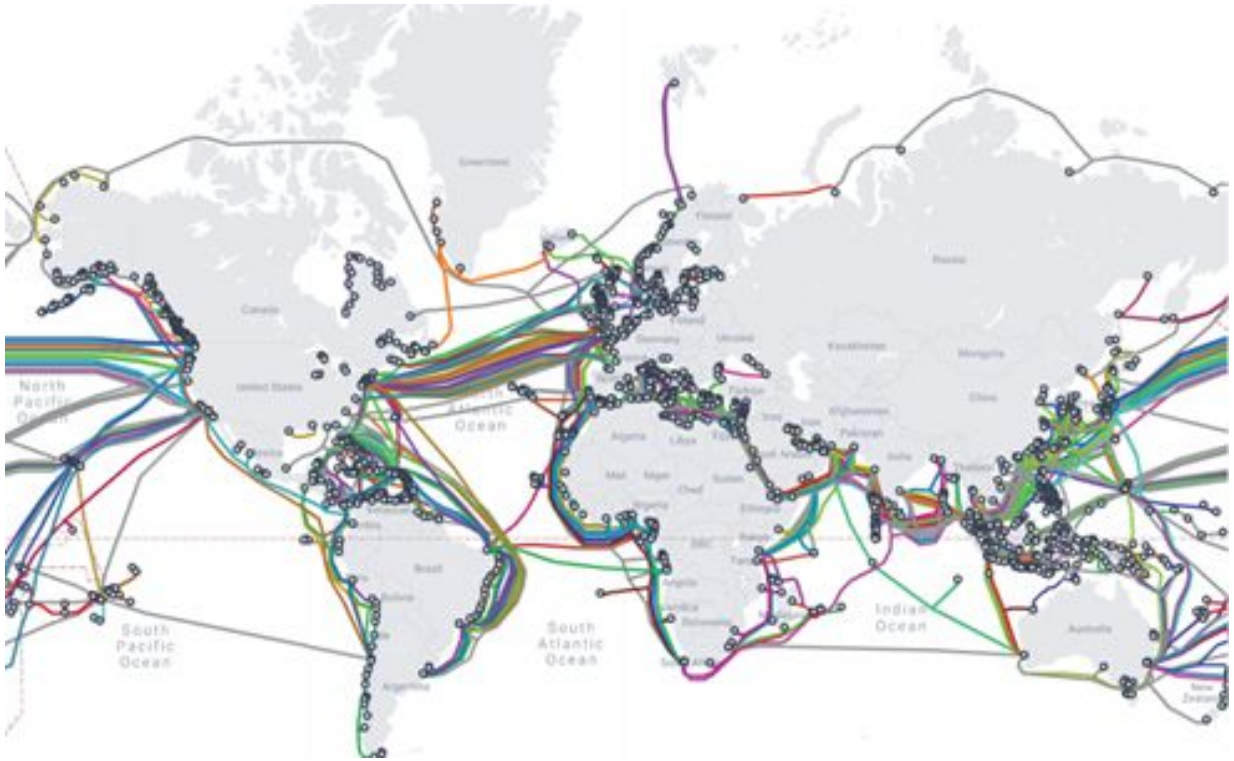
# Protection of CUI: challenges, and solutions




Cdr (OF-4) NLD N Rutger van der Werff, MSc

NMW COE

*Concept Development & Experimentation Branch Head*

# AGENDA

- Challenges:
  - legal,
  - technical,
  - operational challenges

- Solutions for enhancing CUI protection:
  - legal,
  - technical,
  - operational solutions,
  - cooperation & coordination



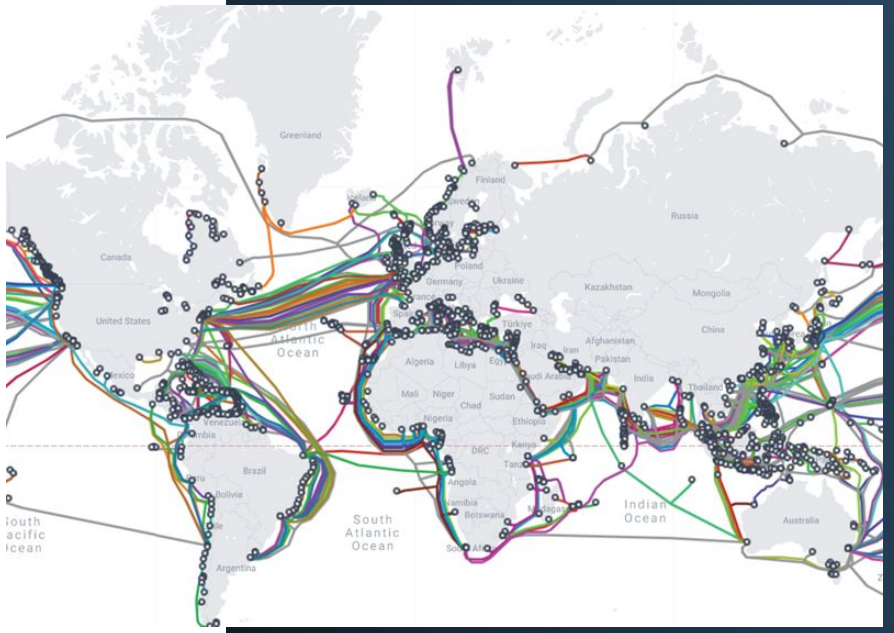
# Critical Underwater Infrastructure: Challenges

