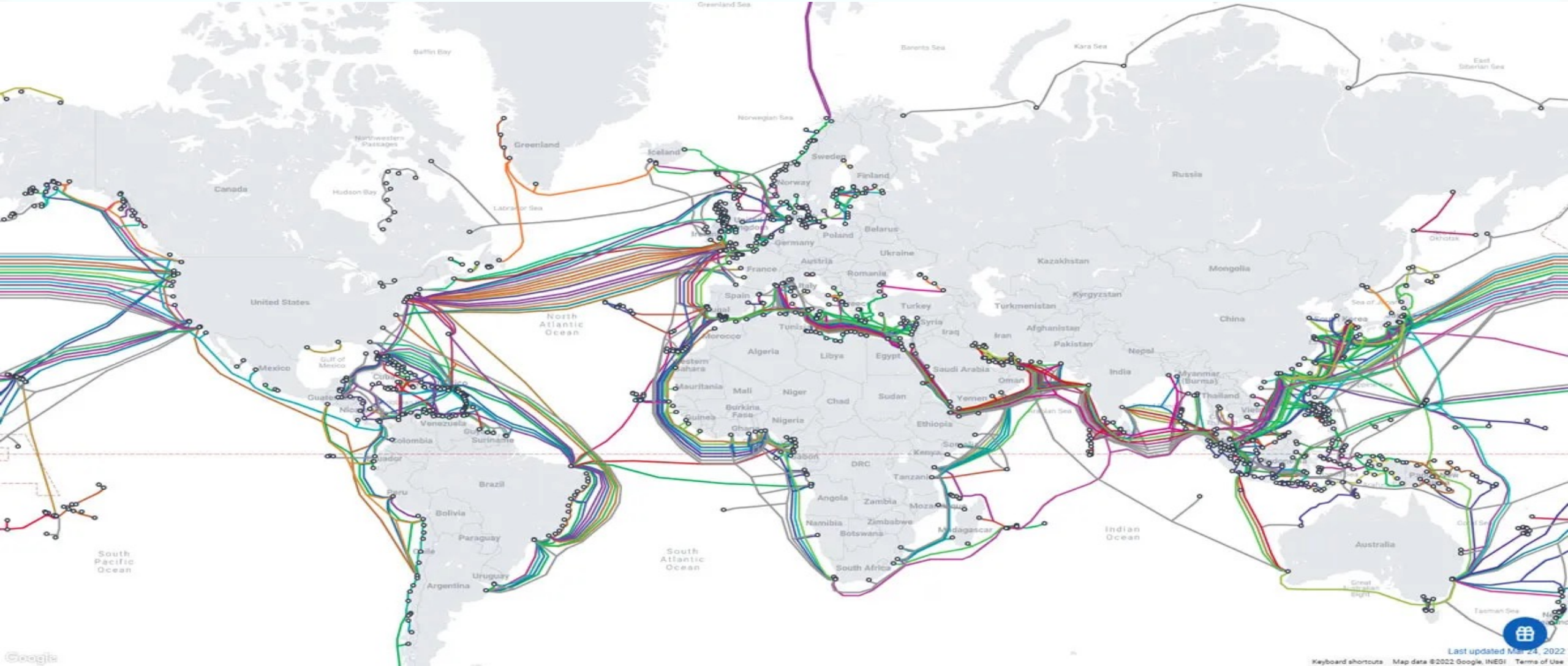
Flowing Data and Competing Powers

Dimensions of submarine cable security

Fabrizio Bozzato, PhD
Senior Research Fellow
OPRI/SPF

2022 Submarine Cable Map

(regularly updated by TeleGeography)



Core Critical Infrastructures

- As of 2022 there are over **1.3 million kilometers of submarine cable** around the world, carrying over 97% of intercontinental internet traffic & with roughly **USD 10 trillion in financial transactions** transmitted via these cables each day.
- The submarine data cable network is **essential** to everyday lives, the functioning of states and the running of global economy.
- Increasing dependence on these "largely invisible" infrastructures leads to increasing awareness that submarine data cable networks are core critical infrastructures of the digital era.
- The recognition that the protection of submarine data cables is a matter of national and regional security has been prompting governmental efforts to increase their protection.

Importance for digital economy and digital sovereignty

- Beyond use for civilian purposes, countries depend on undersea cables for **national security**.
-
- *The coordination of military operations, diplomatic missions and the collection of intelligence depend on the cable network*.

- The loss of communications for a few minutes or hours can have **disastrous repercussions in time-sensitive operations** and can have high financial implications.

- **The implications of any form of cable damage are therefore significant.**

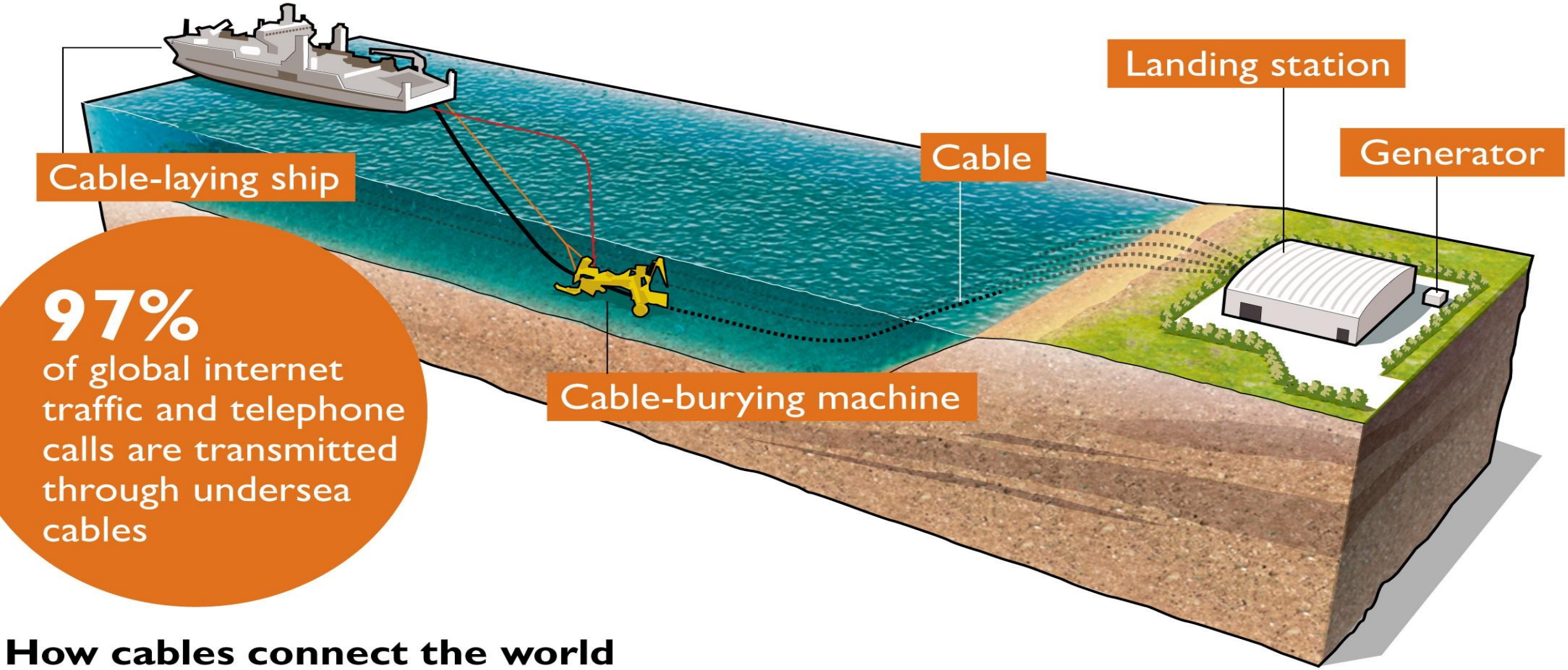
- With the arrival of the 5-6G network, the Internet of Things, artificial intelligence and increasing cloud storage**, the demand for data transfer will only increase**.

