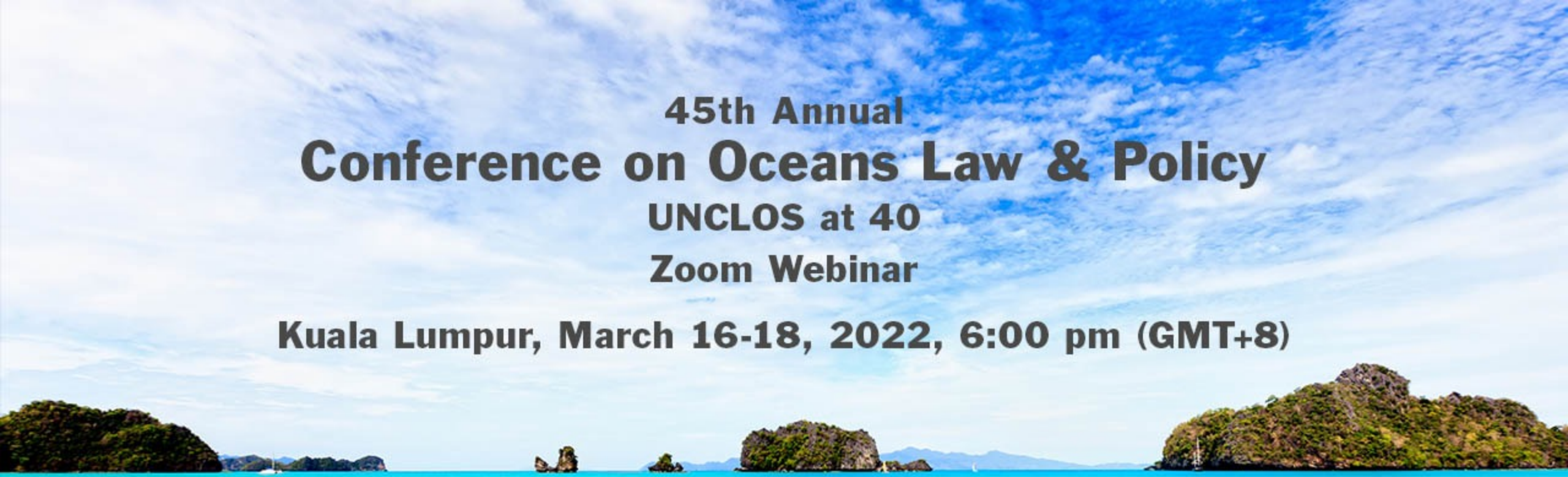


45th Annual
Conference on Oceans Law & Policy
UNCLOS at 40
Zoom Webinar

Kuala Lumpur, March 16-18, 2022, 6:00 pm (GMT+8)

