

Cabluri tăiate: Infrastructura submarină de internet în zone de tensiune geopolitică

Claudiu Codreanu





Cabluri tăiate: Infrastructura submarină de internet în zone de tensiune geopolitică*¹

Claudiu Codreanu²

Analist

Institutul Diplomatic Român

ABSTRACT: Evenimentele recente din Marea Baltică și Strâmtoarea Taiwan evidențiază vulnerabilitatea infrastructurii critice – precum cablurile submarine, conductele sau rețelele energetice – în fața deteriorărilor, fie ele intenționate sau accidentale. Cablurile submarine de internet reprezintă sistemul nervos invizibil al lumii noastre digitalizate. Deși tăierea unuia sau a două cabluri nu duce, de regulă, la întreruperea completă a conexiunilor într-o întreagă regiune sau țară, avarierea unor cabluri strategice poate încetini semnificativ traficul de date sau provoca întreruperi locale de internet. Totodată, disponibilitatea unui actor statal de a sabota astfel de cabluri transmite un semnal de alarmă și ridică riscuri majore pentru rețelele globale de telecomunicații. Acțiunile atribuite Rusiei și Chinei în ultimii doi ani arată că sabotajul fizic nu trebuie neglijat în eforturile de protejare a infrastructurii digitale și a securității cibernetice. Acest studiu analizează incidentele recente din Marea Baltică și Strâmtoarea Taiwan, rolul jucat de Rusia și China ca posibili actori în astfel de acțiuni de sabotaj, precum și reacțiile statelor afectate și ale organizațiilor internaționale precum NATO și Uniunea Europeană. În final, sunt prezentate o serie de recomandări privind consolidarea rezilienței infrastructurii submarine.

CUVINTE CHEIE: cabluri submarine, infrastructură digitală, Marea Baltică, Taiwan, Rusia, China.

*Acest material reprezintă traducerea în limba română a textului original publicat în engleză în iunie 2025.

¹ Această publicație se bazează exclusiv pe surse deschise. Opiniile exprimate aparțin în întregime autorului și nu reflectă neapărat poziția instituției.

² claudiu.codreanu@idr.ro

INTRODUCERE

După invazia pe scară largă a Ucrainei de către Rusia în 2022, s-a înregistrat o creștere semnificativă a incidentelor care au afectat cablurile și conductele submarine (Webster 2025). Încă din acel an, nave comerciale și militare rusești navigau în apropierea sau chiar prin Zona Economică Exclusivă (ZEE) a Irlandei, iar în noiembrie 2024, o navă de cercetare rusească a fost escortată de marina irlandeză după ce a fost surprinsă patrulând într-o zonă unde se află mai multe cabluri submarine și conducte care leagă Irlanda de Regatul Unit (Besch & Brown 2024, 7).

Data	Zona	Infrastructura deteriorată	Actorul suspectat	Nava implicată	Explicația oficială (actorul acuzat)	Explicația oficială (statul afectat)
2-8 Feb 2023	Taiwan	Două cabluri submarine	China	Nespecificat	Niciun comunicat oficial	Deteriorare intenționată suspectată
8-10 Oct 2023	Marea Baltică	Conducta Balticconnector, cablul de telecom EE-S1	China	Newnew Polar Bear	Accident	Anchetă în desfășurare
17-18 Nov 2024	Marea Baltică	Cablurile de telecom BCS East-West Interlink & C-Lion1	China	Yi Peng 3	Negare	Anchetă în desfășurare
25 Dec 2024	Marea Baltică	Cablul de curent Estlink 2 & 4 linii telecom	Rusia	Eagle S	Negare	Anchetă în desfășurare
3 Ian 2025	Taiwan	Cablu submarin de telecom	China	Shunxin 39 (suspectată)	Neagă implicarea	Deteriorare intenționată suspectată
26 Ian 2025	Marea Baltică	Cablul de telecom C-Lion1	Rusia	Vezhen (suspectată)	Niciun comunicat oficial / negare	Anchetă în desfășurare
25 Feb 2025	Taiwan	Cablu de telecom submarin	China	Hongtai	Niciun comunicat oficial / negare	Deteriorare intenționată suspectată

Tabel 1. Incidente recente cu infrastructura submarină în zona Mării Baltice și a Taiwanului.
Surse: Davidson 2025a; Cater 2025; Chang & McCarthy 2025; Miller, Dixon & Stanley-Becker 2025; Martin 2025c; Hale 2025

Chiar dacă regiunea din jurul ZEE a Irlandei găzduiește numeroase cabluri submarine care conectează Europa cu Statele Unite, **atenția Rusiei pare să se fi mutat spre Marea Baltică. Statele NATO riverane au acuzat Moscova că a folosit nave comerciale pentru a deteriora mai multe cabluri în ultimii doi ani.** Previzibil, autoritățile ruse au respins toate acuzațiile. În paralel, situația din jurul Taiwanului este și mai complicată, ținând cont de escaladările militare chineze din regiune (Chang & McCarthy 2025).