- Legal: UNCLOS and the 1884 Cable convention
- Technical: it requires limited technical expertise and resources to damage CUI.
- Operational: which vital infrastructure does one specifically want to protect?

# Critical Underwater Infrastructure: Challenges (MCM-related)

- Huge distances to protect. 900000 miles of underwater cables, 20000 miles of gas pipelines worldwide. HMS: 1nm2/hr. Newer AUV: 2 to 3 times faster. Post- mission analysis.

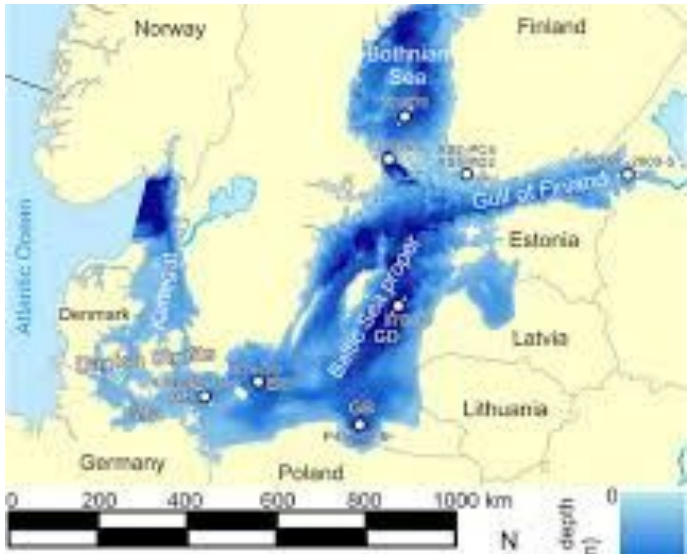
- Detect to engage- cycle. Operators are trained to look for mines. (Remotely) Removing is not our specialty.

