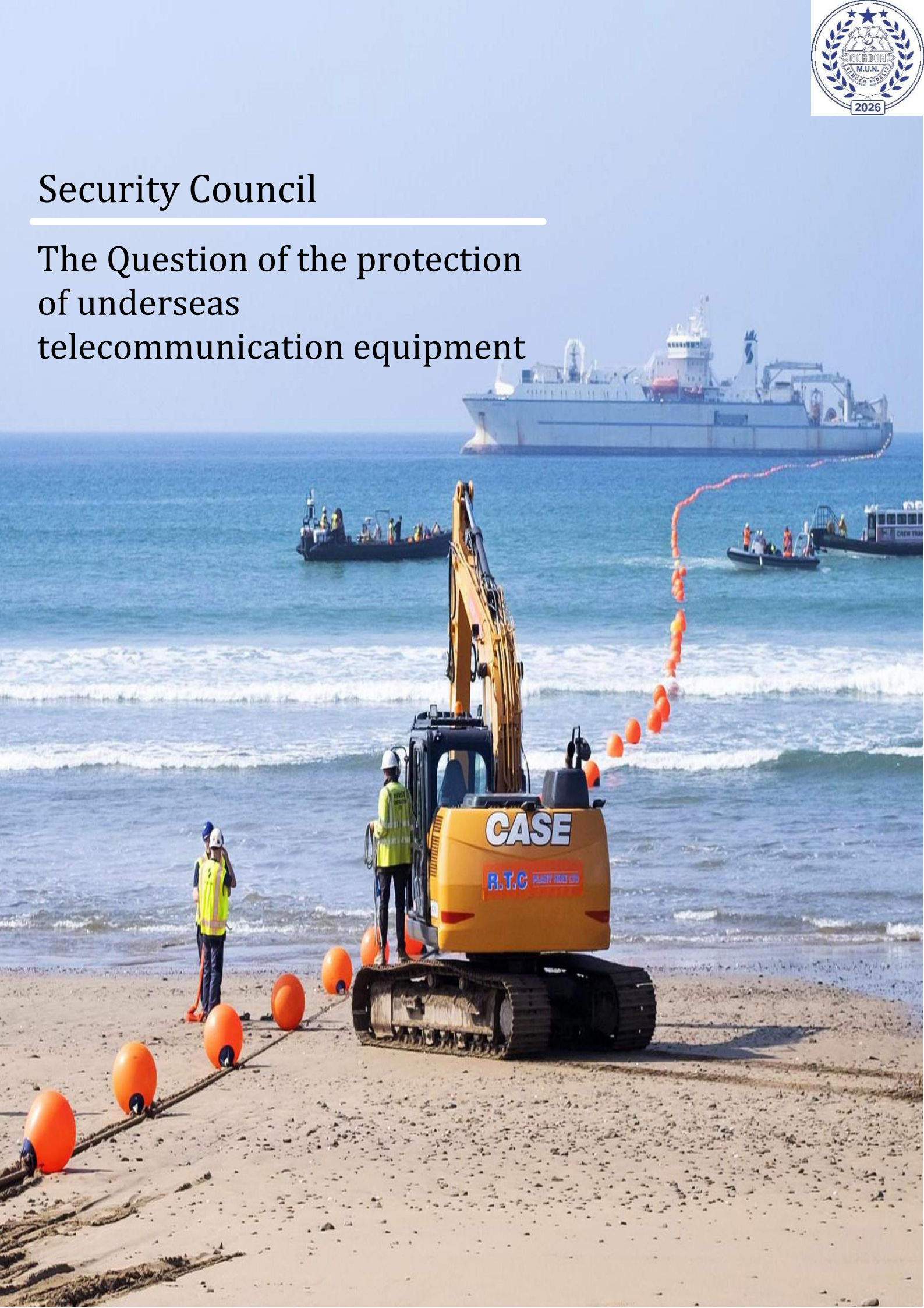
Security Council

The Question of the protection of underseas telecommunication equipment



Committee: **Security Council**

Topic: **The Question of the protection of underseas telecommunication equipment**

Chair: **Eloise Tindale and Ella Mathews**

Summary

The protection of undersea telecommunication equipment, especially fibre-optic submarine cables, is vital because these systems carry almost all international data traffic, including internet, financial, and government communications. Damage or sabotage to key cables can quickly disrupt whole regions, making this a major concern for the UN Security Council and global security.