Zona din jurul Taiwanului și regiunea Mării Baltice au devenit puncte de interes la nivel internațional, marcate de tensiuni geopolitice și incidente care implică infrastructura submarină. Având în vedere că în aceste regiuni au fost avariate mai multe cabluri de internet și curent, precum și o conductă, au existat discuții cu privire la cauza acestor evenimente, acestea reprezentând fie accidente cauzate de o varietate de factori sau acte coordonate de sabotaj, parte a unor campanii hibride (Besch & Brown 2024; Davidson 2025a; Cater 2025; Martin 2025a; Astier & Kirby 2024; Khorrami 2025). Orișicât, evoluțiile sunt îngrijorătoare, dar nu reprezintă semne ale începerii unor scenarii apocaliptice.

CONTEXT

Primul cablu telegrafic de cupru a fost instalat între Statele Unite și Regatul Unit în 1858, permițând celor două țări să transmită mesaje în timp real (Sanger 2022). Aproape 170 de ani mai târziu, rețeaua globală cuprinde 1,4 milioane de kilometri de cabluri submarine de internet (Ganz et al. 2024, 2). Este important de menționat că sabotarea cablurilor submarine nu reprezintă un fenomen complet nou. În 1898, în timpul războiului hispano-american, marina SUA a tăiat un cablu telegrafic în largul Cubei pentru a perturba comunicațiile adversarilor (Milmo 2024). Șaizeci de ani mai târziu, în 1959, Washingtonul a acuzat Uniunea Sovietică că a avariat în mod deliberat un cablu submarin folosind plase de pescuit (Freund 2025).

În prezent, aproximativ **99% din traficul global de date** trece prin cabluri submarine (Ganz et al. 2024, 2; Sanger 2018; European Commission 2025). Pe lângă rolul lor în telecomunicații, unele dintre aceste cabluri sunt utilizate pentru a transporta energie electrică de înaltă tensiune între state, insule sau către turbine eoliene *offshore* (Freund 2025). Tăierea câtorva cabluri principale ar cauza întreruperi sau încetiniri regionale semnificative, dar tăierea tuturor cablurilor ar distruge internetul global (Ganz et al. 2024, 2). **Conexiunile prin satelit**

nu oferă, deocamdată, o alternativă viabilă – sunt mai lente, mai sensibile la interferențe, mai costisitoare și nu pot susține același volum de date (Freund 2025).

Răspunsurile oficiale la aceste incidente sunt la fel de vagi și lipsite de ambiție precum reglementările internaționale în materie. Convenția ONU privind Dreptul Mării conține articole referitoare la guvernarea cablurilor submarine, însă acestea vizează în principal ce pot sau nu pot face actorii statali în diverse zone maritime (Ganz et al. 2024, 5). Cu toate acestea, cablurile submarine de internet nu sunt vizate protecții clare de regimurile legale existente, nefiind prezente nici mecanisme clare prin care actorii malițioși să poată fi trași la răspundere (Besch & Brown 2024, 6).

Totodată, marile companii din sectorul tehnologic își intensifică eforturile de a dezvolta **cabluri submarine pe scară largă**, întrucât majoritatea cablurilor sunt deținute de companii private (Ganz et al. 2024, 5). În același timp, companiile pot influența politicile statelor privind infrastructura de internet prin finanțarea unor proiecte semnificative sau prin controlarea infrastructurii existente, dar și guvernele pot influența companiile prin reglementări, presiuni politice, precum și capitalizarea acestora pentru a-și promova influența în exterior (Ganz et al. 2024, 6).

Cablurile submarine mai au o vulnerabilitate poate la fel de îngrijorătoare ca deteriorarea fizică – **spionajul**. Dezvăluirile făcute de Edward Snowden în 2013 au arătat că serviciile de informații americane și britanice au pătruns în punctele terminale ale rețelei – locurile unde cablurile ies la suprafață – pentru a extrage și colecta date în urma obținerii unor înțelegeri cu operatorii de telecomunicații (Sanger 2022). Oficiali europeni și americani au atras atenția asupra unor astfel de îngrijorări legate de spionaj și securitate cibernetică în ceea ce privește cablurile submarine dezvoltate și operate de compania chineză **Huawei Marine Networks (HMN)** (Besch & Brown 2024). Un exemplu notabil este cablul PEACE (*East Africa Connecting Europe*), finalizat în 2022, care leagă Europa de Asia prin Africa de Nord și Orientul Mijlociu. La începutul anului 2024, Parlamentul European a adoptat o rezoluție prin care își exprimă temerile legate de legăturile dintre HMN Tech și Armata Populară de Eliberare a Chinei, evidențiind posibilele riscuri de securitate cibernetică (Besch & Brown 2024, 8).