WMU WORLD MARITIME UNIVERSITY

U.S. NAVAL WAR COLLEGE
Stockton Center for International Law

MIMA
MARITIME INSTITUTE OF MALAYSIA
INSTITUT MARITIM MALAYSIA

JIIA 公益財団法人日本国際問題研究所
The Japan Institute of International Affairs

KMI

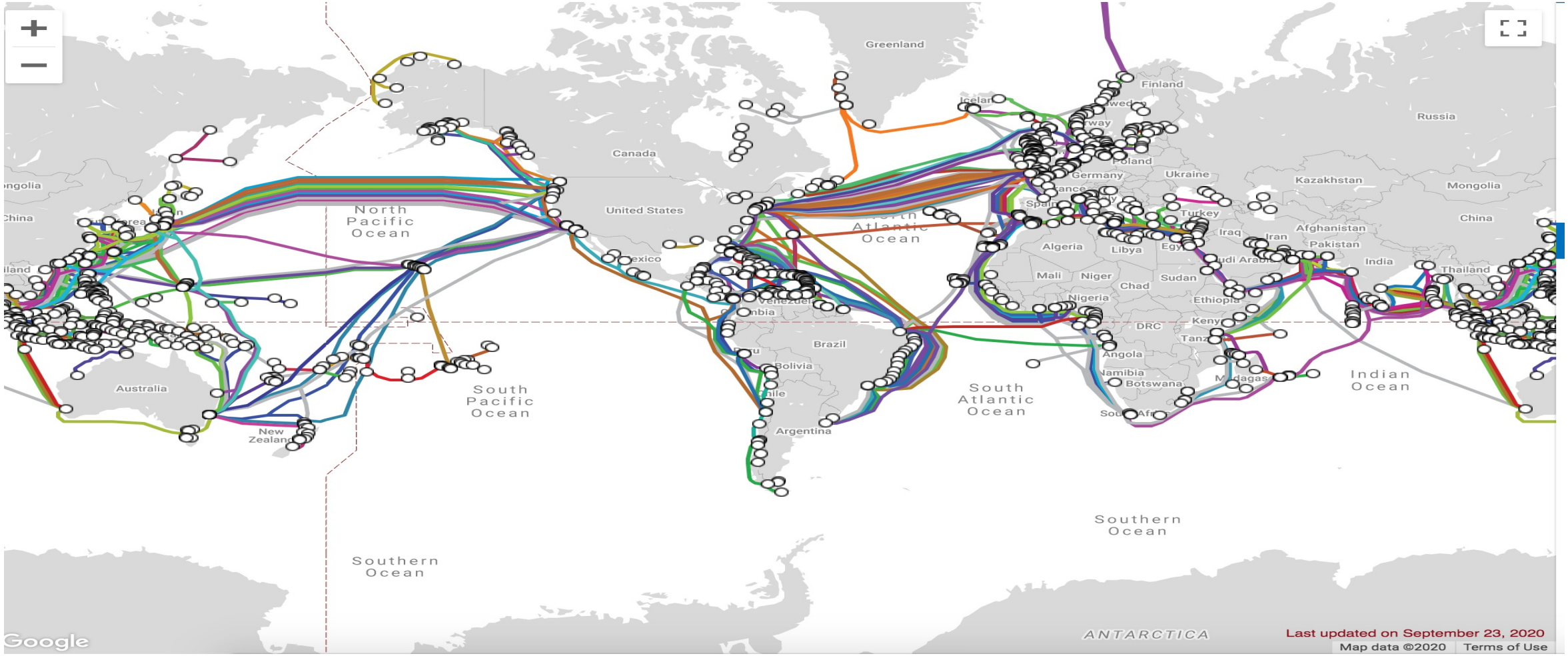
CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

DEHUKAM

INTENTIONAL INTERFERENCE WITH SUBMARINE CABLES: TIME TO UPDATE THE LAW?

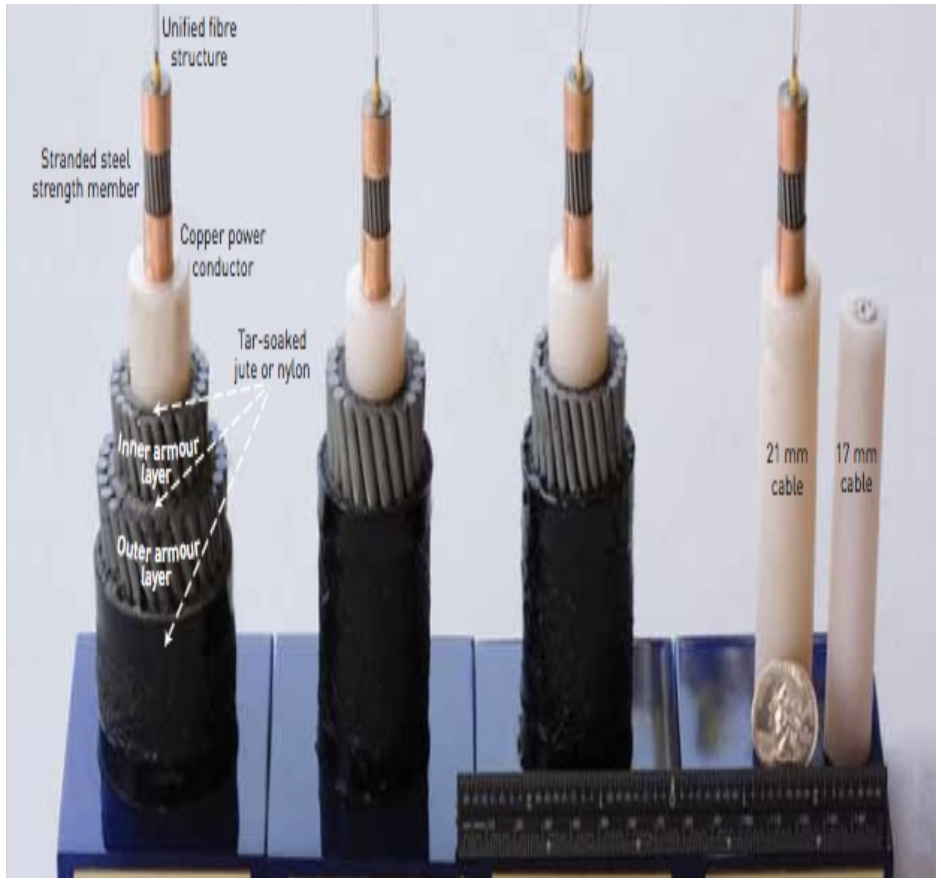
Dr. Tara Davenport
Assistant Professor, Faculty of Law, National University of Singapore (NUS)
Senior Research Fellow, Centre for International Law, NUS