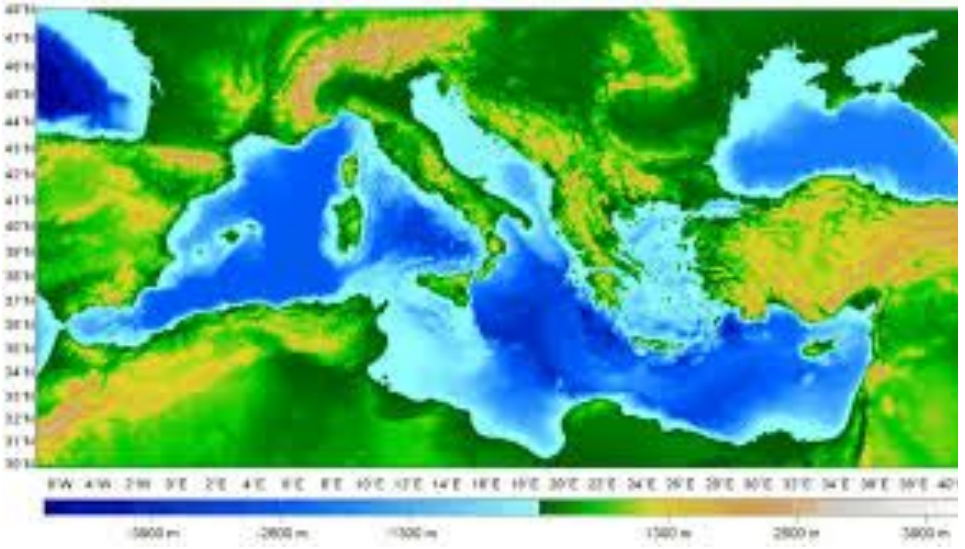


# Critical Underwater Infrastructure: Challenges (MCM- related)

## WATERDEPTH

Baltic sea
Average: 53 m
Deepest: 459 m



Med. Sea
Average: 1500m
Deepest: 5100m

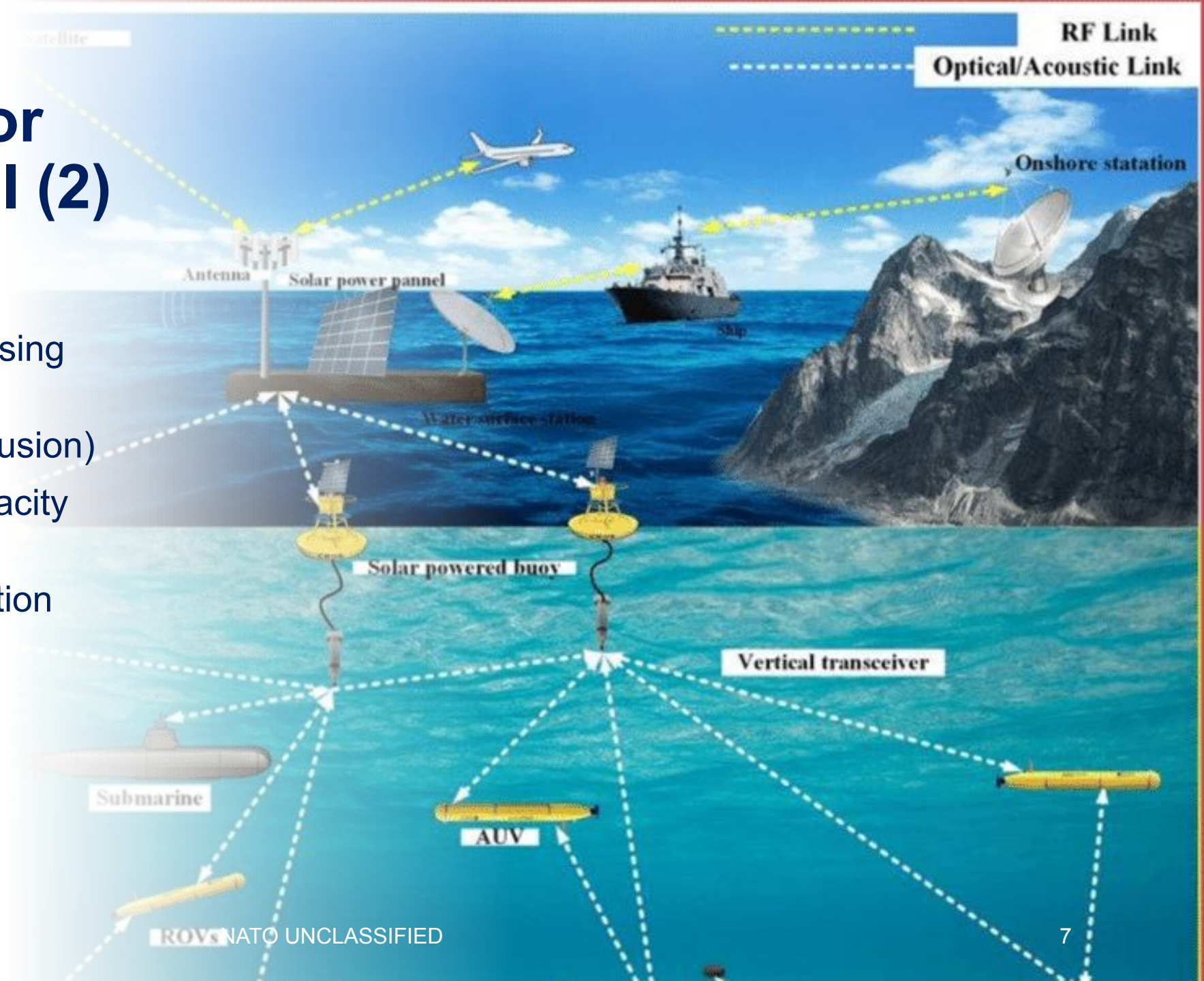
MCM systems: not all go this deep.

# Solutions for protecting CUI (1) Legal

- Intergovernmental organization (UN or it's ITU) to establish internationally recognized protocols under a formalized protection plan
- Give jurisdiction to the cable owner's state. The cable owner's state could take the perpetrator's state to court
- Can Space Law help (EU)?