EVENIMENTE RECENTE

Marea Baltică

În octombrie 2023, gazoductul **Balticconnector** dintre Finlanda și Estonia, precum și cablul telecom EE-S1 dintre Estonia și Suedia au fost avariate într-un aparent accident (Besch & Brown 2024, 8). Incidentul a fost provocat de o navă deținută de o companie chineză, *Newnew Polar Bear*, înregistrată în Hong Kong (Khorrami 2025). În august 2024, **guvernul chinez a recunoscut că incidentul a fost cauzat de navă, subliniind că a fost un accident cauzat de condițiile meteorologice** (Besch & Brown 2024, 8).

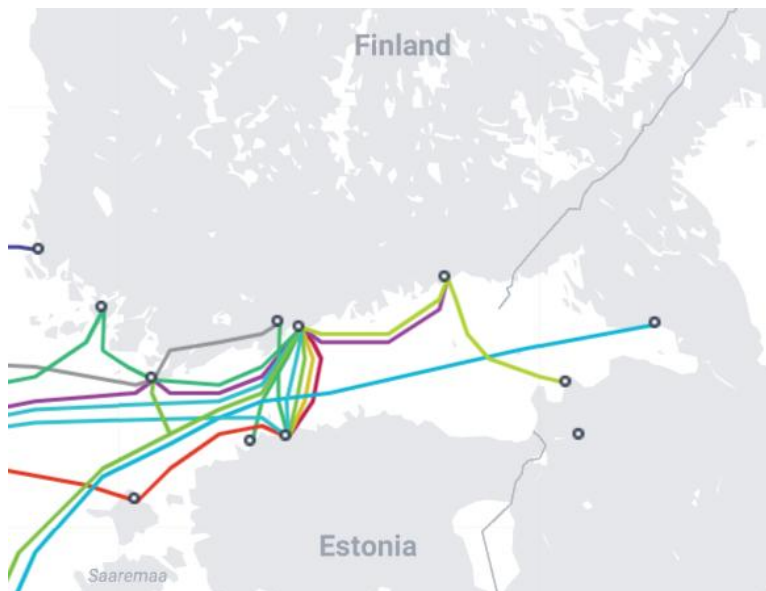


Figura 1. Cablurile submarine din zona Mării Baltice. Sursa: Telegeography 2025

În 17-18 noiembrie 2024, două cabluri telecom submarine – **BCS East-West Interlink**, care leagă Lituania de Gotland, Suedia, și **C-Lion1**, care conectează Germania cu Finlanda – au fost avariate. Autoritățile suedeze și daneze au identificat o navă suspectă de tăierea cablurilor, nava cargo *Yi Peng 3*, înregistrată în China, care a trecut prin zona celor două cabluri în acele două zile (Bryant & Sauer 2024). Imagini sonar au arătat că nava și-a târât ancora pe fundul mării pe o distanță de 160 de kilometri (Hale 2025). Nava *Yi Peng 3* este suspectată de către autoritățile din Germania, Finlanda și Suedia, ridicând astfel suspiciuni privind o posibilă utilizare de către Rusia a unor resurse comerciale chineze pentru acțiuni hibride (Khorrami

2025). În acest context, ministrul german al Apărării, Boris Pistorius, a declarat că există suspiciuni privind acte de sabotaj și acțiuni hibride (Astier & Kirby 2024). China a lansat propria anchetă asupra incidentului, permițând și prezența unor „observatori” din Danemarca, Finlanda, Germania și Suedia la bordul navei (Hale 2025). Ancheta derulată de poliția suedeză este încă în curs (Webster 2025). Cu toate acestea, membri ai Parlamentului European și oficiali din zona de *intelligence*, citați de presa internațională, suspectează implicarea Rusiei (Besch & Brown 2024, 7-8).

Pe 25 decembrie 2024, **patru cabluri de internet submarine și cablul electric Estlink 2** dintre Finlanda și Estonia au fost avariate de un petrolier asociat Rusiei, *Eagle-S*, care și-a târât ancora pe fundul mării timp de 100 de kilometri (Borger 2025). Nava rusească, care transporta petrol din Rusia, a fost reținută de autoritățile finlandeze și a fost eliberată abia în februarie 2025, în timp ce membrii echipajului au primit interdicții de călătorie, iar ancheta penală este în curs de desfășurare (Khorrami 2025; DW 2025; Hale 2025).

Pe 26 ianuarie 2025, **un cablu de internet submarin** din Marea Baltică a fost avariat între Letonia și Suedia (Cater 2025). Operatorul cablului, Centrul de Radio și Televiziune din Letonia, a anunțat că încetirile de internet au fost minime deoarece traficul a fost redirecționat (DW 2025). Prim-ministra letonă Evika Siliņa a declarat că incidentul a fost probabil cauzat de o „influență externă”, în timp ce autoritățile au început să investigheze trei nave suspecte, inclusiv prin trimiterea unei patruli maritime (Cater 2025). Letonia a colaborat îndeaproape cu Suedia și NATO (Cater 2025). În februarie 2025, autoritățile suedeze și finlandeze au anunțat că investighează un alt incident legat de avarierea unui cablu submarin în Marea Baltică, **C-Lion1**, dar a devenit clar că acesta fusese de fapt avariat în urma aceluiași incident investigat în ianuarie (Reuters 2025a; Reuters 2025b).

