Seapower for Africa Symposium 2024

Cape Town, South Africa

Cybersecurity and Subsea Cables: Protecting Critical Infrastructure

Dr Osei Bonsu Dickson

Founding Partner, LexMu

Lex Mundus & Cencla PRUC

International Law Firm

LEX MUNDUS & CENCLA PRUC

CYBERSECURITY LAW | MARITIME LAW | NATIONAL SECURITY LAW | INTERNATIONAL ARBITRATION

Cybersecurity and Subsea Cables: Protecting Critical Infrastructure

DR. OSEI BONSU DICKSON

Founding Partner, LexMu, Speaker

Dr. Osei Bonsu Dickson is an expert in international cybersecurity law. He was Director of Policy at Ghana's Ministry of National Security. Previous to that he was Chief Legal Advisor, Director, Security Governance and Director of Intelligence Analysis. In August 2024, Dr. Dickson awarded the *Distinguished Cybersecurity Personality of the Year* 2024 Award. He is a member of the Board of Directors of Ghana's Financial Intelligence Center and the Ghana Boundary Commission. He is Chairman of Africa's largest cyber incident response conference – CyberX Africa. He was educated at the University of Ghana, Harvard University, Ghana School of Law and Rushford Business School.

PROF. KWADWO APPIAGYEI-ATUA

Chairman, LexMu

Professor Kwadwo Appiagyei-Atua is Associate Professor of Law at the University of Ghana School of Law, where he teaches Public International Law and International Human Rights Law. He has served as a consultant for various inter-governmental organizations and international civil society organizations such as United Nations Office on Drugs and Crime (UNODC) on its Education for Justice (E4J) initiative; the Open Society Foundation's Global Program on Drug Policy (GPDP) and Open Society Initiative for West Africa (OSIWA). He isa board member of the Global Observatory on Academic Freedom, Central European University, Vienna, Austria.

Overview:

- Subsea cables are vital to global communications, carrying 99% of international data traffic.
- They have become a growing concern for cybersecurity due to increased cyber threats targeting critical infrastructure.
- Major seaports suffered average of 10 to 12 cyber attacks daily in 2017. Trend continues to grow - attacks on maritime transport increased by 400% in 2020.
- The ICPC has continuously highlighted strategic role of subsea cables and the need to protect them from physical and cyber threats.

Role and Features of Subsea Cables

- Private companies own and operate more than 500 commercial subsea cables that form the backbone of the internet.
- Subsea cables carry about 99% of transoceanic digital communications (e.g., voice, data, internet), including financial transactions.
- Important for sectors like finance, telecommunications, communications and governments.

Subsea Cable Cuts and Foreseeable Cyber Attacks

Africa Region

- In January & April cable cuts on WACS and SAT3 led to complete outages in West and Southern Africa - impact was region-wide.
- Remote network mgt systems now being used to operate cables, which opens up avenues.
- Best known cyber-attack on subsea cables occurred in April 2022, when US claimed it had foiled an attack on underwater cable linking Hawaii and the Pacific Region.

West African Cable System (WACS) and South Atlantic Telecommunications cable no.3

Vulnerabilities of Subsea Cables:

Africa Region

- Physical threats: natural disasters, fishing activities, and sabotage.
- Cybersecurity risks: wiretapping, data interception, denial of service (DDOS) attacks, risks of cyber espionage, and interference.
- Potential physical or cyber attack on cable landing stations and infrastructure.

West African Cable System (WACS) and South Atlantic Telecommunications cable no.3

Legal Frameworks

Global

- International Regulations Protecting Subsea Cables.
- UN Convention on the Law of the Sea (UNCLOS)
- UN Convention on Cybercrime
- Budapest Convention
- Malabo Convention
- National Frameworks and Cybersecurity Protocols for Cable Protection

Soft Law (Non-Binding Guidelines and Standards)

- Tallinn Manual on Cyber Warfare: Provides a set of non-binding legal guidelines on how international law applies to cyber operations, including those targeting critical infrastructure like undersea cables.

- NIST Cybersecurity Framework (National Institute of Standards & Technology): Widely adopted globally, NIST's framework includes best practices for securing critical infrastructure, including maritime systems.

- OECD Guidelines for Security of Information Systems and Networks: Offers non-binding recommendations on securing digital infrastructure, relevant to protecting undersea cables from cyberattacks.

- EU "Cable Security Toolbox" : An EU initiative that provides guidelines and risk mitigation strategies to protect submarine cable infrastructure across the continent.