Submarine Cables Network



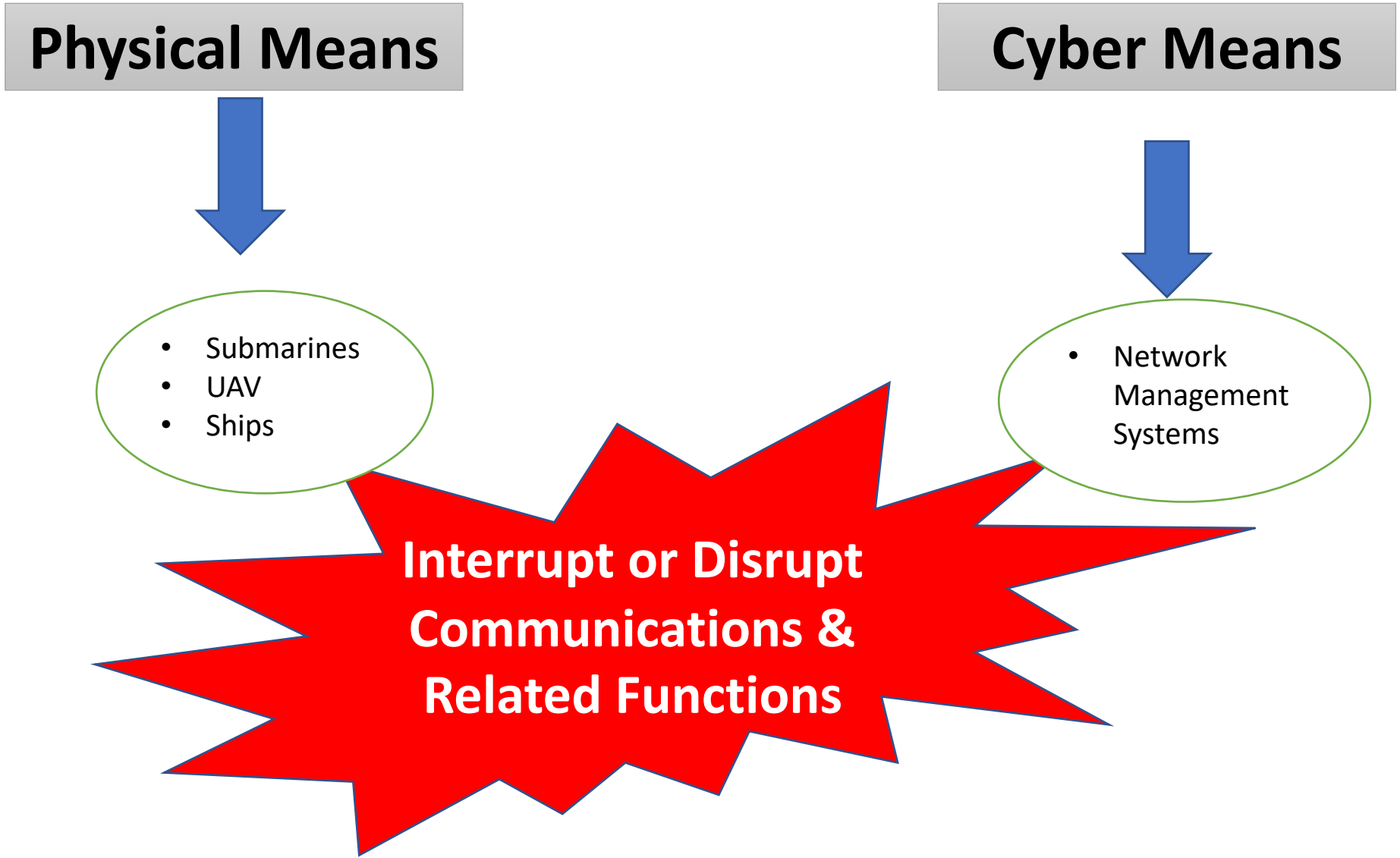
https://www.submarinecablemap.com/

Internet → Banking → Email → Social Media



- Approximately 464 cable systems deployed using approximately 1,245 cable landing stations
- 1.4 million km of fiber-optic cables laid
- Provides 98 % of the world's telecommunications
- Estimates that 59 % of cables are privately-owned; 19 % state-owned and 19 % have both state and private ownership
- 33 % of owned by international consortia of companies whereas 65 % are owned by single owners

Intentional Interference with Submarine Cables by States



Laws Applicable in Peacetime

Laws ...hen Re... ...d Fo... ...s Permis... ...e ...l Bellun...

