EU Cable Security Action Plan: Updates from the Member State Expert Group

EU Action Plan on Cable Security

PREVENT

- Apply existing Security Requirements (**NIS2/CER**)
- **Map** cable infrastructures
- Coordinated **risk assessment** with MS
- **Cable Security Toolbox** with mitigating measures
- Preparedness: **Stress test** security & resilience ➔ DEP
- Investment Framework: focus investment on **Cable Projects of European Interest** (CEF – €540m)
- New technologies: smart cables & industrial roadmap

DETECT

- Integrated **Surveillance Mechanism** per sea basin (voluntary, fuse data, civ/mil approach, real-time situational picture)
- Dedicated regional **Nordic/Baltic Hub**
- Network of **undersea sensors**
- **Drone** surveillance programme (air, surface, underwater)
- Partnership with **cable operators** for increased detection

RESPOND & RECOVER

- Enhance effectiveness of EU crisis response framework (tailor-made approach to cables)
- Enhanced cooperation with NATO
- Increase EU cable vessel capacities (repair vessels & modular equipment)
- Establish Multipurpose Cable **Vessels Reserve** (e.g., RescEU)
- Ensure security of supply of spare parts through target stockpiles

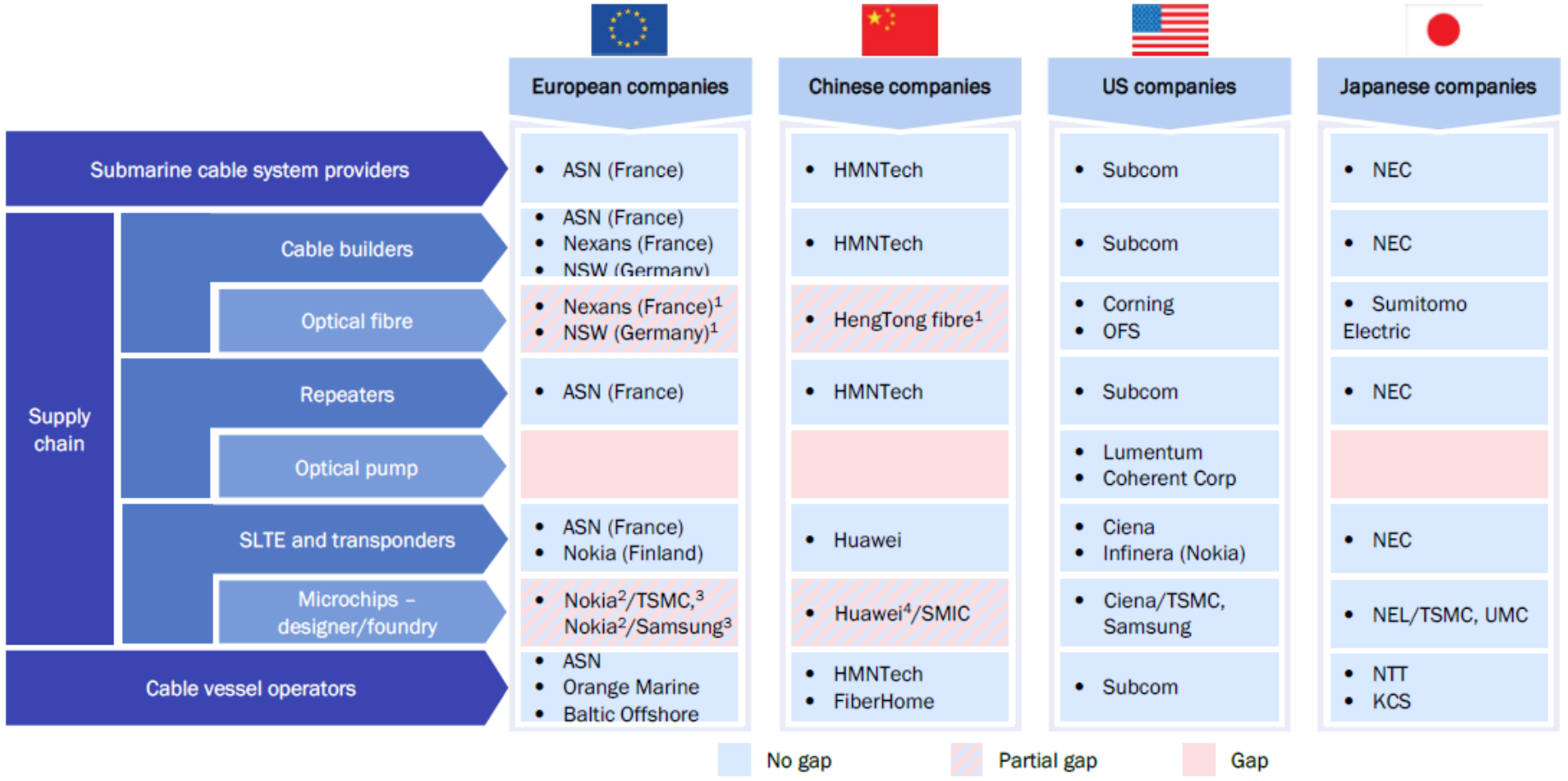
DETER

- Deploy proactive cable diplomacy
- Act against **Shadow Fleet** (common listing, Flag States, sanctions)
- Hold malicious actors accountable (sanctions)
- Step up strategic communication
- Make full use of International Law of the Sea