# Solutions for protecting CUI (2) Technical

- Distributed acoustic sensing (DAS).
- Network of sensors (intrusion)
- Redundancy, and a capacity to repair
- Use of Explosive Collection ROV (Seaeye FALCON, VVLAI ROVs) or
- Divers with Atmospheric Diving Suits (up to 300 meters)



# Solutions for protecting CUI (3) Operational

- Assessment of criticality versus vulnerability (to direct limited resources)
- Continuous Surveillance (Baltic Sentry, NATO Task Force X)
- Route survey on CUI (mapping)
- SNMCMG1 and 2 for CUI protection.
- Joint expeditionary Force (JEF). Nordic Warden




# Solutions for protecting CUI (4)

- Enhanced Cooperation:
  - Centre for Security of Critical Undersea Infrastructure (NATO),
  - North Sea Agreement: Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom
  - Seabed Security Experimentation Center (SeaSEC): Netherlands, Denmark, Germany, Finland, Norway, and Sweden
  - CSIP (PESCO) Maritime: Belgium, Ireland, Italy, Spain, Sweden-, Germany, Portugal and France
- Actions that focus on coordination.
  - Who has a seat at the table:
  - Various initiatives need to be geared to one another

# Questions?

**Rutger van der Werff, MSc.**
**CDR (OF-4) NLD NAVY**
**NATO NMW COE Concept Development & Experimentation Branch Head**
**nmwcoe-cos@mil.be** (UNCLAS)
**nmw-coe@mil.be** (UNCLAS COE collective mail)
**nmwcoe@joint.mil.be** (NSWAN)

# NMW COE POW - Projects

- **CD&E 031.P: Impact of Side Scan Sonars and Synthetic Aperture Sonars on bottom classification in Naval Mine Warfare**
  Requestor: Self generated
  Evaluate if, how (and in what way) bottom classification needs to be adapted (and used in P&E tools)

- **CD&E 032.P: Artificial Intelligence in Autonomous Systems in support of Mine Countermeasures and Seabed Surveillance**
  Requestor: Italian Navy
  The aim of this project is to analyze the possible application of AI in Autonomous Systems operations

- **CD&E 033.P: Protection of CUI**
  Requestor: Self generated
  Inform Steering Committee and the Community of Interest about the legal, technical and operational challenges and solutions.

# What is a COE?

A Centre of Excellence (COE) is an international military organization that trains and educates leaders and specialists from NATO member and partner countries. They assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation

# NMW COE POW 2025

- Support the NATO Defense Planning Process. Capability Area Group
- Development of REPMUS/DYMS25 Operational Vignettes
- Chair the NMW syndicate of the Underwater Warfare Capability group.
- Author (with ACT SEE) of the Naval Mine Warfare Concept
- Maritime Evaluation (MAREVAL) of NATO's MCM staffs

- Current members: NL, BE, ITA, POL, (DEU). ROU and GRC eager to join in 2025
- Co- located with the BEL Navy Academy (NL- BE NMW school) and BE-NL mission support center.

# Threats to CUI: Threats to pipelines

Unintentionally. Corrosion, hydraulic seal failure, natural forces causing pipeline rupture

Intentionally: using unmanned vehicles, fishing/sailing vessels with scuba divers or ships anchoring intentionally in those areas.

# Threats to CUI: Threats to cables

Most cable damage is unintentional. Potential hazards to the cables range from anchoring and fishing equipment to extreme weather such as earthquakes and landslides.

Intentional: there's an increase in the intentional damaging of cables or acts of espionage (gathering intel).

# Challenges when protecting CUI: Legal

First, international treaties (1884 Cable convention & UNCLOS) often lack mandatory power (use of force) to enforce the legal framework (e.g. intelligence gathering)

Second, how to discipline the offender?

Third, critical underwater infrastructure can be seen as lawful military targets in wartime.

# Challenges when protecting CUI: Technical

First: it requires limited technical expertise and resources to damage them.

Second: depth. Working at larger depths is not our specialty

Third: the absence of an accurate mapping of existing cable infrastructures.

# Challenges when protecting CUI: operational

First: Which vital infrastructure does one specifically wants to protect?

Second: Even with prioritization, the geographic scope of necessary protection (900.000 nm of submarine cables and 20.000 nm of pipelines worldwide)

Third: complete freedom of navigation on the high seas

# Solutions for enhancing CUI protection (1)

Better cooperation between countries/entities.

Focus on coordination.

# Solutions for enhancing CUI protection (2)

Technical solutions. Redundancy, capacity to repair, resilience, network of sensors (intruders & response)

Legal solutions. Cable protection plan give jurisdiction to the cable owner's state.

Operational solutions. Continuous surveillance ,route survey on CUI, show of force, establishing security zones (allowed?)