Laws Applicable in Armed Conflict (Jus in Bello)

Law of the Sea

...oes In... ...onal ...nage by ...s ...marine C... Co... ...tute an A... ... Attac... ...onal

Law of Neutrality

Cyber Operations in Peacetime

International Humanitarian Law

Peacetime: UNCLOS

Article 113:

- **States must adopt laws and regulations to provide that a breaking or injury of a submarine telegraph cable by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done willfully or through culpable negligence is a punishable offence**

Inadequate Implementation

Limited Grounds to Exercise Jurisdiction

Limited Applicability: High Seas /EEZ Physical Means not Cyber Means

Does not mention enforcement or interdiction at sea

Peacetime: Law on Cyber Operations

- The international law on cyber-operations in peacetime is still in its nascent stage
- International law is piecemeal and fragmented and does not comprehensively address the security challenges posed by cyber-operations in general
- Speed and anonymity of cyber operations makes proving State responsibility and distinguishing among the actions of terrorists, criminals and nation states difficult
- In 2015, UN Governmental Group of Experts on ICT established some norms applicable in peacetime
    - Including a recommendation that States should not conduct ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public
- 2017 Tallinn Manual 2.0 – agreement that infliction of damage to cables by a State is prohibited as a matter of customary international law since doing so would run contrary to the purpose of the law governing submarine cables
- Question of whether cyber-operation against submarine cable systems intended to disrupt communications constitutes a cyber-attack (no universally accepted definition of cyber-attack but see 2017 Tallinn Manual 2.0: ‘cyber attack is a cyber-operation, that is reasonably expected to cause injury or death to persons or damage or destruction to objects’)

Law of Armed Conflict

View 1: Submarine Cables are Permissible Military Targets

- State practice demonstrates that submarine cables have always traditionally been legitimate military targets
- 1977 Additional Protocol to the 1949 Geneva Conventions: attacks must be limited to military objectives which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage
- Cable infrastructure is unlikely to be considered a pure civilian object considering that it is a dual-use object used for both military and civilian purposes

Law of Armed Conflict

View 2: The Law of Neutrality – Submarine Cables connecting neutral territory are immune to attack but submarine cables linking belligerent territory are subject to attack

- **Series of early 20th century resolutions and statements from Naval Manuals recognize this distinction between cables connecting neutral territory and cables connecting belligerent territory**
- **1995 San Remo Manual: Belligerents shall take care to avoid damage to cables and pipelines laid on sea-bed which do not exclusively serve the belligerents**
- **2017 Tallinn Manual 2.0: Exercise of Belligerent Rights by Cyber Means Directed Against Neutral Cyber Infrastructure is Prohibited**
    - **Neutral cyber infrastructure means public or private infrastructure that is located within neutral territory which includes civilian cyber infrastructure owned by a party to the conflict of nationals of that party, or that has the nationality of a neutral state and is located outside of belligerent territory**
- **Is the law of neutrality still feasible today?**

Law of Armed Conflict

View 3: Submarine Cables should not be subject to either physical or cyber attacks

- **Oslo Manual on Select Issues on Armed Conflict (Rule 69): Submarine Communications Cables, whether or not connecting occupied territory with neutral territory may not be seized or destroyed even if they are serving one or more belligerent States. Belligerent States must take care to avoid damage to such cables unless they qualify as lawful targets**

- **Even if submarine communications cables qualify as legitimate military targets, they are still subject to the traditional limits in IHL of distinction and proportionality (Paige, Guilfoyle and McLaughlin)**
  - **Requires belligerents to identify which section of cable would have a military objective /confer a military advantage**
  - **Damage to submarine cables and the associated potential impact on loss of civilian life, injury to civilians and damage to civilian objects would mean that such attacks would not be considered proportionate to any purported military advantage**

Conclusions

- The international law governing state's intentional interference with submarine cable systems with the intention of disrupting or halting data traffic is woefully inadequate during both peacetime and in times of armed conflict

- Applicable international law in peacetime and in armed conflict was developed at a time when submarine cables were not as ubiquitous and important as they are today

- But what is the solution?

    - Political and practical challenges in adopting an international convention on the issue either in the context of peacetime or armed conflict?

    - Development of customary international law whereby states refrain from such acts?

    - States and cable companies continue to work together to develop cable resilience?


Thank you! lawtmd@nus.edu.sg