I cavi sottomarini per le comunicazioni e la loro sicurezza

La rete di cavi sottomarini per le telecomunicazioni e la sua rilevanza

La rete transnazionale di cavi dati sottomarini per le telecomunicazioni, composta da cavi in fibra ottica posati sul fondale di mari e oceani, costituisce un'infrastruttura critica cruciale nella nostra epoca. Ad oggi vi sono nel mondo più di 400 cavi sottomarini, con una lunghezza totale di almeno 1.300.000 chilometri (Wall e Morcos 2021). Le attività di progettazione, costruzione, posa e manutenzione di queste infrastrutture sono quasi interamente nelle mani del settore privato (Wall e Morcos 2021; Frazier 2023).

I cavi sottomarini per le telecomunicazioni, trasmettendo rapidamente elevati volumi di dati, collegano digitalmente Paesi in tutto il mondo, tra cui anche l'Italia e altri Paesi europei (si vedano, tra gli altri, Wall e Morcos 2021, Bueger et al. 2022).

Secondo le informazioni disponibili, oltre il 95% delle comunicazioni digitali mondiali transita attraverso questa rete globale nel dominio subacqueo. Inoltre, i cavi sottomarini costituiscono una sorta di spina dorsale dell'economia globale (Bueger et al. 2022), con circa 10.000 miliardi di dollari di transazioni finanziarie trasmesse ogni giorno tramite questi cavi (Wall e Morcos 2021).

Oltre all'impiego per scopi civili, gli Stati dipendono dai cavi sottomarini anche per la sicurezza nazionale. Questa infrastruttura critica è infatti cruciale per l'attività e il coordinamento delle operazioni militari, delle missioni diplomatiche e delle attività di *intelligence*.

La sicurezza dei cavi sottomarini

A causa della rilevanza di questi cavi sottomarini, le conseguenze di qualsiasi forma di danneggiamento possono essere assai significative.

Ad oggi i guasti registrati sono quasi sempre dovuti a negligenza ed errori umani, a cominciare da danni provocati da attrezzature per la pesca e da dispositivi di ancoraggio di navi (tra gli altri, Hillman 2021).

Nel 2008, per esempio, un danno non intenzionale a un cavo sottomarino che collega anche l'Italia con l'Egitto lasciò decine di milioni di utenti senza accesso a internet in Medio Oriente e Asia e, secondo le informazioni disponibili, determinò altresì una riduzione dell'impiego di droni da parte delle Forze armate degli Stati Uniti impegnate in Iraq (Hinck 2018).

Nondimeno, non si può escludere il rischio di danni provocati deliberatamente, da attori statali o non-statali, per quanto a oggi i casi confermati di attacchi o sabotaggi siano in numero assai limitato e di modesta portata (per esempio, Hillman 2021, 9).

In generale, la sicurezza e la resilienza della rete dei cavi sottomarini per le telecomunicazioni è un aspetto poco esaminato e studiato della sicurezza internazionale (Bueger e Liebetrau 2021), anche per la scarsa «visibilità» pubblica di queste strutture poste sui fondali di mari e oceani (si veda Bueger e Edmunds 2017).

Minacce intenzionali ai danni dei cavi sottomarini

Studiosi ed esperti hanno delineato diversi scenari relativi a una possibile azione di danneggiamento o compromissione intenzionale.

Attacchi di natura fisica potrebbero essere condotti utilizzando ancore e dispositivi di dragaggio di navi civili (comprese navi da ricerca, pescherecci, navi da trasporto); impiegando esplosivi sottomarini; oppure avvalendosi di sommergibili, sottomarini, droni subacquei o altri mezzi di tipo militare. A essere oggetto di attacchi fisici potrebbero essere anche le strutture terrestri come le «stazioni di atterraggio» (*landing stations*) cui i cavi sottomarini sono collegati (Bueger et al. 2022).

Un altro rischio è quello di un attacco cibernetico all'infrastruttura, per esempio intervenendo sul sistema di gestione della rete.

Infine, si può menzionare l'eventualità di un'azione di intercettazione delle informazioni trasmesse dai cavi, allo scopo di appropriarsene (cfr. Khazan 2013), per esempio per scopi di *intelligence*. Secondo gli esperti, nell'ambiente subacqueo tale genere di operazione sarebbe oggi molto difficoltoso dal punto di vista tecnico; meno complessi potrebbero essere invece interventi alle stazioni a terra oppure a componenti dell'infrastruttura prima della loro posa (Bueger et al. 2022, 30).

Tipi di attori interessati a un attacco

Diversi tipi di attori potrebbero rendersi responsabili di un attacco deliberato, fisico o anche cibernetico, a cavi sottomarini per le telecomunicazioni (tra gli altri, Bueger 2022 et al.). Ad aggravare potenzialmente i rischi vi è anche il fatto che le informazioni sulla posizione di tali cavi sono di facile accesso (Martinage 2015, 119). Attori statati potrebbero essere interessati a danneggiare questa infrastruttura critica per raggiungere diversi obiettivi politici, tra cui, per esempio, interrompere le comunicazioni militari o governative nelle prime fasi di un conflitto armato, bloccare l'accesso a internet per la popolazione di uno Stato avversario, causare danni economici per sabotare un concorrente o per altre ragioni (Wall e Morcos 2021). In particolare, secondo studiosi ed esperti occidentali, le attività della Federazione Russa richiedono particolare attenzione in questo campo (per esempio, Hinck 2018). In anni recenti erano già emerse preoccupazioni sull'interesse mostrato dalla Marina russa per la collocazione geografica di cavi sottomarini rilevanti per Stati membri della NATO (per esempio, Sanger e Schmitt 2015). Le condizioni geopolitiche determinate dallo scoppio della guerra in Ucraina hanno accresciuto ulteriormente i pericoli potenziali (si veda Siebold 2023).

