KAIPTC
...where peace begins

POLICY BRIEF 1 | MARCH 2025

Maritime Security and Cyber Resilience in Africa's Digital Infrastructure

Elsie A. Tachie-Menson
Dirk Siebels

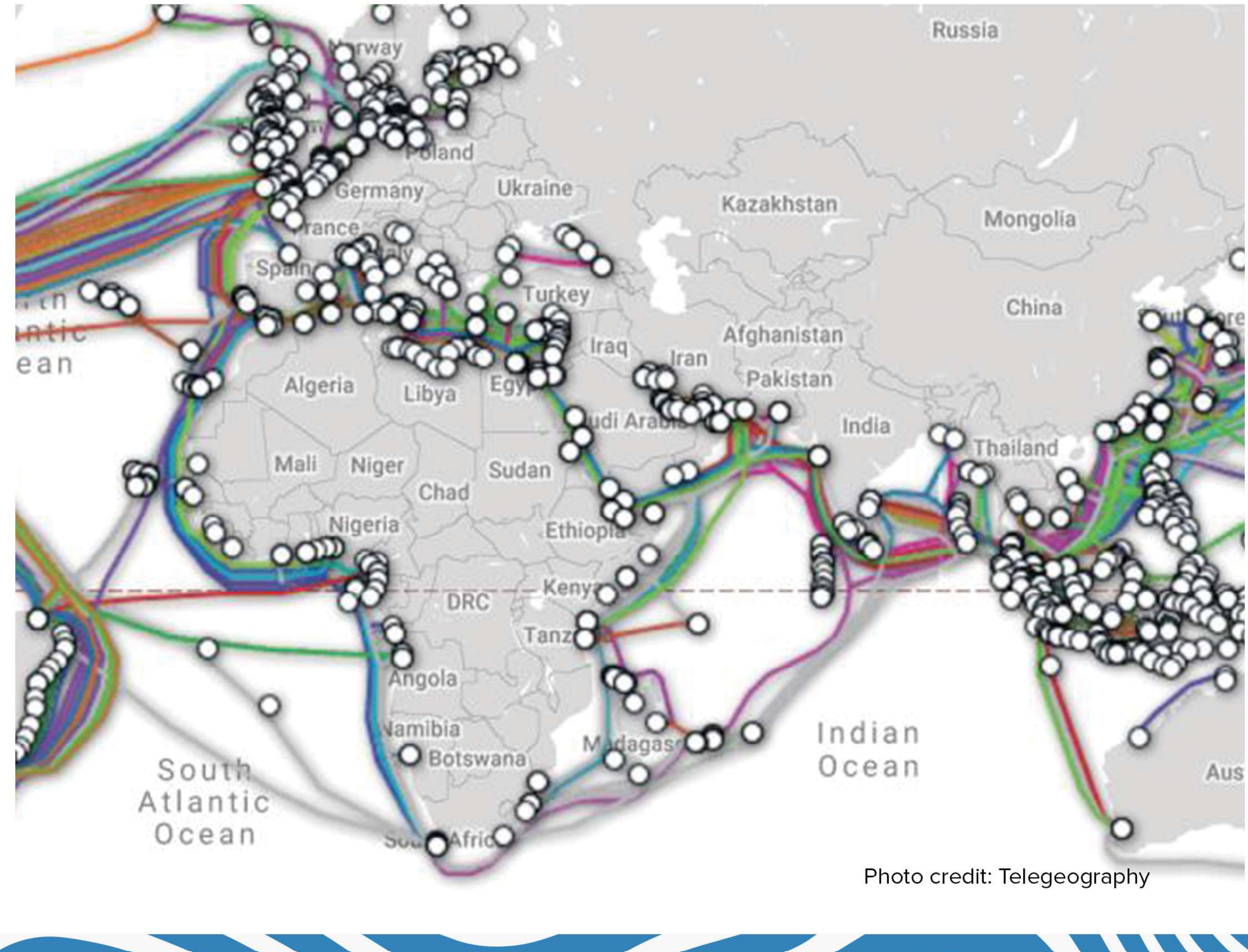

Photo credit: Telegeography

Introduction

On March 14, 2024, Africa experienced a continent-wide internet outage that caused significant disruptions to vital online services and communication channels. The immediate cause of this catastrophe was the destruction of underwater cables in the Red Sea, which occurred as a consequence of attacks by Houthi forces based in Yemen targeting commercial shipping. This policy brief emphasises the deep interdependence between maritime and cybersecurity, emphasising the necessity for a holistic strategy to tackle both concerns.

