POLICY BRIEF · SCHUMAN CHALLENGE

Protecting Transatlantic Subsea Cables

Date: April 2026 Words: 299
Team ST9: Ammon Corpron, Ezekiel Johnson, Josiah Osborne

US–EU Subsea Cable Threat Detection Plan

STRATEGIC CONTEXT

Background: Unmonitored Critical Infrastructure

- **Critical Infrastructure:** 17 transatlantic internet cables carry 95% of global internet traffic and over $10 trillion in daily financial transactions.[1] [2] Fewer than 1% of cable landings have monitoring sensors.[3] Cable breaks result in reduced speeds, possible internet outages, and disruption to time-sensitive financial transactions.[4]
- **Escalating Threats:** Hostile actors utilize civilian vessels and submarines to sabotage cables surreptitiously. A lack of monitoring of cables makes legal attribution of attacks difficult. Russia and China have been caught sabotaging cables, but most attacks go unattributed.[5] Every day a cable is down results in a 1% drop in trade and a 2% drop in GDP per capita growth for affected countries.
- **No Current Strategy:** The Congressional Research Service and EU Commission both found that the US and EU have no plan for responding to attacks on subsea cables.[6] [7]

RECOMMENDED ACTIONS

Policy Proposal: US–EU Threat Detection Plan

1. **Nearshore Monitoring via Distributed Acoustic Sensing (DAS):** Upgrade cable landings with DAS, which uses light injection to detect threats nearshore. Costs range from $100k–$500k per site with a 97-99% detection rate.[8] [9]
2. **Deepwater Patrol via Autonomous Underwater Vehicles (AUVs):** Deploy 30 AUVs to major submarine hubs. Recommended system (HUGIN Endurance) provides transatlantic and seafloor mission capabilities.[10]
3. **Transatlantic Intelligence Sharing:** Establish a joint US–EU intelligence sharing unit to coordinate incident responses and legally attribute attacks on cable infrastructure.

Strategic Objective: Deterrence Through Detection

THREE-PART STRATEGY

Nearshore	Deepwater	Intelligence
Monitoring	Patrol	Sharing

KEY FACTS

17
TRANSATLANTIC INTERNET CABLES

95%
OF GLOBAL INTERNET TRAFFIC AT RISK

$10T
IN DAILY FINANCIAL TRANSACTIONS AT RISK

<1%
CABLE LANDINGS CURRENTLY MONITORED

30
AUV UNITS

$1.2B
INVESTMENT

1. Burdette (2025) – How Many Submarine Cables Are There, Anyway? (TeleGeography): https://resources.telegeography.com/how-many-submarine-cables-are-there-anyway.
2. Brookings (2024) – Protecting Underseas Cables: https://www.brookings.edu/articles/protecting-underseas-cables/.
3. Bryan (2025) – Protecting Internet Infrastructure with Submarine Cable Sensing (TeleGeography): https://resources.telegeography.com/protecting-internet-infrastructure-submarine-cable-sensing.
4. Besch & Brown (2024) – Securing Europe's Subsea Data Cables (Carnegie): https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables.
5. *Ibid.*
6. Congressional Research Service (2023) – Protection of Undersea Telecommunication Cables: https://www.congress.gov/crs-product/R47648.
7. European Commission (2025) – Joint Communication on Submarine Cable Security: https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables.
8. Ramirez-Torres et al. (2025) – Vessel Detection with DAS on Submarine Cables (arXiv): https://arxiv.org/abs/2509.11614.
9. Bandweaver (2017) – Economic Benefits of DAS, DTS and RTTR for Power Cables: https://www.bandweaver.com/wp-content/uploads/2017/02/What-are-the-economic-benefits-of-distributed-acoustic-sensing-white-paper-V0.0.3.pdf.
10. Kongsberg Maritime (n.d.) – HUGIN Endurance AUV Datasheet: https://www.kongsberg.com/globalassets/kongsberg-discovery/commerce/surveillance--monitoring/hugin-endurance/473631a_hugin_endurance_datasheet.pdf.