- **Everything**, from public services over industrial production to citizens' everyday lives, **will become even more dependent on the smooth functioning of submarine data cables**, elevating the strategic importance of the cable infrastructure,
- *Especially considering the limitations of satellite technology in supplementing big data transfers.*

The paradox of "invisibility" of data cable infrastructure

- Physically, submarine cables lie underground, and they are out at sea, rendering them largely "invisible".
- There is a tendency to pay little attention to what happens at sea more generally - a phenomenon that has been described as **"collective sea blindness"** .
- Like other types of infrastructure, **they often go unnoticed until they fail**.
- **Submarine data cables have only very recently seen increasing political and scholarly attention.**

- In particular, **militaries and national security agencies** have expressed public worries about the vulnerabilities of the cable network.
- While there is a **growing awareness**, there continues to be a **lack of care among policymakers and regulators**, against the backdrop of the complexity of governing submarine cable infrastructures.



97%
of global internet traffic and telephone calls are transmitted through undersea cables

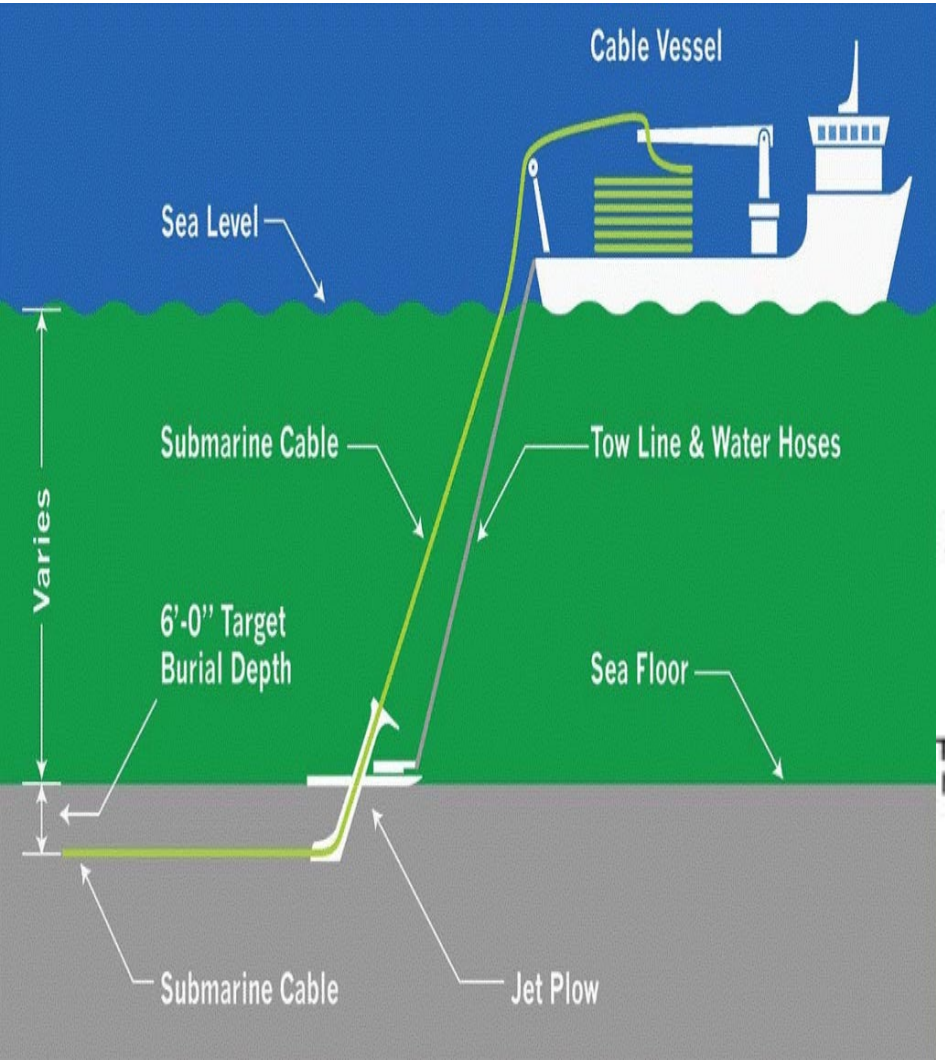
How cables connect the world

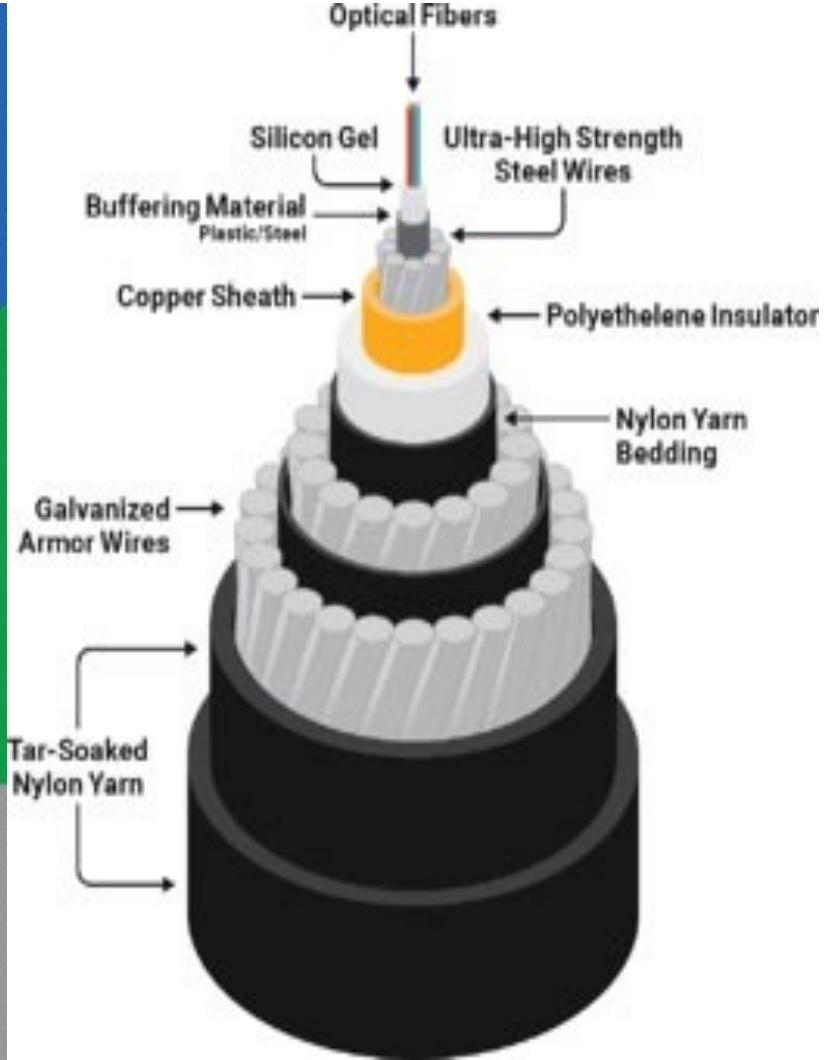
1 The cables, which are the width of a garden hose, are laid by ships using machines that dig trenches on the seabed

