Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Prof. Dr. Alexander Proelss

Protection of Critical Offshore Infrastructure: International Legal Challenges

International Law and the Protection of Submarine Cables and Pipelines: Multi-Dimensional Perspectives

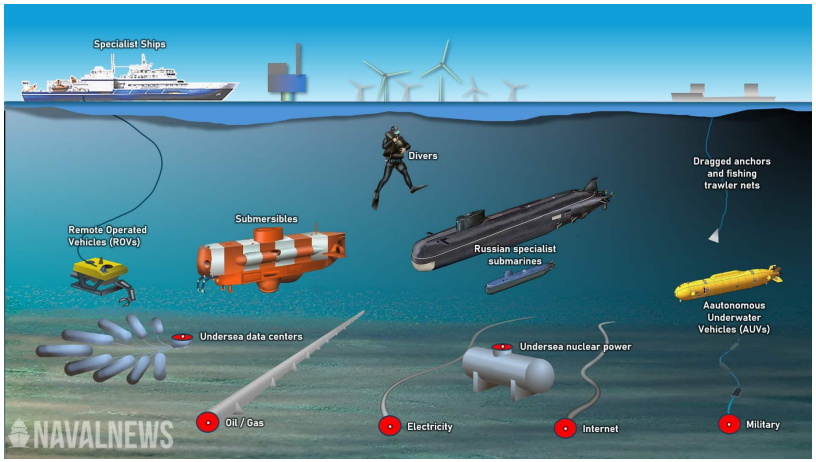
17 September 2025, CIL NUS

© Finnish Border Guard/Reuters

https://www.navalnews.com/naval-news/2024/02/cable-attack-new-undersea-threat-is-starting-to-reshape-naval-wars/

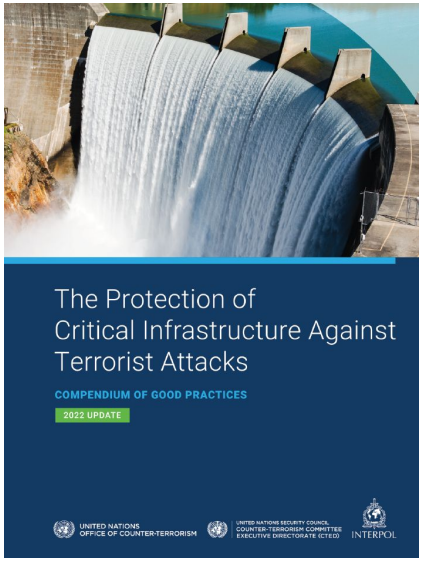
I. Introduction

- Offshore infrastructure = backbone of globalization
- >95% of intercontinental data are transmitted via submarine cables
- Pipelines = essential for energy flows
- Risks: Accidents, sabotage, terrorism, hybrid cyber-physical threats
  - Hybrid activities target different kinds of infrastructure, involve different activities and are conducted by different actors
- International legal protection: fragmented, reactive



II. Concept of Critical Infrastructure (I)

- **No generally accepted international law concept**, no universal definition
  - No international agreements directly and comprehensively governing protection of critical infrastructure
    - But see 2022 Compendium of Good Practices concerning “Protection of Critical Infrastructure Against Terrorist Attacks” published by the UN Office of Counter-Terrorism
  - Fragmented regulation (e.g. law of the sea, international humanitarian law)



II. Concept of Critical Infrastructure (II)

- **EU**: Critical Entities Resilience Directive (EU Directive 2022/2557)
  - Main legislative act aimed at enhancing resilience of critical entities against physical and human-made threats
  - Focus on “essential and important entities” (incl. submarine energy and digital infrastructures)
  - Obliges Member States to adopt:
    - National cybersecurity strategies and designation of competent authorities
    - Risk-management measures and reporting obligations
    - Rules and obligations on cybersecurity information sharing
  - Must be transposed into domestic law by EU Member States by 17 July 2026 (Germany: Draft umbrella law passed by the Cabinet on 10 September 2025)

III. Terrorism Conventions (I)

- Cluster of treaties adopted since the 1960s, negotiated largely under UN auspices
- Each treaty responds to a specific threat/incident (aviation, hostage-taking, bombings, financing)
- Ratio:
  - Criminalize specific conduct, not terrorism in general; avoid jurisdictional gaps; ensure “no safe haven” (aut dedere aut judicare)
- Strong on cooperation, weaker on proactive protection

III. Terrorism Conventions (II)

- Terrorism conventions include:
  - Aviation security conventions (Tokyo 1963, Hague 1970, Montreal 1971 + Protocols)
  - Protection of diplomats (1973)
  - Hostage-Taking Convention (1979)
  - Nuclear material (1980, 2005 amendment)
  - SUA Convention (1988) + 2005 Protocol – maritime focus
  - Convention on the Marking of Plastic Explosives (1991)
  - Terrorist Bombings Convention (1997)
  - Terrorist Financing Convention (1999)
  - Nuclear Terrorism Convention (2005)
- **Only SUA & Bombings Conventions indirectly relevant for offshore infrastructure**

III. Terrorism Conventions (III)

- **1988/2005 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention)**
  - Offences: Violence against ships (Article 3), acts endangering safe navigation
  - Destruction of cables/pipelines covered only indirectly, namely if navigation or platform safety endangered → disruption of communications/energy flows per se = outside SUA scope
  - 1988 Protocol: Fixed offshore platforms added (arguably also applicable to cables and pipelines connected to it)
  - 2005 Protocol: Expands to WMD offences, transport of dangerous materials, ships as weapons → **high relevance**!
  - But no boarding permissible without consent of the flag State!

III. Terrorism Conventions (IV)

Article 3*bis*

1 Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally:

(a) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act:

(i) uses against or on a ship or discharges from a ship any explosive, radioactive material or BCN weapon in a manner that causes or is likely to cause death or serious injury or damage; or

(ii) discharges, from a ship, oil, liquefied natural gas, or other hazardous or noxious substance, which is not covered by subparagraph (a)(i), in such quantity or concentration that causes or
is likely to cause death or serious injury or damage; or

(iii) uses a ship in a manner that causes death or serious injury or damage; or

Article 1

1 For the purposes of this Convention:

(a) "ship" means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft.

(b) "transport" means to initiate, arrange or exercise effective control, including decision-making authority, over the movement of a person or item.

(c) "serious injury or damage" means:

(i) serious bodily injury; or

(ii) extensive destruction of a place of public use, State or government facility, infrastructure facility, or public transportation system, resulting in major economic loss; or

2 For the purposes of this Convention:

(a) the terms "place of public use", "State or government facility", "infrastructure facility", and "public transportation system" have the same meaning as given to those terms in the International Convention

III. Terrorism Conventions (V)

- **1997 International Convention for the Suppression of Terrorist Bombings (Terrorist Bombings Convention)**
  - Obliges States parties to criminalizes unlawful use of explosives in places of public use or against government facilities, public transportation systems and **infrastructure facilities** (= “any publicly or privately owned facility providing or distributing services for the benefit of the public, such as water, sewage, energy, fuel or communications”, Article 1 No. 2)
  - Offshore infrastructure: ambiguous
  - See Article 6:

Article 6

1. Each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 when:

(a) The offence is committed in the territory of that State; or

(b) The offence is committed on board a vessel flying the flag of that State or an aircraft which is registered under the laws of that State at the time the offence is committed; or

(c) The offence is committed by a national of that State.

III. Terrorism Conventions (VI)

- Consequently:
  - Cable landing station = infrastructure facility
  - Submarine cable segments outside of internal waters and territorial sea = only if conducted by own nationals
- **Enforcement Across Conventions:**
  - Aut dedere aut judicare → States must prosecute or extradite
  - Jurisdictional bases: territory, flag, nationality, protective principle, sometimes universal jurisdiction
  - Enforcement = reactive (after acts committed), not preventive
  - No special mandate for coastal States in EEZ and on the high seas to protect infrastructure

IV. Other Developments (I)

- **UN GGE & OEWG**

  - Two UN processes that since the early 2000s have developed non-binding norms of responsible State behavior in cyberspace
    - Submarine cables = physical backbone of ICT networks
  - **UN GGE** = United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
    - Six expert groups since 2004 established by UN GA; reports in 2010, 2013, 2015, 2021 set out agreed norms of responsible State conduct
    - Key points: States should not intentionally damage critical infrastructure using ICTs; they should assist other States under cyberattack; they should protect their own critical infrastructure

IV. Other Developments (II)

- **UN OEWG** = Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security
  - Established by the UN GA in 2018 as a more inclusive process (open to all UN members); concluded its work in mid-2025 with adoption of its final report
  - Its 2021 consensus report reaffirmed the GGE norms and emphasized capacity-building and cooperation
  - Stressed the importance of protecting **critical information infrastructure** against malicious ICT activities
  - Most **controversial issue**: International law
    - Application of existing law (in particular IHL) to cyberspace vs. new binding treaty

IV. Other Developments (III)

- **Global Mechanism to Advance Responsible State Behaviour in Cyberspace**
  - New permanent UN body established in July 2025, building upon 2020 proposal by the EU and its Member States for a UN Cyber Programme of Action
  - All decisions will require unanimous agreement among participating States
  - Focus areas:
    - Exploring the application of existing international law to cyberspace, incl. principles such as State sovereignty and non-intervention
    - Capacity-building
    - Confidence-Building

V. Conclusion

- Current framework: Fragmented, reactive, incident-driven
- Terrorism conventions: Valuable but insufficient for infrastructure protection
- Future directions:
  - Clarify obligations under treaty law
  - Bridge physical and cyber domains
  - Develop cooperative frameworks without undermining freedom of the seas

Thank you very much for your attention!