Strâmtoarea Taiwanului

În februarie 2023, două nave chineze au fost suspectate de autoritățile taiwaneze că ar fi tăiat două cabluri submarine în apropierea **insulelor Matsu**, lăsând locuitorii fără internet (Davidson 2025a). Acesta a fost cel mai grav incident de până acum, fiind provocată o **întrerupere totală a internetului pe insule și necesitând reparații costisitoare**.

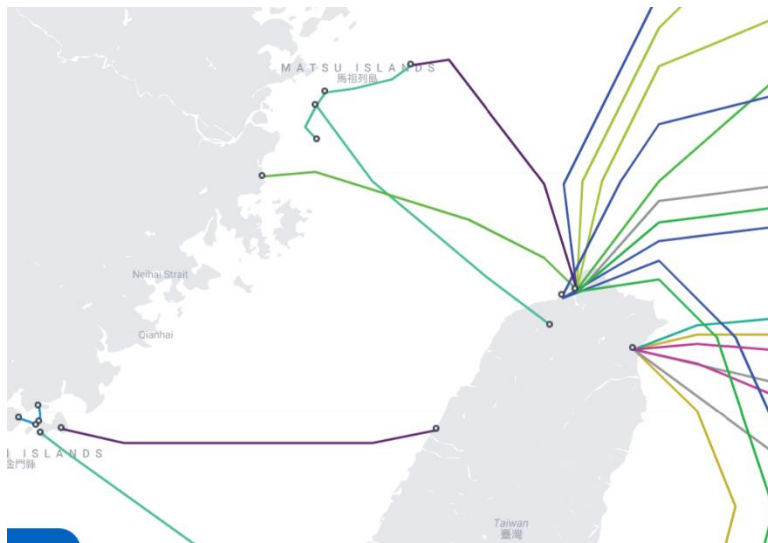


Figura 2. Cablurile submarine din zona strâmtorii Taiwan. Sursa: Telegeography 2025

La începutul lunii ianuarie 2025, un **cablu submarin** dintre Taiwan și SUA a fost avariat în nord-estul Taiwanului. Serviciile au fost în mare parte neafectate, potrivit companiei taiwaneze Chunghwa Telecom, traficul fiind redirecționat către alte cabluri (Davidson 2025a). Cablul a fost avariat de o navă cargo asociată Chinei dar înregistrată în Camerun, *Shunxin 39*, aceasta fiind reținută de către autoritățile taiwaneze după ce a fost suspectată că și-a târât ancora pe fundul mării în zona cablului (Davidson 2025a; Chang & McCarthy 2025). Incidentul este încă în curs de investigare și este considerat drept o posibilă acțiune de sabotaj (Davidson 2025a).

Pe 25 februarie 2025, un alt **cablu submarin** a fost avariat în strâmtoarea Taiwan, între insula principală a Taiwanului și insula Penghu (Davidson 2025b). Autoritățile taiwaneze au reținut o navă cargo sub pavilion togolez cu echipaj chinez și au lansat o investigație oficială, fără a exclude posibilitatea unui act intenționat de sabotaj (Davidson 2025b).

RĂSPUNSURI ȘI IMPLICAȚII

Petrolierul rusesc *Eagle S*, parte din așa-numita **flotă fantomă**, face obiectul unei anchete penale deschise de Finlanda în legătură cu cablul avariat în perioada Crăciunului din 2024 (Cater 2025). Flota fantomă a Rusiei se referă la o rețea de petroliere vechi, cu structuri de proprietate opace, folosite pentru a ocoli sancțiunile internaționale și a vinde petrol pe piețele globale (Miller, Dixon & Stanley-Becker 2025; Jack 2025). Estonia, Finlanda, Letonia și

Lituania analizează mecanismele legale prin care ar putea reține nave din această flotă (Jack 2025).

Într-un alt caz, autoritățile suedeze au eliberat la începutul lunii februarie 2025 nava cargo *Vezhen*, deținut de o companie bulgară, după ce fusese reținut în legătură cu incidentul din 26 ianuarie. Acestea au precizat că nava este suspectată că ar fi provocat avarierea cablului, dar că este vorba de un accident provocat de condiții meteorologice și nu de un act de sabotaj (Martin 2025c). Cu toate acestea, premierul suedez Ulf Kristersson, a declarat în cadrul Conferinței de Securitate de la München din 2025, că **seria de avarieri ale cablurilor submarine nu poate fi considerată pur și simplu o coincidență, sugerând că ar putea fi parte a unor tactici hibride** (Martin 2025b).

