Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

cepAdhoc

Nr. 13 | 2022 27 Ottobre 2022

La vulnerabile spina dorsale dell'Europa

Perché l'UE deve proteggere meglio le proprie infrastrutture digitali essenziali

Anselm Küsters

I recenti attacchi ai gasdotti e ai cavi ferroviari documentano la vulnerabilità delle infrastrutture essenziali. Gli sforzi per proteggere la spina dorsale digitale europea risultano in ritardo ed insufficienti. Il Centres for European Policy Network (CEP) propone quindi una iniziativa europea di *"Clean Cable"*. Inoltre, i nodi della rete dovrebbero essere monitorati militarmente e le iniziative esistenti andrebbero accelerate.

- La dipendenza dell'Europa da cavi marini profondi non europei per il trasporto di dati rappresenta un rischio per la sicurezza. Gli esperti sono a conoscenza di questa **vulnerabilità** da molto tempo. Meno noto è che nemmeno tutti i flussi di dati militari possono essere dislocati sui satelliti, come, ad esempio, il controllo in tempo reale dei droni.
- Tuttavia, **manca un'azione europea concreta e rapida** per garantire reti resilienti, infrastrutture dorsali resistenti e cavi sottomarini sicuri. In futuro, l'UE dovrebbe assumersi un ruolo di **coordinamento essenziale** per migliorare la protezione delle infrastrutture digitali.
- Il CEP chiede un **programma europeo di investimenti di tipo "Clean Cable"** ed una **protezione militare immediata**. Questo dovrebbe garantire che i cavi sottomarini essenziali non vengano intercettati o sabotati. Inoltre, per proteggere meglio i flussi di dati sensibili è necessaria un'attuazione più rapida dei piani della Commissione sulle infrastrutture essenziali e sulle comunicazioni satellitari, nonché una coerente e valida crittografia.

Indice

Lista dei grafici

1 La spina dorsale del mondo digitale è in pericolo

A prima vista, sembra la rete della metropolitana di una moderna metropoli - ma si tratta della rete mondiale dei cavi in fibra ottica oceanica che costituisce la "spina dorsale"[1] del traffico di dati digitali (Fig. 1). Questi cavi permettono agli europei di svolgere agevolmente il proprio lavoro al computer, di consumare notizie e di rimanere in contatto con i propri conoscenti. Tradizionalmente di competenza delle classiche aziende di telecomunicazioni, la loro posa è ora al centro dell'attenzione anche di pionieri digitali globali come Google o Huawei, nonché di esperti militari e di sicurezza.[2] Cosa succede quando questa infrastruttura digitale critica viene meno lo si può intuire leggendo "In the Midst of the Night". Pubblicato nel 2020, il romanzo sociale di Rumaan Alam accenna vividamente al panico che si diffonderebbe rapidamente con la perdita della ricezione di internet o dei telefoni cellulari.[3] Gli eventi delle ultime settimane – dalle falle sul Nord Stream all'atto di sabotaggio contro la Deutsche Bahn - dimostrano che non è detto che un tale scenario sia destinato a rimanere una finzione.