Overview / Explanation of the topic:

Undersea cables are fibre-optic lines laid on the seabed that link continents and allow data to flow between countries at high speed. They are vulnerable to accidental damage from fishing and anchoring, natural hazards, and deliberate actions such as sabotage or espionage, especially near shallow coastal areas and chokepoints.

Origins of the topic:

The first submarine telegraph cables were laid in the nineteenth century, but the issue became critical since the 1980s when fibre-optic cables replaced satellites as the main way to carry international communications. Growing dependence on digital infrastructure and recent incidents of suspected sabotage have pushed cable security onto national and UN agendas.

Why the topic is important:

- Disruption of a small number of key cables can cause major internet outages, interrupt financial transfers, and affect emergency and military communications.
- Because of this, attacks on cables could be used as tools of hybrid warfare or coercion, directly threatening international peace and security.

Who the topic effects:

- Coastal and maritime powers such as the United Kingdom, United States, France, China, and Japan, which host many landing stations and depend heavily on cables for their economies and militaries.
- Transit and chokepoint states like Egypt (Suez/Red Sea), Denmark (North Sea/Baltic), and Singapore, where many cables pass through narrow sea routes and are therefore strategic and vulnerable.
- Small islands and developing states in regions such as the Pacific and parts of Africa, which may rely on only one or two cables and can suffer severe national outages if a single link is cut.

Previous attempts to fix the problem:

- International law, notable the UN Convention on the Law of the Sea (UNCLOS), sets rules for laying and maintaining cables and calls on states to criminalise their intentional damage, though enforcement and coverage remain limited.
- States and industry have created cable protection zones, increased route redundancy, improved monitoring, and strengthened cybersecurity for cable systems, but there is still no comprehensive, globally coordinated protection regime.

Definition of Key Terms

- **Undersea (submarine) telecommunication cable**: A fibre-optic cable laid on the seabed between two or more countries to carry internet, phone, and/or data signals across oceans.
- **Undersea telecommunication equipment:** All the physical parts of the system, including the cables themselves, repeaters (devices that boost the signal), branching units, and landing stations on the coast.
- **Landing station:** A protected facility on land where an undersea cable comes ashore and connects into the national telecom network.
- **Chokepoint:** A narrow or crowded area (for example, a strait or canal) where many cables pass close together, so damage or attack there can have a big impact.
- **Hybrid warfare:** A strategy that uses a mix of military force and non-military tools (like cyber-attacks or sabotage of infrastructure such as cables) to pressure or weaken another state.
- **Critical infrastructure:** Systems and assets that are essential for a country to function (such as energy grids, financial systems, and communication networks), whose failure would cause serious harm.
- **UNCLOS (United Nations Convention on the Law of the Sea):** The main international treaty that sets out states' rights and responsibilities at sea, including rules on laying and protecting submarine cables.
- **Resilience (of cables):** The ability of the cable network to keep working or recover quickly even if cables are damaged or destroyed, often through redundancy and backup routes.

Major Countries / Organisations Involved

- United States – Major owner/user of trans-Atlantic and trans-Pacific cables; strong interest in protecting global cable infrastructure.
- United Kingdom – Hosts landing stations and is a key hub for Atlantic cables and European connectivity.
- France – Important Atlantic and Mediterranean cable routes and strong role in EU security discussions.

- China – Rapidly expanding role as a cable financier, builder, and user across Asia, Africa, and Europe.
- Japan – Major Pacific cable hub and investor in regional and trans-Pacific systems.
- Egypt – Crucial transit state at the Suez/Red Sea chokepoint where many Europe–Asia cables pass.
- Singapore – Key regional hub for South-East Asian and Indo-Pacific cables.
- Denmark and other North Sea/Baltic states – Host important regional cables and have raised concerns about Russian activity near infrastructure.
- Small island states (e.g. Fiji, Seychelles, Mauritius, Caribbean islands) – Highly dependent on a small number of cables and involved in resilience and funding discussions.