The vulnerability of underwater cables to maritime activities is not a new phenomenon. There has been a growing awareness of the potential threats posed by state and non-state actors to this infrastructure. The 2024 incident in the Red Sea, however, has brought this issue to the forefront for decision-makers in Africa, highlighting the urgent need for a comprehensive approach to safeguarding subsea cables and the vital services they support.

This policy brief is a heavy commentary which seeks to underscore the critical vulnerabilities exposed by the 2024 internet outage in Africa, advocating with recommendations for stakeholders and to adopt a comprehensive and integrated approach to safeguarding subsea cables and enhancing the resilience of digital infrastructure against maritime and cybersecurity threats

The Africa's Internet Outage in 2024

This major disruption occurred when important subsea cables in the Red Sea were disrupted by the anchor of a ship which had previously been attacked by Houthi militants. These cables were crucial for facilitating internet connectivity throughout Africa, acting as indispensable channels for transmitting data between continents. The disruption caused widespread internet outages across the continent, cutting off access to vital online services such as banking, healthcare, and emergency communication systems.

The incident occurred as tensions in the region had already increased. Houthi forces had conducted their attacks against merchant ships as a means to expand their influence. They had successfully disrupted an important international trade route with maritime traffic through the Red Sea dropping by 50-60 percent as many ships were re-routed around the Cape of Good Hope. The Houthi attacks occurred at a time of increased geopolitical tensions as well, raising further concerns about the susceptibility of subsea cables to threats from both state-sponsored and non-state actors.

Due to the cable damage, a substantial number of individuals and businesses throughout Africa encountered major disruptions. The power outage obstructed economic activities, restricted information availability, and hampered the provision of vital services. While telecommunications companies swiftly worked to redirect traffic and reinstate connectivity, the magnitude of the damage meant that recovery endeavours were protracted and intricate. This incident not only caused a disturbance in everyday activities but also emphasised the crucial significance of maritime security in preserving the reliability of worldwide communication networks.

The incident highlighted the interdependence of maritime and cybersecurity. The dependence on tangible infrastructure for digital communication has exposed weaknesses that can be manipulated by malicious individuals. This incident highlights the importance of implementing a comprehensive strategy to protect various types of maritime assets.

The Consequences of the Outage

Highlighting the interdependence of our virtual and tangible realms, the internet outage has extensive repercussions. The interplay between maritime security challenges and cybersecurity can have substantial consequences. The lack of access to internet services and limited communication capabilities have exposed the ever-present susceptibility of our dependence on digital infrastructure, which is frequently contingent on physical components such as subsea cables.

This occurrence highlighted that maritime activities may have far-reaching consequences on land. Targeting infrastructure, such as subsea cables, may cause extensive and catastrophic consequences across several sectors, including telecommunications, banking, healthcare, and transportation. In Côte d'Ivoire, hospitals faced challenges accessing patient records due to disruptions in internet connectivity. This delayed critical medical procedures and telemedicine consultations, as reported by NetBlocks and local providers like Orange CI and MTN.[1] In Nigeria, major banks such as Sterling Bank experienced outages that

[1] Le Monde Africa. (2024, March 15). Internet outage hits several African countries as undersea cables fail. *Le Monde*. Retrieved from https://www.lemonde.fr/en/le-monde-africa/article/2024/03/15/internet-outage-hits-several-african-countries-as-undersea-cables-fail_6621444_124.html

rendered banking apps and USSD services unusable. Customers were unable to perform transactions, causing significant disruptions in financial operations.[2] Similarly, South African banks relying on the West Africa Cable System (WACS) faced connectivity issues that slowed down online banking services.[3] South African fruit exporters reported delays in tracking shipments to Europe due to cable failures affecting data transmission. This led to logistical inefficiencies and potential spoilage of goods.[4] MTN Group and Vodacom confirmed intermittent connectivity issues across multiple countries due to damaged subsea cables, including ACE and WACS systems. These providers struggled to reroute traffic through alternative paths while awaiting repairs.[5] Lemfi, an African remittance startup, informed customers of downtime caused by the outage, disrupting cross-border financial transactions.[6] Businesses across Ghana and Liberia also reported reduced internet speeds, affecting their ability to deliver services efficiently.[7]

This emphasises the necessity for a thorough understanding of how maritime and cybersecurity interplay, as either can have a knock-on impact on the other.

