# *Research Report*

## Model United Nations Oud-Beijerland 2026

**Crisis Committee**

**Responding to coordinated threats against global trade routes and communication networks**

**Lea van Alphen and Cynthia de Jong**

## Introduction

Global trade routes and communication networks are essential for the daily lives of human beings all over the world. When these routes or networks face threats, this can lead to companies, organizations, or communities being isolated and disrupted, leading to financial troubles in case of bank attacks, internet outages, cutoffs of the supply of products from other countries, etc. Though oftentimes, issues within these trade routes and communication networks are caused by human error or lone criminals, a coordinated threat can be a lot more damaging, as this entails that multiple attacks are planned around the same time. These planned attacks can be executed by state orders or by other organizations, and may include attacks on communication cables, commercial traffic, or cyberattacks. The goal of the Crisis Committee is to appropriately respond to current threats to global trade routes and communication networks, and to develop a security plan to protect against future threats.

## General Overview

Global trade routes are the aerial, maritime, and terrestrial pathways through which goods are generally transported to other countries or continents. If these pathways are hindered or blocked, the economies and welfare of countries around the world will suffer. The obstruction of so-called chokepoints, narrow sea passages where trade passes through, can have especially vast effects due to the reliance of many global trade on these chokepoints. For example, the Strait of Hormuz has been mostly blocked since February 2026 due to the current war in Iran. This blockage has led to longer shipping routes, and since normally, approximately 25% of maritime oil trade passes through the Strait, this has led to a rise in oil prices across the world due to fuel costs, as well as energy concerns in nearby countries that relied on imported oil. This demonstrates the international effects that the physical blockage of such a chokepoint can have. International communication networks transport information between countries. Threats may include physical attacks, like disruption of infrastructure such as cables, data centers, or satellites, or cyberattacks. Such a cyberattack occurred in June 2017, when the NotPetya cyberattack targeted Ukrainian and international websites, disrupting banks, governments and trade, including the activities of the shipping company Maersk. It can be difficult to monitor and protect submarine cables; however, since over 95% of international data traffic happens through undersea cables, it is especially important to ensure the

protection of infrastructure involving these. Disruption of communication networks via these attacks may affect financial services, governments, privacy, and healthcare.

Vital locations to protect include so-called canal chokepoints like the Suez Canal, the Strait of Hormuz, and the Panama Canal, where many ships depend on a singular route. Singapore is also a vulnerable target due to its strategic role in international shipping and trade.

Coordinated threats may originate from international conflict, with states striving for political or economic advantages, or from organized crime. For example, criminal groups may attempt to steal data, attack businesses, or extort money from businesses or organisations. However, since not every disruption is deliberate, thorough investigations need to be carried out before measures against states or organisations are carried out.

Finally, it is important to consider that not all member states will support measures that improve the security of global trade routes and communication networks, due to geopolitical conflicts between states or economic dependency. Furthermore, many countries will not support the implementation of measures against states such as sanctions. Therefore, the Crisis Committee needs to strive to create a consensual, effective, and cooperative resolution to tackle the issue of coordinated threats against global trade routes and communication networks.

## Major Parties Involved

### European union

The European Union (EU) depends heavily on communication networks and international trade. The EU therefore strongly supports international cooperation and security measures such as the protection of critical infrastructure.

### NATO

The North Atlantic Treaty Organisation (NATO) also contributes to the protection of infrastructure in areas important to its members. For example, in January 2025, NATO established Baltic Sentry with the goal of strengthening the security around Baltic Sea cables through enhanced surveillance and enforcement to help detect and respond to threats.

### IMO, ICPC and ITU

There are several international cooperative organisations that address the security of trade routes and communication networks. The International Maritime Organisation (IMO) addresses maritime safety and international shipping, while the International Cable Protection Committee (ICPC) focuses on the security around submarine cables. Finally, the International Telecommunication Union, a specialised agency of the United Nations, coordinates cooperation regarding communication networks.

### United Nations (UNCLOS & UNSC)

The United Nations Convention on the Law of the Sea (UNCLOS) is an international treaty adopted in 1982, which establishes rules regarding maritime activities such as the laying of maritime cables, while respecting the rights of individual countries.

Though the United Nations Security Council (UNSC) may be limited in its ability to counter attacks caused by geopolitical motives due to its veto rights, the UNSC is involved in ensuring the international security of all countries, including in the field of trade and communication.

### Private sector

Finally, trading and communication companies, such as Maersk and Orange, a telecommunications company that operates international cable infrastructure, are strongly involved, as they build and operate trade and communication systems. These companies may provide technical knowledge and report suspicious cases. To ensure the proper execution of solutions employed by the Crisis Committee, it will therefore also have to cooperate with companies within the private sector.

## Possible Solutions

A viable resolution is not limited to, but may include, clauses that work towards the following solutions:

- The protection of vulnerable infrastructure against coordinated threats via funding, monitoring, information sharing regarding suspicious activities, and cooperation with experts.
- The strengthening of cybersecurity within countries by means of international cooperation.
- The reduction of international tensions that may cause coordinated attacks by carefully establishing responsibility and, where appropriate, responding with diplomatic negotiations or other measures such as targeted sanctions.
- The preparation of governments, businesses, and citizens via established emergency and recovery plans.
- The development of the quality and quantity of alternative communication networks and trade routes to reduce dependency on singular pathways.
- The improvement of international cooperation via information sharing or providing experts in order to equalize the quality and security of trade routes and communication networks across the world.