Priorities for Expert Group

Expert Group report (1/7): Key EU players & supplier dependencies

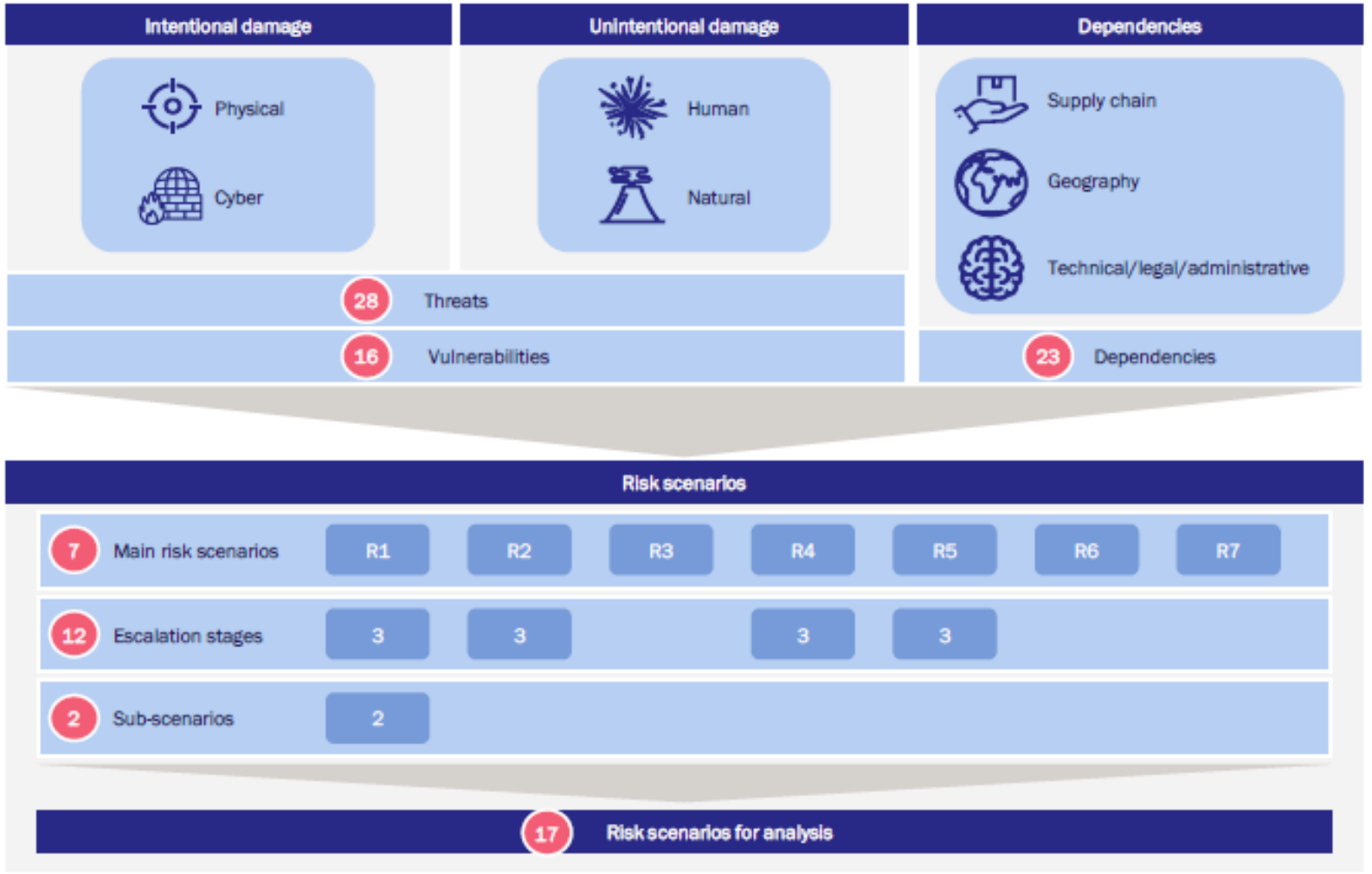
Figure 2.1: Key players and EU supplier dependencies in the submarine cable ecosystem (7) [Source: Analysys Mason/Axiom, 2024]



(7) (1) Only for small unrepeated submarine cable systems; (2) Lack of state-of-the-art European foundry, although TSMC is building a new plant in Germany to mitigate Chinese take-over threat; (3) TSMC (Taiwan, under US influence) and Samsung (South Korea); (4) The US is preventing TSMC from providing microchips to Huawei, hence Huawei uses SMIC, which has volume-production issues.