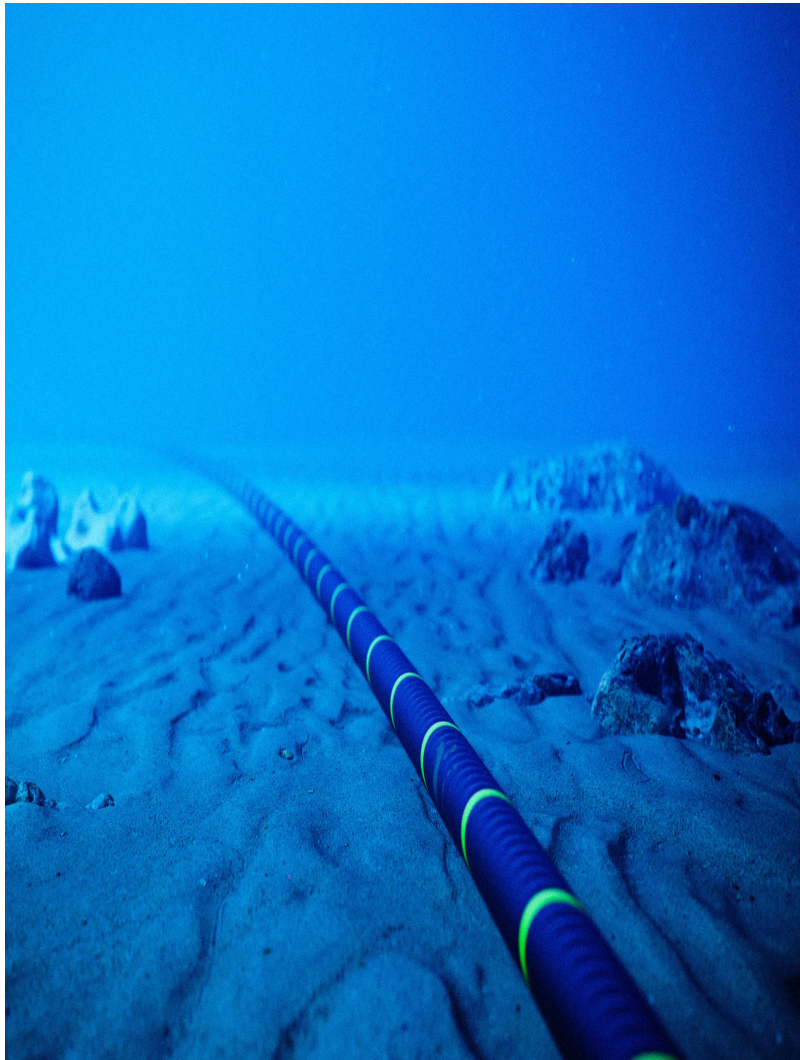
2 They come ashore on beaches, hidden 6ft under the sand

3 Several cables will then emerge together at 'landing stations' nearby. A 10,000-volt current runs through each cable

The infrastructure:
1. Cables (25-year “life expectancy”)





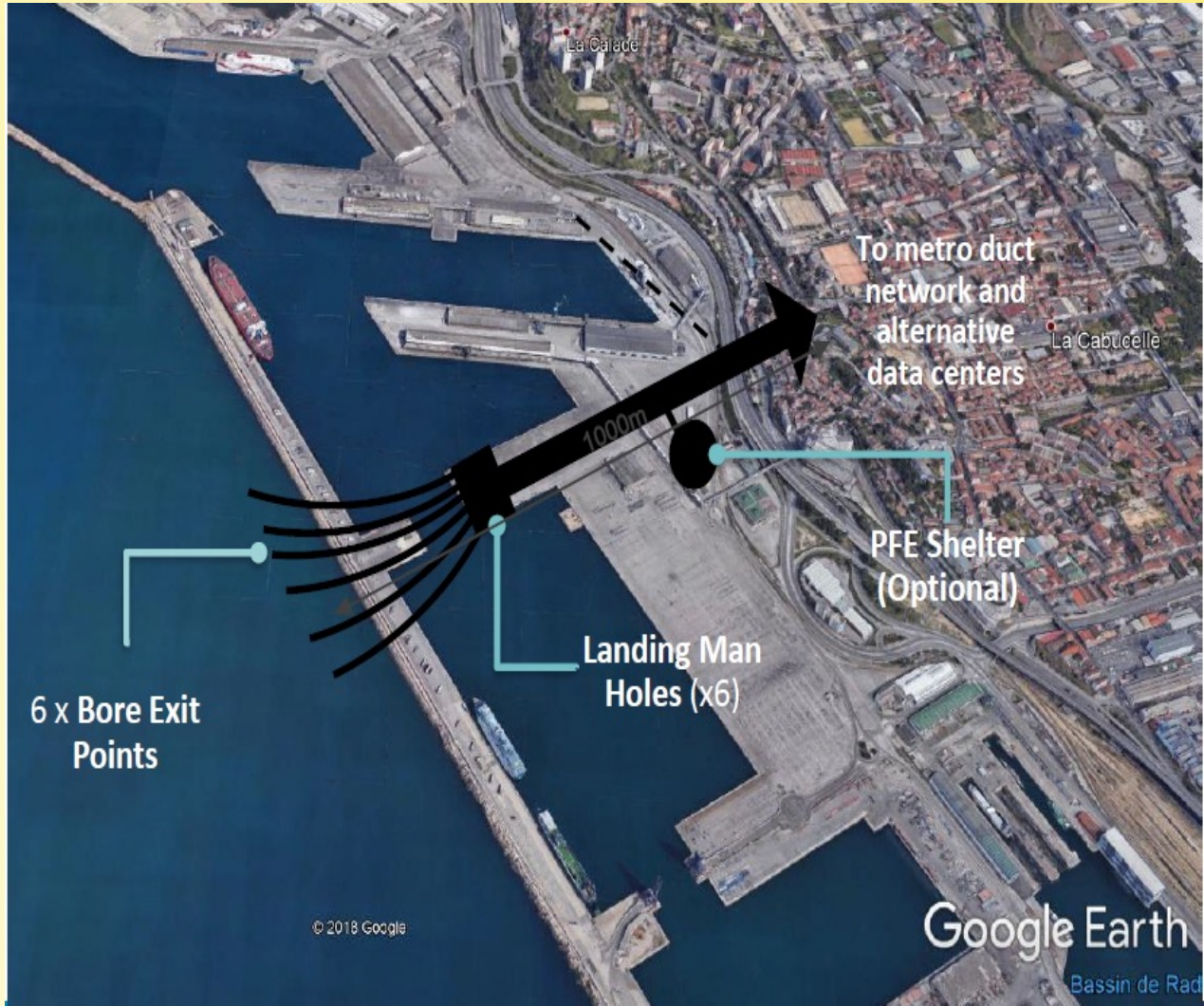


The Infrastructure: 2. Cable landing stations

- The point where all the submarine cables land is called “Cable Landing Point” or “Cable landing Station.”
- The cable landing point powers the cable.
- It hosts the Submarine landing terminal, which is responsible for modulation and transmitting high speed and high-frequency signals all over the submarine cable.

