Internet will always be there. Still, without urgent action to protect subsea cables, we risk a future where connectivity is unstable, vulnerable to attacks, and controlled by a few influential players. Governments, industry leaders, and telecom providers must act now to safeguard the digital economy and ensure internet access remains open, secure, and resilient. Our digital world depends on it – the time to act is now!

**ENDS**

>1044 words<

**EDITORS' NOTES:**

**About SEACOM**

SEACOM is a diversified ICT provider of scale, offering a wide range of voice, managed networks, security, cloud, and server hosting solutions and services to businesses, network carriers, service providers and enterprises. SEACOM Digital Infrastructure owns and operates one of Africa's largest networks of ICT infrastructure, including multiple subsea cables, a resilient, continent-wide IP-MPLS Network, and Fibre networks in and across the continent. With a network spanning South Africa to Europe and Asia, SEACOM empowers African businesses to connect seamlessly and securely to global markets. Businesses partner with SEACOM's Digital Services for cybersecurity solutions, including firewalls, threat detection, cloud-based solutions and secure network infrastructure, to safeguard their digital assets.