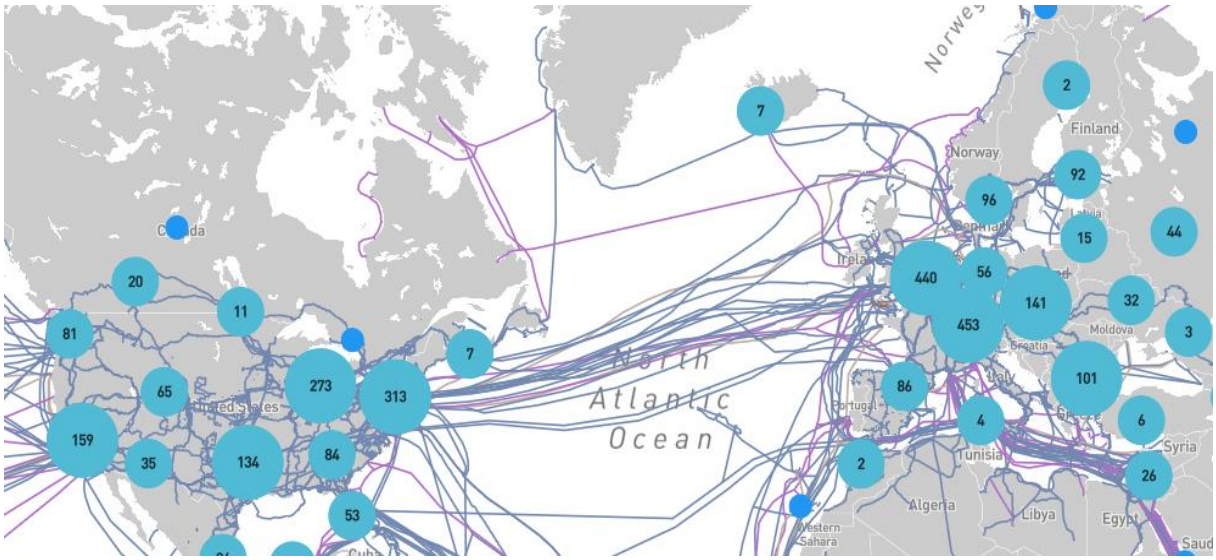

Figura 1: La Rete internet occidentale

Nota: i centri dati sono rappresentati da cerchi blu, i cavi di profondità da linee (blu = attivo; viola = progetto). Fonte: Schermata di Infrapedia con selezione propria dei dati (al 13 ottobre 2022).

Nelle ultime settimane le segnalazioni di cavi interrotti sono apparse con maggiore frequenza ed hanno suscitato una maggiore sensibilità a causa delle tensioni geopolitiche con la Russia. Ad esempio, la notte del 19 ottobre, i cavi in fibra ottica francesi sono stati deliberatamente tagliati in almeno tre punti vicino a Marsiglia[4]. Questo ha interrotto il flusso internazionale di informazioni, essendo Marsiglia un importante centro di smistamento dati. Il giorno successivo si è saputo che due cavi sottomarini a nord della Scozia erano stati danneggiati contemporaneamente, con la

[1] Boie, J. / Frederik Obermaier, F. (2013), Rückgrat des weltweiten Datenverkehrs, SZ 4.8.2013, https://www.sueddeutsche.de/digital/infrastruktur-des-internets-rueckgrat-des-weltweiten-datenverkehrs-1.1737792.
[2] Hummel, T. / Karon, J. (2022), Das Geschäft mit Tiefseekabeln, SWR2 16.6.2022.
[3] Alam, R. (2022), Inmitten der Nacht, btb Verlag: Deutsche Erstausgabe 18.10.2021.
[4] Ermert, M. (2022), Frankreich: Anschlag auf Glasfaserkabel, Heise Online 20.10.2022, https://www.heise.de/news/Frankreich-Anschlag-auf-Glasfaserkabel-bremst-internationalen-Datenverkehr-aus-7315563.html.

conseguenza che gli abitanti delle isole Shetland non potevano accedere ad Internet o effettuare chiamate di emergenza con il telefono cellulare.[5]

In linea di principio, la rottura di cavi sottomarini e soprattutto di cavi posati sulla terraferma non è affatto rara, senza che vi siano scenari geopolitici o gravi conseguenze da tirare in ballo. L'Agenzia per la sicurezza informatica dell'Unione europea (UE) pubblica un rapporto annuale sui principali incidenti di sicurezza delle telecomunicazioni. Questo per lo scorso anno elenca 168 incidenti presentati dalle autorità nazionali di 26 Stati membri dell'UE e 2 di Paesi EFTA. La maggior parte di queste rotture nell'infrastruttura digitale sono dovute a incidenti per ragioni diverse quali; lavori di costruzione, fenomeni naturali come incendi o altre esternalità casuali ed hanno solo un impatto locale, cioè riguardano solo poche migliaia di utenti internet[6]. Solo il 5% degli incidenti è stato classificato come doloso, pari a 73 incidenti nel corso di oltre 11 anni[7]. Tuttavia, è anche dimostrato che i dati sono incompleti[8]e il contesto geopolitico in rapida evoluzione porteranno a una nuova valutazione della sicurezza dei cavi più strategici.

Negli ultimi giorni il dibattito ha raggiunto, ad esempio, con veemenza il livello politico tedesco ed europeo. I membri del Bundestag temono che la Russia stia pianificando anche attacchi alle infrastrutture essenziali tedesche.[9] Già nella riunione informale del Consiglio europeo del 7 ottobre 2022, i leader dell'UE hanno discusso della protezione delle infrastrutture essenziali, accanto alle questioni urgenti della crisi dei prezzi dell'energia e del sostegno all'Ucraina.[10]Il presidente francese Macron ha chiesto una strategia europea comune. Secondo Macron, anche la lotta contro gli attacchi informatici russi o iraniani rende indispensabile un adeguato approccio europeo. Tre giorni dopo, la Presidente della Commissione europea Ursula von der Leyen ha annunciato al Digital Summit di Tallinn che l'UE vuole investire di più nella connettività affidabile.[11]Queste parole saranno seguite da azioni per proteggere il traffico di dati digitali nel continente? E se così fosse, arriveranno in tempo?

2 Le attuali iniziative dell'UE e le loro carenze

Poiché oltre il 95% del traffico dati mondiale passa attraverso gli oceani, la minaccia più grave per l'infrastruttura digitale europea è probabilmente rappresentata dal sabotaggio di alcuni cavi di profondità. È qui che l'ampia dipendenza dell'Europa da fornitori stranieri si sta prendendo la sua rivincita. Nel suo discorso di Tallinn, la Presidente von der Leyen ha menzionato il cavo transatlantico EllaLink che collega l'Europa all'America Latina ed ha elogiato il nuovo cavo in fibra ottica che sta per

---

5 Holland, M. (2022), Zwei Unterseekabel beschädigt, Heise online 20.10.2011, https://www.heise.de/news/Zwei-Unterseekabel-beschaedigt-Shetlandinseln-vom-Internet-abgeschnitten-7315534.html.

6 ENISA (2022), Telecom Security Incidents 2021. Annual Report, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021, S. 13.

7 ENISA (2022), Telecom Security Incidents 2021. Annual Report, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021, S. 22.

8 Ermert, M. (2022), Missing Link: Angriffe auf Backbones, Heise Online 29.05.2022, https://www.heise.de/hintergrund/Missing-Link-Informationsgesellschaft-Wie-sicher-sind-die-Glasfaserkabel-7123783.html?seite=all.

9 Z.B. Roderich Kiesewetter, zitiert in: „Wir sind viel zu passiv.“, Welt Video-Interview 12.10.2022, https://www.welt.de/politik/ausland/video241552891/Ukraine-Roderich-Kiesewetter-zu-den-Angriffen-auf-kritische-Infrastruktur.html.

10 Anghel, Z. (2022), Outcome of the European Political Community and European Council meetings in Prague on 6-7 October 2022, EPRS 11.10.2022, https://epthinktank.eu/2022/10/11/outcome-of-the-european-political-community-and-european-council-meetings-in-prague-on-6-7-october-2022/.

11 Von der Leyen, U. / Kallas, K. (2022), Ein entscheidender Moment der Wahrheit, Gastbeitrag t-online 8.10.2022, https://www.t-online.de/nachrichten/ausland/eu/id_100063020/neue-eu-strategie-diese-lehren-koennen-wir-aus-dem-ukraine-krieg-ziehen.html.

essere posato sotto il Mar Nero come parte della strategia dell'UE *Global Gateway*. Questa è la risposta europea alla *Belt and Road Initiative* cinese, proclamata circa un anno fa, e promette investimenti fino a 300 miliardi di euro per rendere l'Europa più resistente alle crisi, anche attraverso una connettività digitale più forte e diversificata. Inoltre, vi sono prime indiscrezioni non ufficiali rispetto alla volontà della Commissione di cofinanziare un cavo in fibra ottica di 14.000 chilometri che collegherebbe la Scandinavia e l'Irlanda al Giappone attraverso l'Artico.[12]Gli investimenti previsti sono ben visti perché riducono la dipendenza dai cavi terrestri che attraversano la Russia. Inoltre, rappresentano un'alternativa alla Repubblica Popolare Cinese che, con il suo cavo sottomarino *Peace* di 12.000 chilometri, collega l'Europa all'Asia ed insieme alla sua tecnologia 5G, è ora fortemente coinvolta nell'espansione dell'infrastruttura digitale europea – dato di fatto che si teme possa anche permettere di intercettare i dati dei cittadini europei e guadagnare così a potere contrattuale.[13] I cavi europei aggiuntivi non solo proteggerebbero dalle dipendenze e dal furto di dati, ma aumenterebbero anche la resilienza della rete infrastrutturale digitale essenziale europea grazie alla diversificazione.

Tuttavia, finora solo una piccola parte della *Global Gateway Strategy* è stata destinata al miglioramento di questa situazione: l'invito della Commissione a presentare proposte nell'ambito del Meccanismo per collegare l'Europa, pubblicato il 12 ottobre, indica una cifra di 277 milioni di euro per reti sicure, ad alta velocità e ad alta capacità, infrastrutture dorsali e cavi sottomarini.[14] Questo è troppo poco. Inoltre, il termine per la presentazione delle domande si protrae fino al 23 febbraio 2023. Nel complesso, una revisione delle strategie dell'UE commissionata dalla sottocommissione per la sicurezza e la difesa del Parlamento europeo mostra che i cavi e le altre infrastrutture marittime sono menzionati più spesso, ma non esistono quasi misure concrete per generare una protezione effettiva in modo tempestivo.[15] È quindi necessario un potente insieme di strumenti analoghi al *5G Cybersecurity Toolbox* della Commissione, che ha sviluppato misure strategiche e tecniche chiave per la Commissione e/o gli Stati membri sulla base di una valutazione del rischio coordinata a livello europeo. A livello dell'Unione, queste misure concrete includono, ad esempio, un maggiore controllo degli investimenti diretti esteri, strumenti di protezione della politica commerciale, un'applicazione rigorosa del diritto della concorrenza e il coordinamento della standardizzazione, degli obiettivi della politica di sicurezza e dei certificati. Tuttavia, la lentezza con cui è stato attuato finora questo *toolbox* dimostra quanto possa essere lunga la trasformazione delle infrastrutture digitali nonostante i piani dettagliati ed i quadri giuridici.[16]