Location matters. A lot.

- The location of cable landing stations is **vital to the resiliency of the cable infrastructure**.
- Ex: If multiple cable landings are constructed in mutual proximity, there is an enhanced risk of failure due to the same disruption event.



CLS securitization is a crucial matter too

Privacy Policy | Feedback

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money

Argos | AO.com | River Island | Groupon | Debenhams | Wayfair | Very | eBay | Boohoo | Nike | Currys

表参道セラ治療院
ビタミンEオイルマッサージ
≪表参道徒歩３分≫ビタミンEを肌から浸透させるオイルマッサージ

ウェブサイト

Revealed: Unlocked hut in a caravan park with no guards is all that protects Britain's £30billion internet link to the US from sabotage

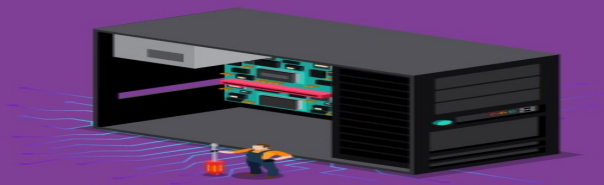
- A shock report has revealed the security threat faced by the fibre-optic cable
- The building home to the £230m Hibernia Express has no security guard
- An Al Qaeda plot to blown up a London internet hub was previously stopped

By MARK HOOKHAM FOR THE MAIL ON SUNDAY and GREG WOODFIELD FOR THE MAIL ON SUNDAY
PUBLISHED: 23:30 GMT, 9 March 2019 | UPDATED: 00:32 GMT, 10 March 2019

Many crucial infrastructure sites such as nuclear power stations and military bases are guarded around the clock by armed police, yet the building that houses the £230 million Hibernia Express at the spot where it comes ashore in Britain doesn't even have a permanent security guard.

Barely 200 yards from a funfair, below, this unremarkable green hut is where vital transatlantic internet cables worth billions to Britain surface from the ocean. But our reporter Mark Hookham was able to stroll up a ramp and walk through an open gate without challenge before peering through an open door

HARDWARE VULNERABILITIES



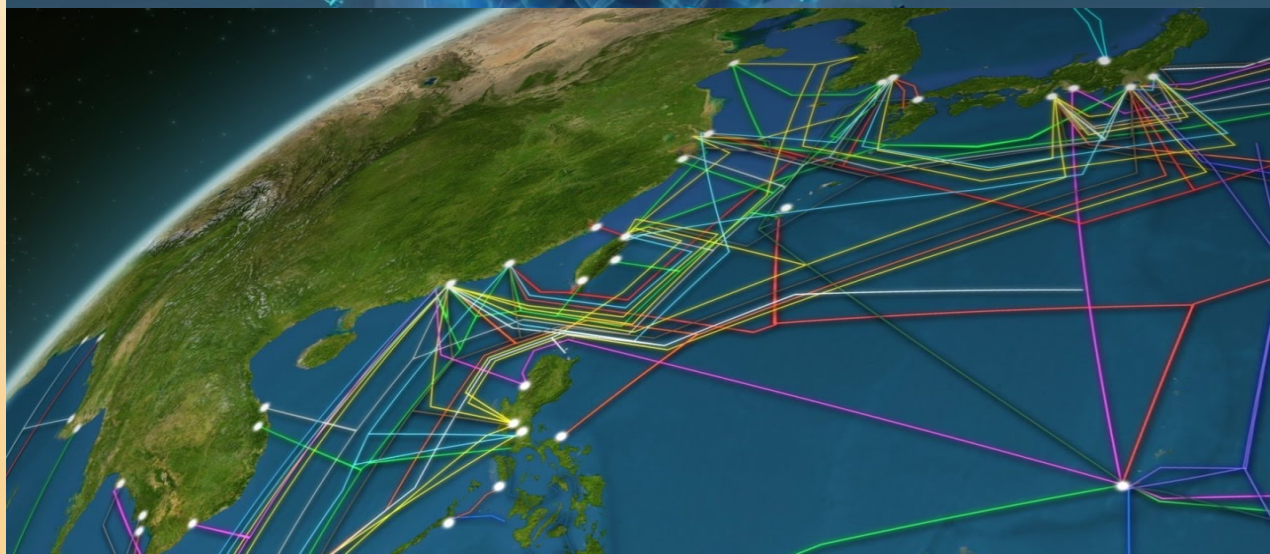
Normally, CLS look like this.

… they should look like this!

Satellite internet networks VS undersea cable networks (?)

- In comparison with satellites, submarine cables provide **high capacity, cost-effective, and reliable connections** that are critical for our daily lives.

- While undersea cables handle hundreds of terabits of data per second and can connect entire continents very low latency (compared to satellite communication).
- … satellite internet systems target individual homes, businesses, and communities in rural, underserved, and remote locations.



Satellites VS Cables: Speed comparison

- **Satellites typically offer only 1,000 megabits per second and have high latency**, which is the time it takes for data to travel between its source and destination.
- Google's new Grace Hopper Cable, on the other hand, has a capacity of **340 terabits per second**.
- This, Google said, is equivalent to about **17.5 million people streaming 4K videos at once**.
- It's no contest, really.

Highly complementary and synergistic
They are not intended to compete

- Satellite internet networks and undersea cables are **"highly complementary"** and not intended to compete against each other.

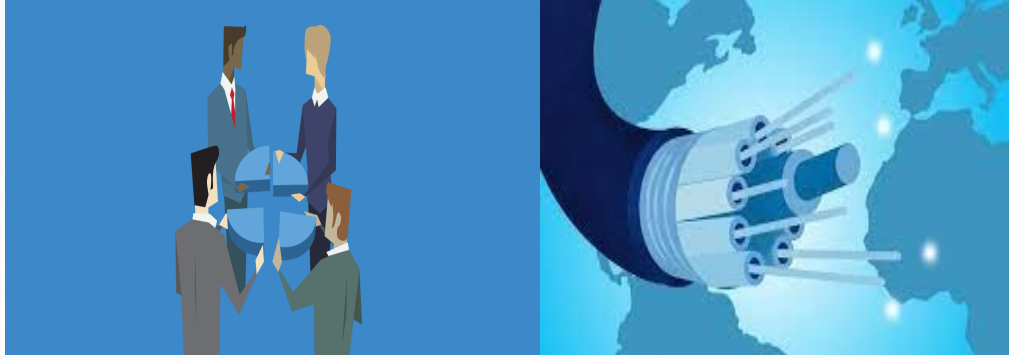
- **"Think of satellite networks as on-ramps to highways with the highways being the submarine networks.** For small islands with no submarine cables, satellite networks are a viable, or sometimes the only, alternative."