Expert Group report (2/7): Risk assessment methodology

Figure 4.1: Risk assessment methodology [Source: Analysys Mason, 2025]



Expert Group report (3/7): Intentional cable damage (threats & vulnerabilities)

*Figure 4.2: Consolidated view of threats and vulnerabilities related to **intentional** submarine cable damage [Source: Analysys Mason, 2025]*

	Intentional damage	
	Physical	Cyber
Threats	• **T1.** Cable cuts in territorial waters • **T2.** Cable cuts in Exclusive Economic Zones (EEZs) • **T3.** Cable cuts in high seas • **T4.** Cable cuts in backhaul • **T5.** Damage/destruction of beach manhole • **T6.** Physical security breach at cable landing stations • **T7.** Damage/destruction of cable landing stations • **T8.** Power outage due to damage to grid/transformer • **T9.** Blockage of access to depot • **T10.** Damage to/destruction of depot • **T11.** Blockage of access to vessels • **T12.** Damage to/destruction of maintenance vessels • **T13.** Physical attack on the supply chain causing disruption	• **T14.** Network intrusion/intrusion into the operating system • **T15.** Insider threat • **T16.** Cybersecurity attack on a Managed (Security) Service Provider (M(S)SP) or other third-party service provider • **T17.** Cybersecurity attack on the supply chain causing disruption
Vulnerabilities	• **V1.** Insufficient physical security at beach manhole • **V2.** Insufficient physical security at cable landing station/Network Operation Centre (NOC) • **V3.** Insufficient physical security at depots • **V4.** Lack of depot backup location • **V5.** Exact position of cable, depots and cable landing station available in the public domain (eases targeting infrastructure by a third party) • **V6.** Lack of backup power supply at cable landing station	• **V7.** Insufficient cybersecurity in network management • **V8.** Insufficient cybersecurity of network equipment • **V9.** Insufficient cybersecurity of end-user devices

Expert Group report (4/7): Unintentional cable damage (threats & vulnerabilities)

*Figure 4.3: Consolidated view of threats and vulnerabilities related to **unintentional** submarine cable damage [Source: Analysys Mason, 2025]*

	Unintentional damage	
	Human	Natural
Threats	• **T18.** Fishing (cable cut) • **T19.** Anchors (cable cut) • **T20.** Civil works and dredging (cable cut) • **T21.** Deep sea mining (cable cut) • **T22.** Misconfiguration of network	• **T23.** Undersea seismic activity • **T24.** Undersea volcanos • **T25.** Slumping • **T26.** Beach erosion • **T27.** Bottom current • **T28.** Adverse weather events
Vulnerabilities	• **V10.** Lack of education on submarine cables for the fishing industry • **V11.** Lack of protection area around the submarine cable route in territorial waters	• **V12.** Cables located in geographically unstable areas
	• **V13.** Unreliable network equipment • **V14.** Exposed cable at fishing/anchoring depth • **V15.** Lack of cable armouring at fishing/anchoring depth • **V16.** Lack of surveillance/advanced monitoring systems	

Expert Group report (5/7): Dependencies

*Figure 4.4: Consolidated view of **dependencies** [Source: Analysys Mason, 2025]*

Dependencies		
Supply chain	**Geography**	**Technical/ legal/administrative**
• **D1.** Supplier dependency (in particular non-EU) • **D2.** Lack of components due to nation state influence/control of supplier • **D3.** Lack of components in the market due to high demand or insufficient supply • **D4.** Lack of standardisation in submarine system components • **D5.** Shifting market demand from telecoms towards hyperscaler (data centres/AI) business model • **D6.** Lack of maintenance capability in the EU • **D7.** Lack of EU shipyard capacity for building new vessels • **D8.** Dependency of power supply	• **D9.** US dependency • **D10.** UK dependency • **D11.** Chinese dependency • **D12.** Russian dependency • **D13.** Cables located in geopolitically unstable areas • **D14.** Lack of route diversity • **D15.** Chokepoints	• **D16.** Dependency on technical expertise • **D17.** Long process to obtain repair permit • **D18.** Lack of jurisdiction for incidents in EEZs and high seas • **D19.** Lack of plan to respond to emergency situations • **D20.** Lack of centralised reporting of physical and/or cyber incidents • **D21.** Lack of co-ordination entity in each Member State or between countries to respond to a submarine cable incident or emergency situation • **D22.** Lack of information sharing between public entities from different Member States • **D23.** Lack of public–private co-ordination