În ianuarie 2025, aliații **NATO** din zona Mării Baltice au emis un comunicat în care condamnă actele de sabotaj împotriva infrastructurii critice submarine, precizând totodată că își rezervă dreptul de a lua măsurile necesare împotriva navelor implicate în astfel de incidente (Martin 2025a). Rolul NATO în protejarea infrastructurii critice și prezența sa în Marea Baltică au devenit vizibile în a doua parte a anului 2024. Merită menționat în acest context patrurile navale NATO din Marea Baltică, lansate în decembrie 2024, precum și inițiativa HEIST (*Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications*), care urmărește să asigure redirectionarea traficului de internet prin satelit în cazul unor avarii majore ale cablurilor submarine (Khorrami 2025; NATO 2024; Besch & Brown 2024). La jumătatea lunii ianuarie 2025, NATO a lansat o misiune de protejare a infrastructurii critice în Marea Baltică, desfășurând fregate, drone navale și avioane (DW 2025). Cu toate acestea, riscurile și amenințările la adresa infrastructurii submarine erau cunoscute de Alianță de mai mult timp. Încă din 2023, NATO a înființat *Critical Undersea Infrastructure Coordination Cell*, un mecanism de coordonare menit să sporească colaborarea între state și actorii privați și să evalueze vulnerabilitățile din acest sector (Besch & Brown 2024, 14).

În ceea ce privește Taiwanul, situația este mult mai complicată decât în Europa. **Dacă un actor ar reuși să taie toate cablurile de internet submarin care leagă Taiwanul de restul lumii, țara ar fi nevoită să se bazeze exclusiv pe comunicațiile prin satelit, ceea ce ar provoca perturbări majore în societate, economie, comerț ș.a.m.d.** (Chang & McCarthy 2025). Incidentele din jurul Taiwanului pot fi considerate ca parte a unor interferențe hibride – operațiuni de nivel scăzut care au scopul de a submina și hărțui statul și cetățenii săi – sau care

să pregătească și să testeze terenul pentru eventuale atacuri la scară largă în viitor, având în vedere tensiunile din regiune (Chang & McCarthy 2025).

Până în prezent, **reacțiile sunt încă ambigue**, inclusiv atribuirile făcute țărilor implicate, în timp ce investigațiile sunt încă în desfășurare și nu este clar dacă toate sau doar unele din aceste incidente sunt acte deliberate de sabotaj sau simple accidente. Planul de acțiune al UE pentru Securitatea Cablurilor, publicat în februarie 2025, sugerează faptul că **tiparul observa în ultimul timp indică faptul că infrastructura submarină a devenit ținta unor „acte ostile deliberate” care pot fi considerate elemente ale unor campanii hibride** (European Commission 2025, 1). Planul clarifică aceste acțiuni drept acte de sabotaj care reprezintă „riscuri semnificative pentru securitatea UE” (European Commission 2025, 1). Totuși, *The Washington Post* relatează în ianuarie 2025 că agențiile de informații din SUA și Europa ar fi ajuns la un consens conform căruia majoritatea incidentelor implicând cabluri submarine au fost cauzate de **accidente**, nu de acțiuni deliberate de sabotaj (Miller, Dixon & Stanley-Becker 2025). Prin urmare, au existat declarații contradictorii din partea oficialilor europeni, ceea ce sugerează că atât investigațiile autorităților, cât și evaluările de *intelligence* nu sunt suficient de concludente.

CONCLUZII ȘI RECOMANDĂRI

O întrerupere totală a conexiunilor la internet în Europa, cauzată de tăierea cablurilor submarine, este extrem de puțin probabilă, deoarece există suficiente rute alternative care pot asigura acoperirea în continuare (Besch & Brown 2024, 5). Totuși, țările insulare precum Irlanda, Cipru sau Malta, dar și diverse insule care aparțin altor state, sunt mai vulnerabile din cauza dependenței lor de cablurile submarine (Besch & Brown 2024, 5). Astfel, actori malițioși ar putea sabota aceste cabluri pentru a submina guvernele, a provoca pierderi economice sectorului privat și a stimula neîncrederea cetățenilor în instituții și în securitate, prin întreruperi locale, încetiniri sau testarea terenului pentru un atac mai amplu (Besch & Brown 2024, 5).

Evoluțiile recente privind cablurile de internet submarine sunt îngrijorătoare, dar nu vor duce la scenarii apocaliptice de distrugere a internetului global. Similar cu atacurile cibernetice, riscul unui eveniment catastrofal precum o întrerupere majoră de lungă durată a internetului este scăzut, dar acest lucru nu înseamnă că guvernele nu ar trebui să se pregătească pentru un asemenea scenariu. Astfel de acțiuni pot produce perturbări serioase alături de alte

operațiuni hibride, subminând autoritatea statelor și a societăților sau afectând activitățile economice. Tăierea unuia sau a câtorva cabluri submarine nu va duce la prăbușirea rețelei de internet a unei țări întregi, dar poate perturba furnizorii de telecomunicații și genera costuri inutile de ordinul milioanei de dolari pentru actori publici și privați.