[Brian Lavallée, senior director at telecoms equipment supplier Ciena]

- *"Satellite internet access is **not** likely to overtake undersea cable infrastructure in our lifetime, primarily because they're not intended to compete.“*
    - **“Satellite networks are synergistic and pose no threat to undersea cables.”**

[Howard Kidorf, managing partner of undersea telecoms consultancy Pioneer Consulting]

Who does own the cables?



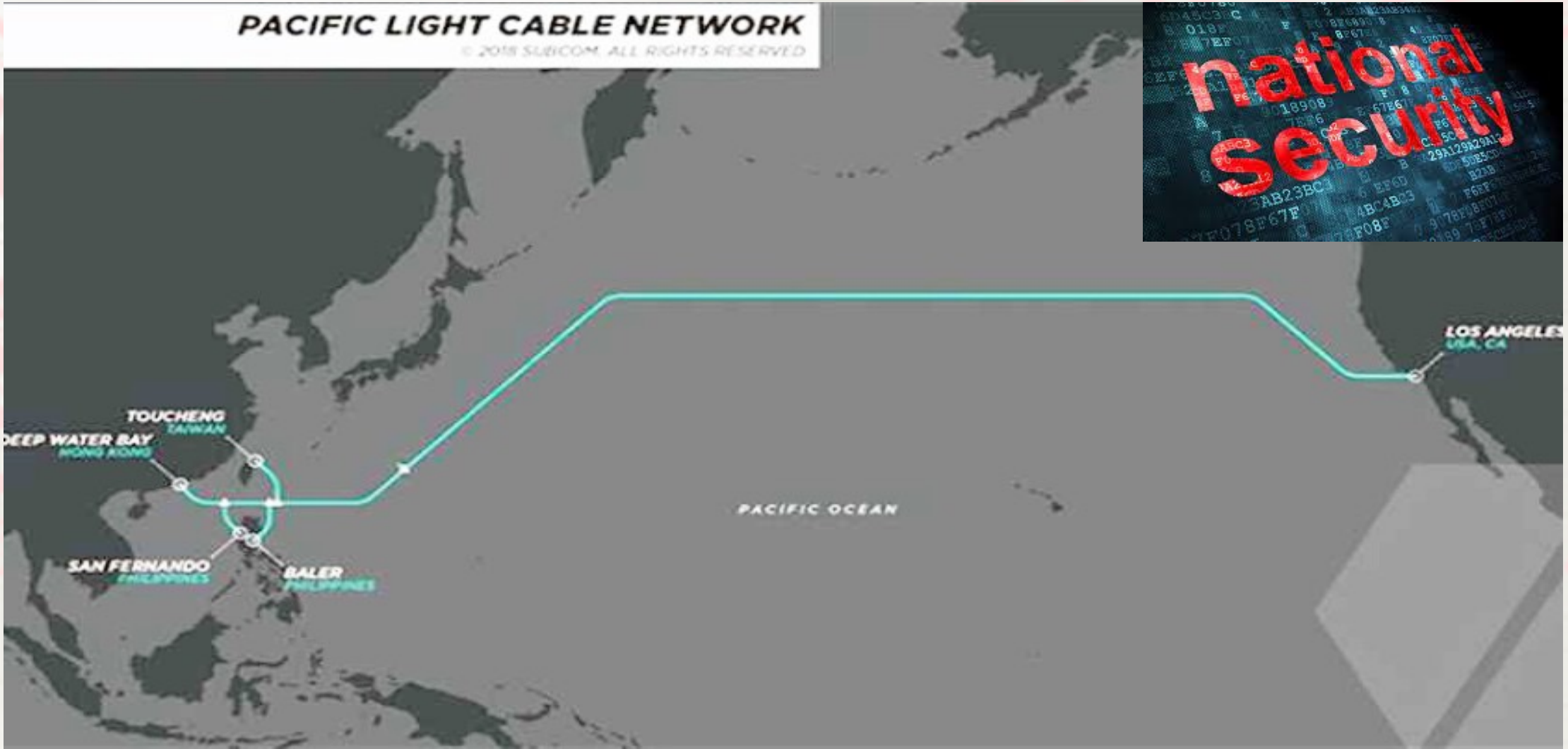
- These cables are **largely owned by private companies**, often in partnership with one another (**consortium model**), though some firms involved in cable network management are state-controlled or intergovernmental.
- The consortium model complicates financial responsibility for repairing the cable when it is damaged; more generally, it removes ownership - with all of its responsibilities and incentives - from the state.
- **Large Internet companies** such as Google, Microsoft, Facebook etc. are now major players in the submarine data cable industry.
- **Google** is the biggest private owner of submarine internet cables.
- **Controlling submarine cables (and their routes) is a major vector of influence** that private or state-owned companies have on the global Internet's shape, behavior, and security.

Besides $ . . . **Geopolitics** influences/determines the development and the routes (shape) of the network

For example … the Pacific Light Cable Network (PLCN)

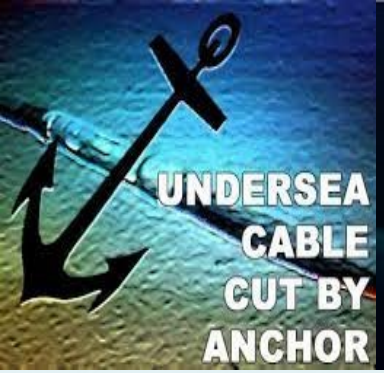
- The PLCN - funded by Facebook and Alphabet, Google's parent company - was originally intended to link the United States, Taiwan, Hong Kong and the Philippines.
- These plans were withdrawn in 2020 following **national security concerns** raised by the Trump administration, but Facebook confirmed it was still working on them.
- A separate proposal with Amazon to connect San Francisco with Hong Kong through undersea cables was also abandoned.
- In March 2021, a further scheme known as the Hong Kong-Americas project was also dropped by Facebook because of "ongoing concerns from the US government about direct communication links between the United States and Hong Kong".
- Facebook said it would "reconfigure" the plans to meet US government concerns. Yet …

PLCN: The Transpacific cable “that could not be”



The “geopolitically correct” Transpacific cables: Echo and Bifrost connecting Singapore and Indonesia to North America (2024)

facebook Google Cloud Telin XL axiata Keppel Corporation



Causes of cable faults

- There are *around 100 cable faults per year*, on average.
- In general terms, the causes of these faults can be divided into three categories:

  1. external (technical issues or economic factors)

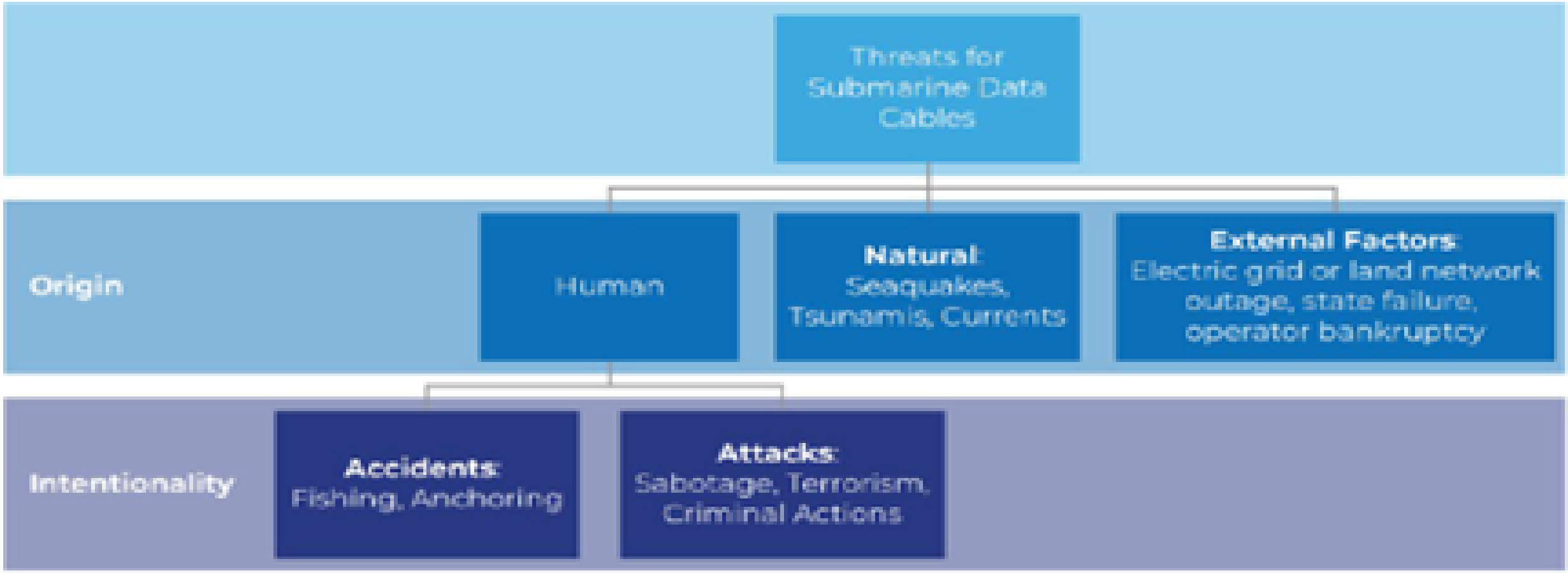
  2. natural (seismic activity, extreme weather events, and black swan events)

  3. human-based (accidental or intentional)

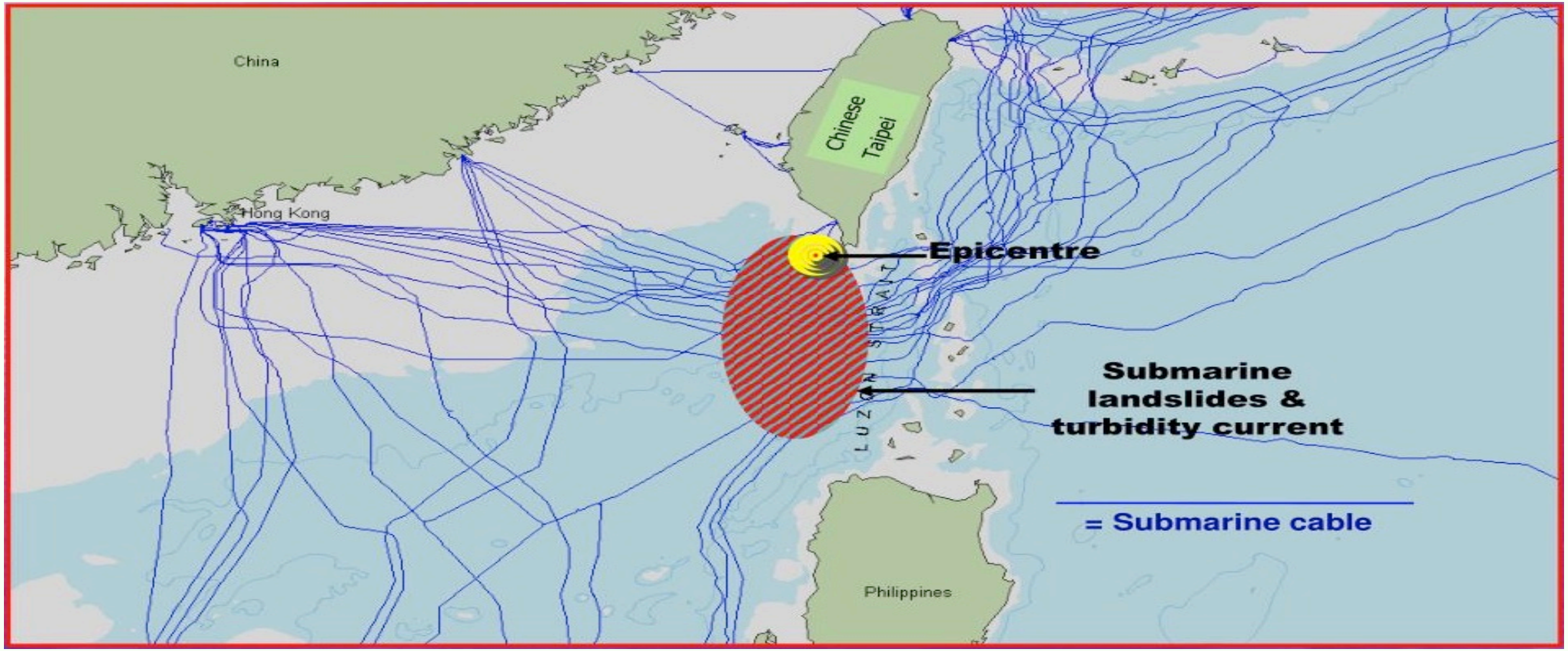
intentional = deliberate attacks

Threats for submarine data cables: natural, human, and external

(image credit: European Parliament)



Natural: Hengchun, 2006: An Earthquake that Caused Major disruption to the Cable Network



Accident or Sabotage?
Sequentially 6 cables were snapped in 12 days

"We do not want to preempt the results of ongoing investigations, <u>but we do not rule out that a deliberate act of sabotage</u> caused the damage to the undersea cables over two weeks ago."
Sami Al Basheer Al Morshid, Director BDT, ITU (AFP: February 18, 2008)

Threat analysis

with a focus on deliberate attacks

- **Modes of attack:**

1. **Physical destruction**
2. **Data theft and intelligence**
3. **Digital means**