Expert Group report (6/7): Risk scenarios

Escal. stage	Sub-scenario
R1. Co-ordinated physical sabotage or attack on submarine cable (R6 in the Nevers Report)	
Escal.1: base	**R1.1.** Cable cut in territorial waters/EEZ of an EU Member State affecting at least two EU Member States
Escal.2	**R1.2.** Cable cut in territorial waters/EEZ of a third country affecting at least two EU Member States
Escal.3	**R1.3.** Cable cut in high seas affecting at least three EU Member States
N/A	**R1.4.** Cutting off an entire island
N/A	**R1.5.** Cutting off an entire region
R2. Co-ordinated sabotage or attack on cable landing site (beach manhole and/or landing station) (adapted from R6 in the Nevers Report)	
Escal.1: base	**R2.1.** Cyber intrusion into a cable landing station where cables land, affecting at least two EU Member States
Escal.2	**R2.2.** Sabotage of beach manholes where cables land, affecting at least two EU Member States
Escal.3	**R2.3.** Physical intrusion into a cable landing station where cables land, affecting at least two EU Member States, and destruction of equipment (including potentially the entire cable landing station)
R3. Power cuts to cause a regional network outage (adapted from R9 in the Nevers Report)	
R4. Disruption of maintenance capability	
Escal.1: base	**R4.1.** Market dynamics resulting in a temporary shortage of maintenance vessels in EU waters
Escal.2	**R4.2.** Sabotage of a maintenance vessel serving EU waters or of a spares depot
Escal.3	**R4.3.** Co-ordinated sabotage of several maintenance vessels serving the EU or of several spares depots
R5. Disruption of the supply chain	
Escal.1: base	**R5.1.** Market dynamics resulting in a temporary supply shortage of key components
Escal.2	**R5.2.** Third-country interference on a supplier of key components (including cyber espionage) (adapted from R2-4 in the Nevers Report)
Escal.3	**R5.3.** Block of supply (for example, embargo) or backdoor access to a system, enabling a malicious system shutdown
R6. Unintentional cable damage caused by human activity	
R7. Natural events leading to physical damage on multiple cables or cable landing stations	

Expert Group report (7/7): Stress test stages

*Figure 5.23: Stress test stages [Source: Analysys Mason, 2025]**

Stage	Risk scenario/sub-scenario
Stage 1	R1.1. Cable cut in territorial waters/EEZ of an EU Member State affecting at least two EU Member States
	R2.1. Cyber intrusion into a cable landing station where cables land, affecting at least two EU Member States
	R4.1. Market dynamics resulting in a temporary shortage of maintenance vessels in EU waters
	R5.1. Market dynamics resulting in a temporary supply shortage of key components
Stage 2	R1.2. Cable cut in territorial waters/EEZ of a third country affecting at least two EU Member States
	R2.2. Sabotage of beach manholes where cables land, affecting at least two EU Member States
	R4.2. Sabotage of a maintenance vessel serving EU waters or of a spares depot
	R5.2. Third-country interference on a supplier of key components (including cyber espionage) (adapted from R2-4 in the Nevers Report)
Stage 3	R1.3. Cable cut in high seas affecting at least three EU Member States
	R2.3. Physical intrusion into a cable landing station where cables land, affecting at least two EU Member States, and destruction of equipment (including potentially the entire cable landing station)
	R3. Power cuts to cause a regional network outage (R9 in the Nevers Report)
	R4.3. Co-ordinated sabotage of several maintenance vessels serving the EU or of several spares depots
	R5.3. Block of supply (for example, embargo) or backdoor access to a system, enabling a malicious system shutdown
Optional	R1.4. Cutting off an entire island
	R1.5. Cutting off an entire region
	R6. Unintentional cable damage caused by human activity
	R7. Natural events leading to physical damage on multiple cables or cable landing stations

*updated on 3 November 2025 to correct minor mistakes

Next steps & timeline

21 February 2025:
EU Cable Security Action Plan

12 March 2025:
3rd Expert Group meeting

24 June 2025:
News item on status of EG work

7 November 2025:
- 5th Expert Group meeting
- Tentative agreement on Toolbox and CPEI list

18 June 2025:
4th Expert Group meeting

23 October 2025:
- EG deliverables 1&2: *Report on Mapping, Risk Assessments, Stress Tests*
- DEP Calls on stress tests & Cable Hubs

January 2026:
EG deliverables 3&4: *Cable Security Toolbox & CPEI list*

Drafting of report, validation, gap analysis

NB: Public information on Commission register

Thank you for listening!

CNECT E.1 Submarine Cable Infrastructure team:

Miguel.GONZALEZ-SANCHO-BODERO@ec.europa.eu

Agustin.DIAZ-PINES@ec.europa.eu

Johannes.THEISS@ec.europa.eu

Achilleas.KEMOS@ec.europa.eu

Enrique.Gomez@ec.Europa.eu

European Commission