Nel campo degli attori sub-statali, si può sostenere che anche organizzazioni terroristiche e gruppi ribelli potrebbe essere interessati ad attaccare cavi sottomarini. Un certo numero di organizzazioni terroristiche ha già dimostrato la volontà e persino la capacità di colpire infrastrutture critiche, anche in anni recenti; inoltre, alcune organizzazioni terroristiche hanno anche dato prova di poter operare anche in mare (per esempio, Tallis 2022). In alcune regioni del mondo, come nell'Oceano Indiano occidentale, il rischio è presumibilmente meno ridotto di quanto possa apparire in Occidente.

Infine, organizzazioni o reti criminali, comprese quelle dedite alla pirateria, potrebbero ricercare opportunità per sfruttare le vulnerabilità della rete di cavi sottomarini, per scopi economici; potrebbero, per esempio, minacciare un attacco per ottenere un riscatto (Bueger 2022 et al.).

Conclusioni

Nell'ultimo decennio, anche a seguito della salienza politica e visibilità della guerra in Ucraina, così come dell'azione non rivendicata di sabotaggio del gasdotto Nord Stream nel Mar Baltico il 26 settembre 2022, i cavi sottomarini per le telecomunicazioni hanno apparentemente attirato un'attenzione crescente da parte dei decisori politici (per esempio, Bueger et al. 2022, Keller 2023), oltre che degli esperti. Nondimeno, com'è stato notato, il regime giuridico internazionale che può essere applicato a queste infrastrutture critiche è spesso percepito come obsoleto e disorganico e di fatto come non adatto alle sfide attuali (si veda, in particolare, Marina Militare e Civiltà delle Macchine 2023). Secondo alcuni studiosi ed esperti, anche la *governance* europea della protezione dei cavi sottomarini richiede ulteriori progressi (tra gli altri, Bueger et al. 2022). Per tutte queste ragioni, la rete globale dei cavi sottomarini per le telecomunicazioni e la sua sicurezza meritano grande attenzione.

Bibliografia

- Bueger C. e Edmunds T. (2017). Beyond seablindness: a new agenda for maritime security studies. *International Affairs*, 93(6): 1293-1311.
- Bueger C. e Liebetrau T. (2021). Governing hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, 3: 391-413.
- Bueger C., Liebetrau T. e Franken J. (2022). *Security threats to undersea communications cables and infrastructure – consequences for the EU*. In-depth Analysis, European Parliament, testo disponibile al sito: https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557 (consultato il 4 settembre 2023).
- Frazier K. (2023). On Protecting the Undersea Cable System. *Lawfare*, 12 gennaio, testo disponibile al sito: https://www.lawfaremedia.org/article/protecting-undersea-cable-system (consultato il 4 settembre 2023).
- Hillman J. (2021). *Securing the Subsea Network: A Primer for Policymakers*. Report. Center for Strategic and International Studies (CSIS), 9 marzo, testo disponibile al sito: https://www.csis.org/analysis/securing-subsea-network-primer-policymakers (consultato il 4 settembre 2023).
- Hinck G. (2018). Evaluating the Russian Threat to Undersea Cables. *Lawfare*, 5 marzo, testo disponibile al sito: https://www.lawfaremedia.org/article/evaluating-russian-threat-undersea-cables (consultato il 4 settembre 2023).
- Keller J.B. (2023). The Disconnect on Undersea Cable Security. *Lawfare*, 7 maggio, testo disponibile al sito: https://www.lawfaremedia.org/article/the-disconnect-on-undersea-cable-security (consultato il 4 settembre 2023).
- Khazan O. (2013). The Creepy, Long-Standing Practice of Undersea Cable Tapping. *The Atlantic*, 16 luglio, testo disponibile al sito: https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (consultato il 4 settembre 2023).
- Marina Militare e Civiltà delle Macchine (2023). *Geopolitica, strategia, interessi nel mondo subacqueo. Il ruolo dell'Italia*. Rapporto, Fondazione Leonardo – Civiltà delle Macchine e Marina Militare, 28 marzo, testo disponibile al sito: https://www.civiltadellemacchine.it/documents/14761743/0/Rapporto_Civilt%C3%A0+del+Mare.+Geopolitica%2C+strategia%2C+interessi+nel+mondo+subacqueo.pdf?t=1679995813451 (consultato il 4 settembre 2023).
- Martinage R. (2015). Under the Sea: The Vulnerability of the Commons. *Foreign Affairs*, 1: 117-126.
- Sanger D.E. e Schmitt E. (2015) Russian Ships Near Data Cables Are Too Close for U.S. Comfort. *The New York Times*, 25 ottobre, testo disponibile al sito: https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html (consultato il 4 settembre 2023).
- Siebold S. (2023). NATO says Moscow may sabotage undersea cables as part of war on Ukraine. *Reuters*, 3 maggio, testo disponibile al sito: https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/ (consultato il 4 settembre 2023).
- Tallis J. (2022). Maritime Terrorism. In: R.-L. Boşilcă, S. Ferreira e B.J. Ryan, a cura di, *Routledge Handbook of Maritime Security*. Abingdon: Routledge, 189-199.

- Wall C. e Morcos P. (2021). Invisible and Vital: Undersea Cables and Transatlantic Security. Commentary. Center for Strategic and International Studies (CSIS), 11 giugno, testo disponibile al sito: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security (consultato il 4 settembre 2023).