In addition, the widespread internet outage throughout the continent exposed the absence of robustness and redundancy in communication networks. The fact that a solitary weak spot, such as the disrupted subsea cables, led to a broad-scale lack of connection underlined the need to expand communication infrastructure and strengthen the overall durability of digital networks.

Lessons Worth Noting

The 2024 internet outage in Africa highlights the interdependence of our society and the repercussions that can arise from disruptions to vital infrastructure. Although the initial effects were primarily experienced in the areas of communication, commerce, and everyday activities, the wider significance of this event goes well beyond the boundaries of the digital realm.

The susceptibility of underwater cables to maritime threats highlights the delicate nature of the systems that are essential for the functioning of modern society. The potential disruption of these physical connections within the global network has the capacity to weaken the fundamental basis of our interconnected world, gradually eroding the confidence in the stability and dependability of the systems we depend on.

Furthermore, the incident in 2024 – in combination with similar cases in other areas such as the Baltic Sea and the Taiwan Strait – serves as a warning example of how maritime security challenges can worsen pre-existing tensions and conflicts. In a society where having access to information and communication is considered a valuable advantage, the deliberate targeting of subsea cables can be seen as a type of hybrid warfare.

As policymakers and stakeholders analyse[8] the consequences, it is evident that a fresh approach is necessary. This approach should acknowledge the vital significance of maritime security in protecting the digital infrastructure that plays a crucial role in our modern lives. This strategy must be comprehensive, including not only the physical safeguarding of underwater cables but also the creation of strong backup plans and the promotion of international collaboration.

The incident serves as a reminder of the vulnerability of the systems that support our interconnected world and the pressing need to address the weaknesses that jeopardise their stability. By acknowledging the significant consequences of maritime security challenges on the digital domain, we can initiate the formulation of strategies and solutions required to construct a future that is more robust and protected for everyone. To that effect, we suggest the following forward-facing approaches in the next section.

[2] Opejobi, A. (2024, March 14). Fibre cut takes banks offline. *TechCabal*. Retrieved from https://techcabal.com/2024/03/14/fibre-cut-takes-banks-offline/

[3] Ibid.

[4] David, O. (2024, March 14). Several African countries suffer Internet disruptions due to damaged submarine cables. Techpoint Africa. Retrieved from https://techpoint.africa/2024/03/14/several-african-countries-suffer-internet-disruptions/

[5] Le Monde Africa. (2024, March 15). Internet outage hits several African countries as undersea cables fail. *Le Monde*. Retrieved from https://www.lemonde.fr/en/le-monde-africa/article/2024/03/15/internet-outage-hits-several-african-countries-as-undersea-cables-fail_6621444_124.html

[6] Opejobi, A. (2024, March 14). Fibre cut takes banks offline. *TechCabal*. Retrieved from https://techcabal.com/2024/03/14/fibre-cut-takes-banks-offline/

[7] Le Monde Africa. (2024, March 15). Internet outage hits several African countries as undersea cables fail. *Le Monde*. Retrieved from https://www.lemonde.fr/en/le-monde-africa/article/2024/03/15/internet-outage-hits-several-african-countries-as-undersea-cables-fail_6621444_124.html

[8] A report from RETN(a telecommunications company) revealed that the damage affected up to 70% of Europe-Asia data traffic, far exceeding initial estimates, and emphasised the need for additional cable routes to prevent single points of failure. Also, The International Cable Protection Committee (ICPC) noted that most incidents involving cable damage are caused by activities like anchoring, as seen in this case where a ship's anchor severed multiple cables during Houthi attacks.

Recommendations

The authors offer the following approaches:

• Governments in Africa and regional organisations like the African Union should establish a Subsea Cable Protection Task Force to coordinate efforts in safeguarding underwater cables. This includes enforcing spatial separation between cables and maritime activities, as recommended by the International Cable Protection Committee (ICPC). Additionally, governments should adopt regulations that mandate cable route planning to avoid high-risk areas, such as conflict zones or regions prone to heavy maritime traffic.

• Telecom companies should invest in redundant and diverse cable routes to mitigate the risk of single points of failure. Deploying multiple cables along varied paths will ensure that connectivity can be maintained even if one cable is damaged. Operators should also implement advanced fibre-optic sensors and AI-driven monitoring systems to detect potential disruptions early and enable swift repairs.

• The International Telecommunication Union (ITU) and the International Cable Protection Committee (ICPC) should promote global best practices for cable resilience. This includes facilitating agreements between countries to protect subsea cables under international law, such as the United Nations Convention on the Law of the Sea (UNCLOS), and encouraging joint investments in cable infrastructure security.

• Governments and private operators must enhance cybersecurity protocols for subsea cable networks. This involves deploying end-to-end encryption for data transmitted through cables and implementing robust defences against cyberattacks targeting critical infrastructure. National cybersecurity agencies should collaborate with telecom operators to conduct regular vulnerability assessments.

• Governments should foster public-private partnerships to fund research and development in satellite technology and alternative communication methods.These technologies can provide backup connectivity during outages, reducing reliance on subsea cables alone. PPPs can also support training programs for rapid response teams specialised in cable repair and maintenance.

Conclusion

The internet blackout in Africa, resulting from the disruption of subsea cables as a consequence of attacks by Houthi forces based in Yemen targeting commercial shipping, highlights the interdependence of maritime security and cybersecurity. This episode exemplifies the significant influence that maritime matters may have on our digital existence, underscoring the necessity for a comprehensive and cooperative strategy to tackle these difficulties. Policymakers and stakeholders must acknowledge the interconnections between the physical and digital domains and collaborate in order to strengthen the resilience and security of our linked world.

Sources

• CNN. (2024, March 4). *Red Sea cables have been damaged, disrupting internet traffic.* Retrieved from https://www.cnn.com/2024/03/04/business/red-sea-cables-cut-internet/index.html

• Techpoint Africa. (2024, March 14). *Several African countries suffer Internet disruptions due to undersea cable damage.* Retrieved from https://techpoint.africa/2024/03/14/several-african-countries-suffer-internet-disruptions/

• CSIS. (2024, March 7). *Red Sea Cable Damage Reveals Soft Underbelly of Global Economy.* Retrieved from https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy

• Halog, J., Margat, P., & Stadermann, M. (2024). Submarine Infrastructures and the International Legal Framework. *Transactions on Maritime Science, 13*(1).

• Folk, Z. (2024, March 4). Four fiber optic cables damaged in Red Sea—Here's what we know. *Forbes*. Retrieved from https://www.forbes.com/sites/zacharyfolk/2024/03/04/four-fiber-optic-cables-damaged-in-red-sea-heres-what-we-know/

• Total Telecom Staff. (2024). Submarine cable damage in the Red Sea severely underestimated. *Total Telecom.* Retrieved from https://totaltele.com/submarine-cable-damage-in-the-red-sea-severely-underestimated/

About the Authors

Elsie Amelia Tachie-Menson is a researcher and an editorial professional at the Department of Research at the esteemed Kofi Annan International Peacekeeping Training Centre (KAIPTC) located in Accra, Ghana.

Dr. Dirk Siebels (PhD) is a senior analyst at Risk Intelligence, a Denmark-based security intelligence company. His research areas include maritime security-related issues with a focus on commercial impacts, ranging from day-to-day impacts to long-term consequences.

How to Cite

Tachie-Menson. E. A. & Siebels. D. Maritime Security and Cyber Resilience in Africa's Digital Infrastructure. *Policy Brief 1*, March, Accra: KAIPTC.

About

The opinions expressed in this policy paper do not necessarily reflect those of the Kofi Annan International Peacekeeping Training Centre, its Governing Board or partners. Authors contribute to KAIPTC publications in their individual capacity

About the Centre

Kofi Annan International Peacekeeping Training Centre (KAIPTC) is an ECOWAS Centre of Excellence that provides globally recognised capacity for international actors on African peace and security through training, education and research to foster peace and stability in Africa.

KAIPTC ...where peace begins

Scan to see all Publications

KOFI ANNAN INTERNATIONAL PEACEKEEPING TRAINING CENTRE
PMB CT 210, CANTONMENTS, ACCRA-GHANA | T: 233(0)302718200 | F: 233 (0)302718201
www.kaiptc.org kaiptcgh kaiptc kaiptc-official page