Cybersecurity Best Practices for Subsea Cables:

- Secure cable infrastructure and landing stations.
- Encryption technologies to safeguard data transmission.
- Collaboration between governments, private sector, and international organizations.
- Real-time monitoring and detection systems for cyber intrusions.

Current and Emerging Trends in Cybersecurity:

- Secure cable infrastructure and Content:
- Growing use of AI and machine learning for cable monitoring.
- Development of quantum encryption methods for subsea cables.
- Emerging threats, such as ransomware attacks on critical infrastructure.

Challenges in Protecting Subsea Cables

- Geographic challenges: cover thousands of kilometers under the sea.
- Jurisdictional complexities: cables crossing multiple countries and territorial waters.
- High costs of monitoring and protecting cables.

Future of Subsea Cable Security

Africa Region

Jurisdiction and ownership of landing stations may ground claim for damages for IWAs

UNCLOS Art 113 provides clear obligation to protect subsea cables and prosecute willful or negligent damage to them.

Attribution is complex. Budapest/UNC allows cross-border cooperation in investigation and prosecution of subsea cybercrimes.

AI Innovations in cyber tools likely to resolve in better protection.

Education on cyber-physical threats will be crucial to ensuring security.

LEX MUNDUS & CENCLA PRUC
International Law Firm

Quo Vadis

Maritime Cybersecurity

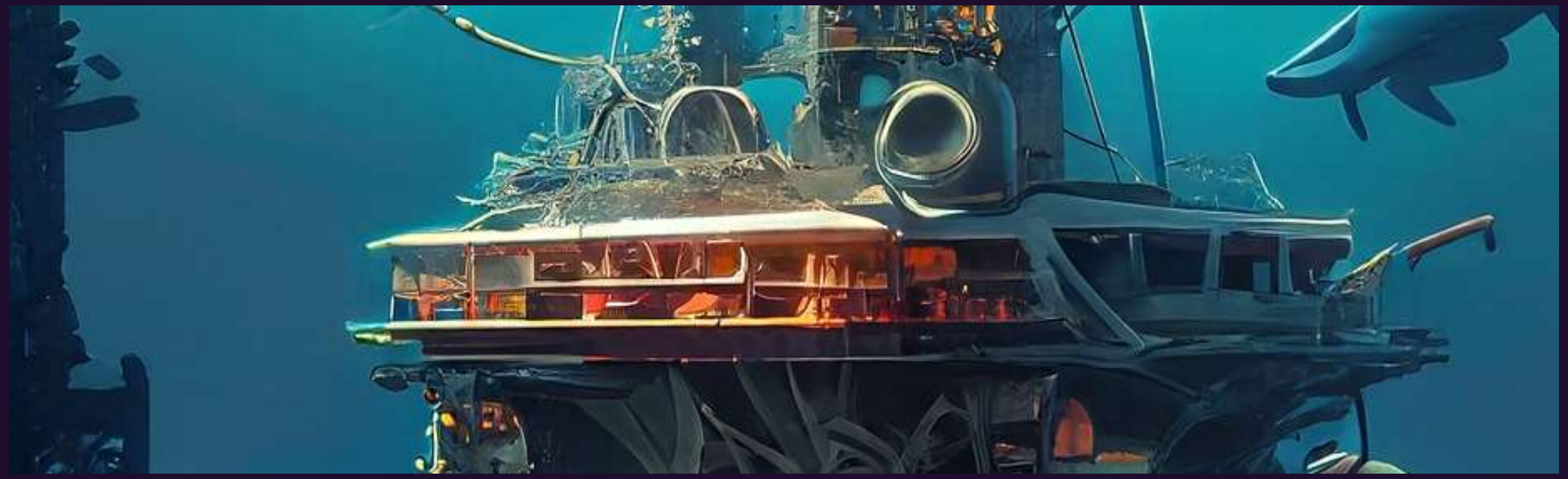
A shift or change has occurred in the very landscape of maritime threats:

- Where there is no change, there is no growth
- Change is inevitable
- Africa region must adapt or perish

Closing Discussions
Q & A

Seapower for Africa Symposium
Cape Town

Lex Mundus & Cencla PRUC
International Law Firm



Dr Osei Bonsu Dickson FCIMA ArbP

Lex Mundus + Cencla PRUC
T: +233 241 022 964 E: obdickson@gmail.com
GHANA

15 October, 2024