Ways to cut cables

A Remotely operated vehicles

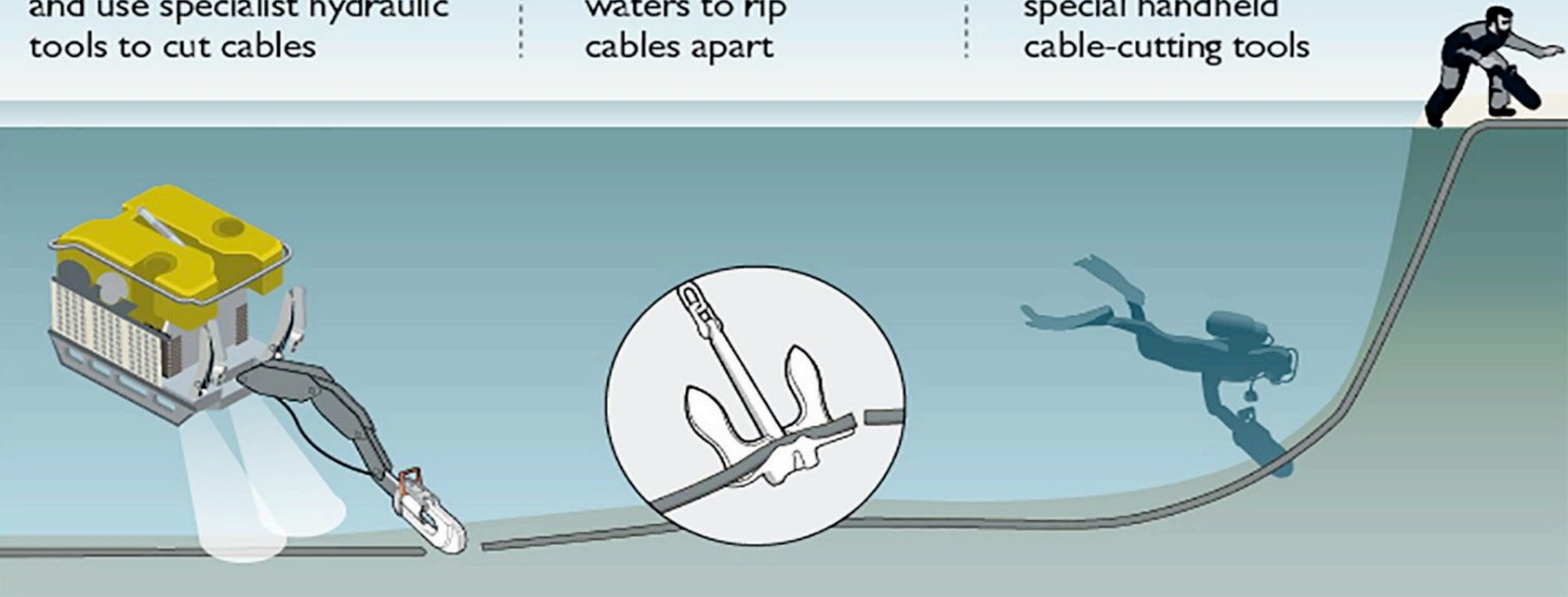
ROVs can descend to depths of up to 6,000m and use specialist hydraulic tools to cut cables

B Anchors

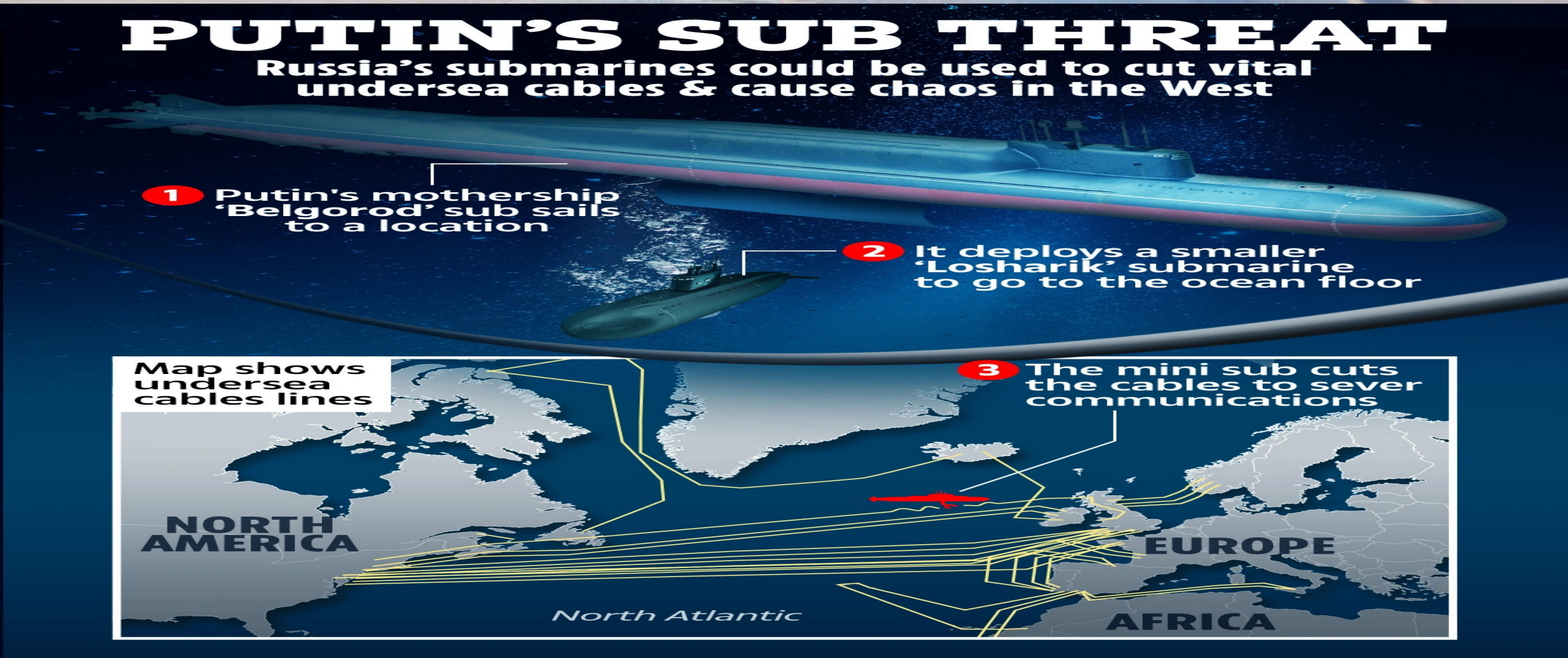
Anchors can be dragged in shallow waters to rip cables apart

