O futuro dos cabos submarinos: 48% mais longos até 2040. Estamos realm

Data: 2025-10-02 15:10:29

Autor: Inteligência Against Invaders

Redazione RHC**:2 Outubro 2025 17:06**

Os cabos submarinos que ligam o Reino Unido ao mundo exterior são vitais para o país, **com transações no valor de £ 220 bilhões todos os dias.** O Comitê Conjunto de Estratégia de Segurança Nacional (JCNSS) *exortou o governo a proteger mais ativamente a infraestrutura de cabos,* o Registro *Relatórios* . Um relatório publicado em setembro chamado **o governo "excessivamente tímido"** em sua abordagem a esta questão.

O relatório observa que **64 cabos ligam o país ao mundo exterior** , transportando a grande maioria do tráfego, **enquanto o tráfego de satélite for insignificante** . Além disso, os backbones digitais são bastante difíceis de proteger: **Aproximadamente 200 cabos quebram a cada ano em todo o mundo devido a causas "naturais".** Quanto mais longe da costa, mais fraca se torna a sua segurança, enquanto os operadores dependem de instalações a maiores profundidades e longe da costa.

Algumas regiões *têm redundâncias para lidar com interrupções.* Por exemplo **75% do tráfego transatlântico do Reino Unido viaja em apenas dois cabos com estações de aterrissagem na Cornualha** , mas o país dispõe de infraestruturas adicionais suficientes para desviar o tráfego em caso de incidente. No entanto, os problemas de ligação com o resto da Europa podem causar problemas muito mais graves, pelo que deve ser dada maior atenção à capacidade de lidar com choques inesperados.

A Rússia é mencionada como um adversário em potencial, supostamente tendo explorado a possibilidade de guerra de informação destinada a cortar certos territórios das telecomunicações por muitos anos. **A Rússia teria os meios técnicos para detectar cabos em grandes profundidades.** No entanto, na prática, os danos ocorrem com mais frequência em profundidades relativamente rasas e não requerem equipamentos especializados. Por exemplo, em novembro de 2024, o **Navio Yi Peng 3** danificou dois cabos entre a Suécia e a Lituânia com sua âncora. Um mês depois, **o navio Eagle S** danificou um cabo de eletricidade e três cabos de telecomunicações que ligam a Finlândia e a Estônia. Os cabos no Mar Vermelho também foram danificados por âncoras em várias ocasiões.

Um dos principais problemas com esses acidentes é *a dificuldade em provar sua intencionalidade, especialmente porque os especialistas ainda discordam sobre a natureza dos acidentes.* No entanto, um precedente já foi estabelecido em Taiwan. O JCNSS acredita **é necessário estar preparado para tais acidentes, independentemente de sua natureza, especialmente considerando que, de acordo com a TeleGeography** , a necessidade de novos cabos **levará a um aumento de 48% em sua duração até 2040** , e o volume anual de trabalhos de reparação aumentará em **36% até**

2040. Existem *62 embarcações de colocação e reparo de cabos em todo o mundo, o suficiente para durar 15 anos.*

De acordo com o JNSS , **o Reino Unido não tem seus próprios navios de reparo e o acesso a alguns cabos é caro e difícil,** com um navio capaz de trabalhar em apenas um cabo de cada vez. O comitê recomenda **estabelecer um navio de reparo no Reino Unido até 2030 e treinar sua tripulação na Marinha** . Em tempos de paz, poderia ser alugado para empresas privadas. O JCNSS argumenta que *a situação na próxima década pode ser imprevisível, deixando o Reino Unido vulnerável.* Mesmo uma declaração pública de preparativos de defesa robustos poderia reduzir a probabilidade de sabotagem.

Além disso, recomenda-se que *os cenários de risco incluem a possibilidade de uma campanha coordenada contra cabos e estações de aterrissagem localizadas em áreas remotas do Reino Unido.* Estudos detalhados do potencial de desprendimento do cabo também são recomendados. O governo afirma que já adotou medidas abrangentes de proteção, incluindo a iniciativa Baltic Sentry, a atualização do **Lei de Proteção de Cabos Submarinos de 1885** , e a compra de uma embarcação para monitorização e proteção de cabos, sendo improvável o cenário apresentado pelo JCNSS.

Em qualquer caso, **Alguns especialistas observam um interesse crescente entre governos e empresas privadas em examinar até que ponto suas atividades dependem da integridade das comunicações.** O rápido crescimento das leis de soberania digital provavelmente está ligado ao desejo de imprResiliência das infra-estruturas de informação. No entanto, tais iniciativas têm muitas consequências negativas. Por exemplo, localizar o poder de computação e os dados no próprio território, em vez de onde é economicamente viável, inevitavelmente leva ao aumento dos custos.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli