



Thematic approaches to Protection of Submarine Cables on the High Seas as Cyber Infrastructure

Istanbul, Türkiye
27-28 June 2024

Soojeong Choi

Faculty of Law, Hamburg Universität,

soojeongchoi1209@gmail.com



NATO-MARSEC



Contents

I. Introduction

- Objective
- Background

II. Approach 1: Piracy and Universal Jurisdiction

- Article 101 of UNCLOS and Universal Jurisdiction
- Variation of the Rule of Piracy for Protection of Submarine Cables on the HS

III. Approach 2: Maritime Terrorism and Cyber Terrorism

- Maritime Terrorism and Physical Attack on Submarine Cables on the HS
- Cyber Attack on Cyber Infrastructure on the HS

IV. Approach 3: Self-help by Injured States

- Extension of Legal Term of an Injured State
- Circumstances Precluding Wrongfulness on State Interception

VI. Approach 4: “Consent Regime” for Supplement of Jurisdiction on the HS

- Change of Legal Paradigm on “Freedom of High Seas”
- “Prior-Consent” by a Flag State on the HS : Port State Jurisdiction, PSI, MPA

V. Conclusion





I. Introduction

- Background: Non-exercise of Flag State Jurisdiction in Article 113 of UNCLOS, Trusteeship to “Duty of flag State” in Article 94 on the HS as a Primary Principle??

- Objectives : Elevated Protection Regime for Submarine Communication Cables as Cyber Infrastructure on the HS
 - Extension of Jurisdictions and Injured States
 - Private Ends to Cyber Infrastructure on the HS in Article 101 and 102 of UNCLOS
 - Exception to State Immunity
 - Justification of Self-help
 - Consent-Regime by Flag States for Protection of Cyber Infrastructure as Global Commons





II. Approach 1: Piracy and Universal Jurisdiction

➤ Article 101 of UNCLOS and Universal Jurisdiction

- Exceptional Affordability to a foreign vessels on the HS
- Right of Visit (Art.110)/Seizure of the foreign vessel(Art.105)/Domestic Indictment on the “piracy”

➤ Limitations in “piracy” in Attack on Submarine Cables on the HS

- Less Effective Enforcement of Universal Jurisdiction
- Not obligated for the non-relevant State in “Right of Visit” and “Hot pursuit”
- Concurrent Jurisdiction between a Flag State and an Interdicting State
- No Appetite by the non-relevant State to punish the Attack
- Piracy to “State-sponsored Attack”(=non-private ends?)

➤ Variation of the Rule of Piracy

- Role of UN, UNODC, ITU, and NATO
- Private Ends on “State-sponsored Attack” : Munity exception to State Immunity (Russian Submarine’s Attack on Submarine Cables as munitied as a private vessel in Article 102 of UNCLOS)





III. Approach 2: Maritime Terrorism and Cyber Security

➤ Maritime Terrorism and Damage to SCC on the HS

- 2005 SUA Legal Framework for Maritime Terrorism (Treaty Law, non-Universal Jurisdiction)
- Fixed Platform, Sea-bed area beyond Continental shelf
- Non-applicable to governmental ships

➤ Cyber Attack on Cyber Infrastructure on the HS

- Maritime Cyber Attack and Tallinn Manual 2.0 : SCC as Cyber Infrastructure, out of State Responsibility, Commercial ends in Private Sector(Rule 54), Open to any Cyber attack and any Cyber Espionage
- Cyber Terrorism and Budapest Convention : Cyber Sabotage on the HS in line with article 113 of UNCLOS(Art.22 of BC), the Principle of “*aut dedere aut judicare*”(extradite or prosecute) (Art.24 of BC), Contracting Parties’ alternative approach

➤ Maritime Cyber Terrorism and *lex specialis* for Protection of Cyber Infrastructure





IV. Approach 3: Self-help by an Injured State

➤ Extension of Injured States

- Art.113 of UNCLOS punishment of commission only by flag States, how about cable owner State or registered State, data-loss State, a State with collateral damage of communication networks?
- Failure of “freedom of laying submarine cables on the HS”, International Community as a whole?
- directly injured State and indirectly injured State?

➤ Circumstances Precluding Wrongfulness by Injured State’s Intervention

- Countermeasures as non-forcible means(Art.22 of ARSIWA) : Attribution of a State act, impossible to apply to a non-State actor
- Self-defense as forcible means (Art.51 of UNC, Art.21 of ARSIWA) : inherent right, threshold of an armed attack, imminent and proportionate, low scale of use of force(test of gravity) by a non-state actor with state-sponsorship(Terrorism Exception to State Immunity)/**non state-sponsorship (non-application)**
- State of Necessity with attribution of a State act(Art.25 of ARSIWA) : self-defense(X), but essential interests, non-State actors(non-attribution of a State Act, due diligence of the State, Norway’s approach), interests of international community as a whole(Art.48 of ARSIWA)

➤ Self-help for Protection of Cyber Infrastructure on the HS





V. Approach 4: “Consent Regime” by Flag States

- Change of Legal Paradigm on “Freedom of High Seas”
 - non-exercise of flag State jurisdiction : source of conflict → lawful allocation of jurisdiction by consent regime
- “Prior-Consent” by a Flag State on the HS
 - Port State Jurisdiction in sustainable fisheries on the HS (UNFSA, PSMA), non-reciprocity, community interest
 - PSI and National Security: bilateral agreement with FOC (70% of vessels of FOC)
 - Third State Intervention in marine biodiversity on the HS (MPA of BBNJ)
- “Concession of Flag State” and Community Interests on the HS





VI. Conclusion

- Feasibility : Consent Regime → Consistent Practices of Piracy application to SCC (Function of NATO, UN, UNODC...) → Terrorism with non-private ends (attack on SCC on the HS → categorization of SCC as private property, always attack with private ends), grey area between piracy and terrorism
- However, the enforcement by a confiscating State toward foreign warship or governmental ship in its national court by application of tort law (??)
- Comprehensive roadmap to ill-minded approach to SCC on the map (MCS, amendment of 1884, application strategy of piracy by regional security regime)