C Divers and on land

Personnel can be dispatched with special handheld cable-cutting tools



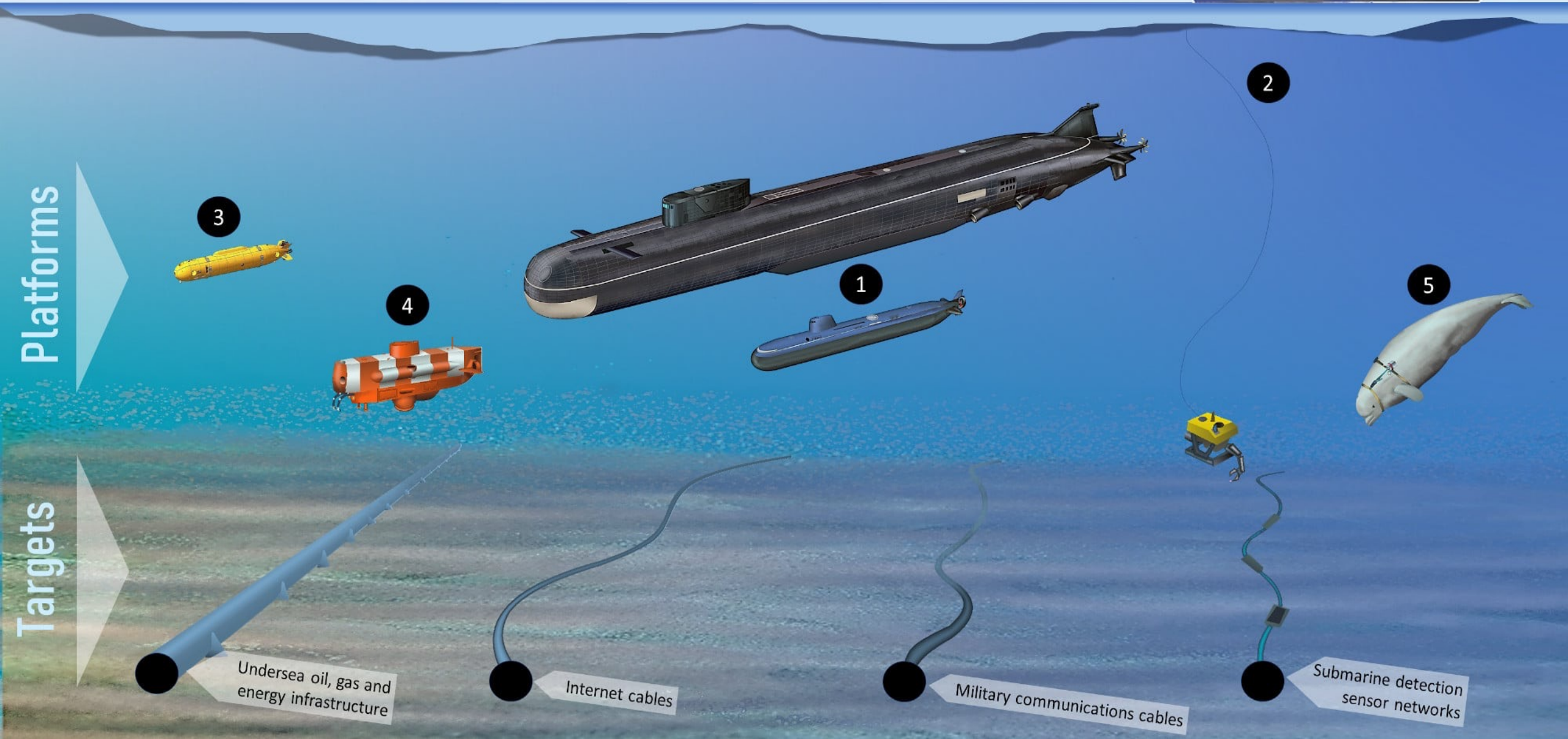
State-sponsored threats



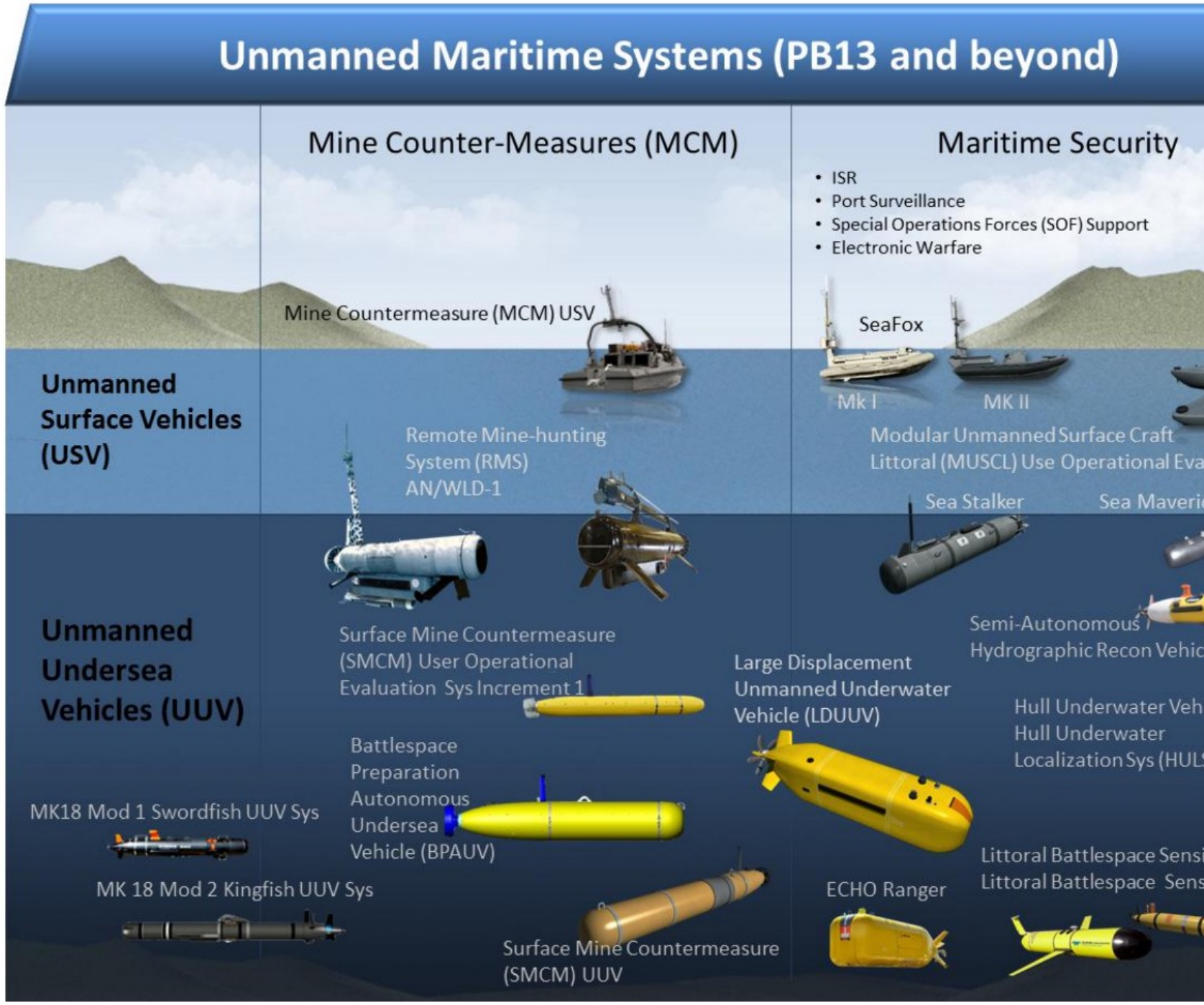
NAVALNEWS

COVERTSHORES
www.hisutton.com

Russian Seabed Warfare Capabilities



A new paradigm of underwater warfare in the 21st Century



Threats emanating from non-state actors

1. Violent extremism and maritime terrorism

2. Criminal organisations

Espionage: Tapping into submarine data cables

- More difficult and subtle than destroying the cables is tapping them to record, copy, and steal data, which would be later collected and analyzed for espionage.
- It is believed this could be done in one of three ways:

1. inserting backdoors during the cable manufacturing process
2. targeting onshore landing stations and facilities linking cables to networks on land
3. tapping the cables at sea

- *the last—tapping the cables at sea— is believed to be so technically challenging that there are only a few countries allegedly capable of it.*

Cyber or network attacks @ submarine cables

- The final type of threat is **cyber or network attacks**.
- By **hacking into the network management systems** that private companies use to manage data traffic passing through the cables, malicious actors could disrupt data flows.

- **A "nightmare scenario"** would involve a hacker gaining control, or administrative rights, of a network management system. At that point, they could discover physical vulnerabilities, disrupt or divert data traffic, or even execute a "kill click" deleting the wavelengths used to transmit data.

Thank you for your time and attention

みなさんありがとうございます！