Chiar dacă unele incidente din zona Taiwanului și a Mării Baltice par să fi fost doar accidente costisitoare, nu toate au fost clasate complet drept posibile acte de sabotaj. **Este puțin probabil ca întreaga serie de incidente să reprezinte doar un șir lung de accidente.** Atribuirea publică este similară cu atribuirea operațiunilor cibernetice malițioase, ambele putând fi încadrate în categoria actelor de sabotaj. Chiar dacă, cel puțin momentan, nu există dovezi concrete că Rusia și/sau China ar fi utilizat deliberat nave comerciale pentru a sabota infrastructură submarină critică, se conturează un model asemănător interferențelor hibride. În același timp, unele incidente pot fi, pur și simplu, accidente, având în vedere cazurile documentate de deteriorare a cablurilor submarine din cauza incidentelor navale sau a unor cauze naturale.

În ansamblu, acest tip de activități se încadrează în așa-numita „zonă gri” sau în sfera influențelor hibride a operațiunilor malițioase, mai apropiate de sabotaj decât de un act de război – subminează statele țintite, hărțuiesc autoritățile, impun costuri inutile fără consecințe directe (ex.: milioane de euro necesare pentru repararea cablurilor) ș.a.m.d. La fel ca în cazul operațiunilor cibernetice ofensive, obiectivul principal pare a fi subminarea suveranității, autorității și securității statului țintit, nu cauzarea unor pierderi catastrofale sau pregătirea unui război. Cu toate acestea, asemenea operațiuni reprezintă și o formă de semnalizare a posturii, indicând disponibilitatea de a deteriora infrastructura critică în timp de pace sau de a lansa atacuri la scară largă în timpul unui război.

Așadar, este necesară atât **protejarea fizică a cablurilor, cât și protejarea lor împotriva atacurilor cibernetice, precum și împotriva activităților de spionaj.** În plus, statele ar trebui să tragă la răspundere actorii care intervin asupra acestor cabluri, cel puțin în mod similar cu reacțiile uzuale în fața operațiunilor cibernetice: **atribuiri publice, sancțiuni internaționale și/sau anchete penale.** Totodată, ar trebui realizate verificări riguroase și anchete privind **proiectele desfășurate de companiile private,** în special HMN Tech și alte companii similare. Europa ar trebui, de asemenea, să monitorizeze și să mențină un echilibru față de dependența de proiecte de cabluri submarine provenite din SUA și de la companii de

tehnologie americane, ținând cont de ultimele evoluții legate de Starlink și companii similare (The Economist 2025).

Recomandările Uniunii Europene asupra acestor chestiuni sunt esențiale. Atât regulamentul DORA (*Digital Operational Resilience Act*) și directiva NIS2 (*Network and Information System 2*) au propus măsuri pentru asigurarea securității infrastructurii de cabluri submarine (Khorrami 2025). În plus, **Planul de acțiune al UE privind securitatea cablurilor** propune utilizarea *Hybrid Toolbox*-ului, care include reacții precum comunicate publice de atribuire comună sau activarea regimului de sancțiuni al UE (European Commission 2025, 15). Alte măsuri propuse includ îmbunătățirea capacităților UE de a răspunde la flota fantomă a Rusiei, consolidarea mecanismelor de tragere la răspundere a actorilor malițioși, consolidarea cooperării cu NATO pe această chestiune și intensificarea comunicării strategice privind securitatea cablurilor și amenințărilor hibride (European Commission 2025, 17).

În ceea ce privește **Romania**, singurul cablu telecom submarin din zona economică exclusivă a țării este cablul KAFOS. Punctele în care intră pe uscat sunt Mangalia (România), Varna (Bulgaria), Iğneada (Turcia) și Istanbul (Turcia). Nodul din Istanbul conectează cablul la sistemul MedNautilus Submarine, care conectează mai multe țări: Cipru, Grecia, Israel, Italia și Turcia. Celelalte cabluri submarine din Marea Neagră sunt Caucasus Cable System (Bulgaria-Georgia), cablul telecom dintre Georgia și Rusia și cele două cabluri din strâmtoarea Kerchi, care conectează regiunea rusă Krasnodar cu peninsula Crimeea, ocupată ilegal de Rusia.

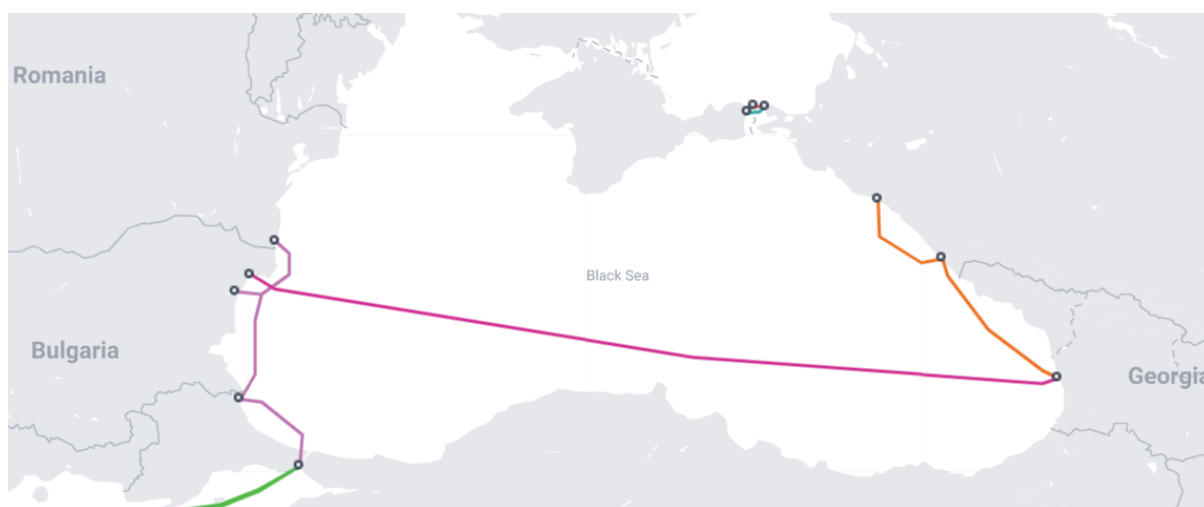


Figura 3. Cabluri submarine în zona Mării Negre. Sursa: Telegeography 2025

Așadar, rolul principal al Bucureștiului este acela de a sprijini țările din jurul Mării Baltice, întrucât zona Mării Negre nu a fost, până acum, un punct central pentru astfel de incidente, în ciuda războiului de agresiune al Rusiei împotriva Ucrainei. România ar trebui să implementeze recomandările Planului de Acțiune al UE în ceea ce privește cablul din propria zonă economică exclusivă și stația din Mangalia, precum și să își intensifice cooperarea cu partenerii din zona Mării Negre și să sprijine aliații din regiunea baltică.

BIBLIOGRAFIE

- Astier, H., & Kirby, P. (2024, 19 noiembrie). Germany suspects sabotage over severed undersea cables in Baltic. *BBC*. <https://www.bbc.com/news/articles/c9dl4vxw501o>
- Besch, S., & Brown, E. (2024, 16 decembrie). Securing Europe's Subsea Data Cables. *Carnegie*. <https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en>.
- Borger, J. (2025, 19 ianuarie). Nato flotilla assembles off Estonia to protect undersea cables in Baltic Sea. *The Guardian*. <https://www.theguardian.com/world/2025/jan/19/nato-flotilla-assembles-off-estonia-protect-undersea-cables-baltic-sea>
- Bryant, M., & Sauer, P. (2024, 20 noiembrie). Swedish police focus on Chinese ship after suspected undersea cable sabotage. *The Guardian*. <https://www.theguardian.com/world/2024/nov/20/sweden-denmark-undersea-cable-sabotage-navy-investigation>
- Burgess, M. (2022, 2 noiembrie). The Most Vulnerable Place on the Internet. *Wired*. <https://www.wired.com/story/submarine-internet-cables-egypt/>
- Cater, L. (2025, 26 ianuarie). Baltic undersea cable likely damaged by 'external influence,' Latvian broadcaster says. *Politico*. <https://www.politico.eu/article/baltic-undersea-cable-damaged-external-influence-latvia/>
- Chang, W., & McCarthy, S. (2025, 10 ianuarie). A cut undersea internet cable is making Taiwan worried about 'gray zone' tactics from Beijing. *CNN*. <https://edition.cnn.com/2025/01/09/china/undersea-cable-taiwan-intl-hnk/index.html>
- Davidson, H. (2025a, 7 ianuarie). Taiwan investigating Chinese vessel over damage to undersea cable. *The Guardian*.

<https://www.theguardian.com/world/2025/jan/07/taiwan-investigating-chinese-vessel-over-damage-to-undersea-cable>

Davidson, H. (2025b, 25 februarie). Taiwan detains Chinese-crewed cargo ship after undersea cable damaged. *The Guardian*.

<https://www.theguardian.com/world/2025/feb/25/taiwan-detains-chinese-crewed-cargo-ship-after-undersea-cable-damaged>

DW (2025, 27 ianuarie). Latvia: Undersea cable likely damaged by external influence. *DW*.

<https://www.dw.com/en/latvia-sweden-cable-damage-nato/a-71416470>

European Commission (2025, 21 februarie). EU Action Plan on Cable Security. *European Commission JOIN(2025) 9 final*. <https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables>

Freund, A. (2025, 2 martie). How sabotage on undersea cables affects our digital world. *DW*.

<https://www.dw.com/en/how-sabotage-attacks-on-undersea-cables-affect-our-digital-stability/a-71494600>

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines*, 34(3), 31.

<https://doi.org/10.1007/s11023-024-09683-z>

Hale, E. (2025, 10 martie). As undersea cables break off Europe and Taiwan, proving sabotage is tough. *Al Jazeera*. <https://www.aljazeera.com/news/2025/3/10/as-undersea-cables-break-down-proving-sabotage-a-difficult-task>

Jack, V. (2025, 11 februarie). Russia lashes out at EU plans to seize its 'shadow fleet' in the Baltic Sea. *Politico*. <https://www.politico.eu/article/russia-lashes-out-against-eu-plans-to-seize-its-shadow-fleet-in-the-baltic-sea/>

Khorrami, N. (2025, 9 ianuarie). Subsea sabotage should spark review of critical infrastructure security. *Binding Hook*. <https://bindinghook.com/articles-binding-edge/subsea-sabotage-should-spark-review-of-critical-infrastructure-security/>

Martin, A. (2025a, 14 ianuarie). Russia warned its 'shadow fleet' could face action from NATO allies. *The Record*. <https://therecord.media/baltic-nato-allies-warning-russia-shadow-fleet>

Martin, A. (2025b, 15 februarie). Sweden's PM on suspected cable sabotage: 'We don't believe random things suddenly happen quite often'. *The Record*.

<https://therecord.media/sweden-pm-on-suspected-russian-cable-breaks-not-an-accident>

Martin, A. (2025c, 3 februarie). Sweden releases suspected ship, says cable break ‘clearly’ not sabotage. *The Record*. <https://therecord.media/sweden-releases-ship-suspected-cable-sabotage>

Miller, G., Dixon, R., & Becker-Stanley, I. (2025, 19 ianuarie). Accidents, not Russian sabotage, behind undersea cable damage, officials say. *The Washington Post*. <https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/>

Milmo, D. (2024, 22 noiembrie). Wire cutters: How the world’s vital undersea data cables are being targeted. *The Guardian*. <https://www.theguardian.com/world/2024/nov/22/wire-cutters-how-the-worlds-vital-undersea-data-cables-are-being-targeted>

NATO (2024, 28 august). *NATO-funded project to reroute internet to space in case of disruption to critical infrastructure*. NATO. https://www.nato.int/cps/en/natohq/news_228257.htm

Reuters (2025a, 21 februarie). Finland, Sweden investigate suspected sabotage of Baltic Sea telecoms cable. *Reuters*. <https://www.reuters.com/world/europe/sweden-investigates-possible-breach-undersea-cable-baltic-sea-prime-minister-2025-02-21/>

Reuters (2025b, February 24 februarie). Damage to Baltic Sea telecoms cable may have occurred in January, operator says. *Reuters*. <https://www.reuters.com/world/europe/damage-baltic-sea-telecoms-cable-may-have-occurred-january-operator-says-2025-02-24/>

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age* (First edition). Crown Publishing Group.

Telegeography (2025). *Submarine Cable Map*. Retrieved 2 April 2025, from <https://www.submarinecablemap.com/>

The Economist (2025, 13 martie). Could Europe replace Starlink if America pulls the plug? *The Economist*. <https://www.economist.com/international/2025/03/13/could-europe-replace-starlink-if-america-pulls-the-plug>

Wall, C., & Morcos, P. (2021, 11 iunie). Invisible and Vital: Undersea Cables and Transatlantic Security. CSIS. <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>



Webster, E. (2025, 21 februarie). Sweden investigates suspected sabotage of undersea telecoms cable. *BBC*. <https://www.bbc.com/news/articles/cy5nydr9rqvo>

IDR

Institutul Diplomatic Român

Misiune. Institutul Diplomatic Român (IDR) își asumă misiunea de a contribui substanțial la creșterea calității diplomației românești prin formare, educare continuă, cercetare, prin dezvoltarea gândirii critice și strategice, prin conectare internațională. O politică externă bună servește unei politici interne benefice.

Principii: valorizarea resurselor umane, profesionalismul, respectul și dialogul, responsabilitatea pentru comunitate.

Pornind de la atribuțiile legale fondatoare ale IDR, dezvoltarea în continuare a institutului se realizează, în funcție de nevoile identificate în MAE, pe următoarele patru direcții:

- Formarea și educarea continuă a diplomaților și a altor categorii de cursanți;
- Aprofundarea dimensiunii de cercetare și expertiză pe spații regionale și problematice funcționale;
- Funcționarea IDR ca *think-tank* al MAE;
- Integrarea IDR în cadrul unei rețele internaționale de institute relevante similare.

Autor: Claudiu Codreanu (PhD) este analist la Institutul Diplomatic Român – Serviciul Furnizare de Expertiză pentru MAE.

Seria Policy Brief IDR

ISSN 2066-5989

ISSN-L 2066-5989

Imagine copertă:

https://commons.wikimedia.org/wiki/File:Telstra_submarine_cable_caution_sign,_Milsons_Point.jpg

Institutul Diplomatic Român - IDR

<https://www.idr.ro/en/> | secretariat@idr.ro

Primăverii 17, sector 1, București, 011972