In teoria sarebbero disponibili più fondi e spazio di manovra se le piattaforme ad alta intensità di dati fossero anche obbligate a finanziare le reti digitali, come è stato proposto nell'attuale dibattito sul futuro modello di fatturazione dell'infrastruttura di telecomunicazione dell'UE.[17] Anche se dal punto

---

[12] Bertuzzi, L. (2022), EU visiert arktisches Internetkabel zur Verbindung Europas mit Asien an, Euractiv 14.10.2022, https://www.euractiv.de/section/innovation/news/eu-erwaegt-arktisches-internetkabel-zur-verbindung-europas-mit-asien/.

[13] Anonym (2022), Die Infrastruktur des Internets, LeitzCloud 6.1.2022, https://leitz-cloud.com/internetkabel.

[14] https://digital-strategy.ec.europa.eu/de/news/launch-new-calls-proposals-budget-eu277-million-support-investments-digital-connectivity (Abruf: 18.10.2022).

[15] Sawall, A. (2022), Europäische Seekabel sollen militärisch geschützt werden, Golem.de 30.9.2022, https://www.golem.de/news/europaparlament-europaeische-seekabel-sollen-militaerisch-geschuetzt-werden-2209-168655.html.

[16] NIS Cooperation Group (2020), Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. Per ulteriori evoluzioni dopo il 26.10.2022 si veda: https://5gobservatory.eu/5g-cybersecurity-toolbox-implementation/.

[17] Bertuzzi, L. (2022), Telekommunikation: Experten sprechen sich gegen Kostenbeteiligung großer Plattformen aus, Euractiv 12.10.2022, https://www.euractiv.de/section/innovation/news/telekommunikation-experten-sprechen-sich-gegen-kostenbeteiligung-grosser-plattformen-aus/.

di vista normativo vi sono problemi fondamentali con questo modello "*Sender Party Pays*", è già un dato di fatto che un numero crescente dei circa 500 cavi di profondità situati in tutto il mondo sono finanziati da società *Big Tech*, mentre le partecipazioni più importanti di Deutsche Telekom risalgono all'inizio del millennio.[18] L'esempio dell'Africa dimostra che il coinvolgimento di attori potenti sul mercato come Google o Microsoft porta a rapidi miglioramenti nelle infrastrutture, ma anche a minacciose dipendenze. In ogni caso, la corrispondente proposta della Commissione sul modello di fatturazione dell'infrastruttura di telecomunicazione dell'UE non figura nel recente programma di lavoro per il 2023; ma è prevista solo una consultazione sul tema all'inizio del prossimo anno. In questo caso, non andrebbero studiati solo i possibili effetti sull'innovazione e sulla concorrenza, come attualmente previsto, ma soprattutto pure gli aspetti legati alla politica di sicurezza.

Oltre alla *Global Gateway Strategy*, il Consiglio e il Parlamento europeo hanno raggiunto un accordo di principio su una Direttiva sulla resilienza delle strutture essenziali, basata su un progetto della Commissione già proposto nel 2020[19]. Questo mira a ridurre la vulnerabilità delle strutture essenziali, anche nei settori della tecnologia dell'informazione e delle telecomunicazioni[20]. Questa proposta integra le proposte della Commissione per una Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS 2), che elenca esplicitamente gli operatori dei nodi internet, e il Regolamento sulla resilienza operativa digitale (DORA), che mira a rafforzare la sicurezza informatica delle imprese finanziarie in caso di crisi.[21] Tutti e tre i nuovi atti giuridici devono ancora essere attuati in modo coordinato dagli Stati membri. Come richiesto dalla Commissaria europea per gli Affari interni Ylva Johansson il 18 ottobre,[22] il lavoro di preparazione, anche da parte degli Stati membri, deve essere accelerato al fine di applicare queste nuove regole il più rapidamente possibile.

Va ricordato che le competenze dell'UE in materia di politica di sicurezza sono definite in modo restrittivo e che il principio di sussidiarietà ha un valore anche in questo caso. Ad esempio, uno Stato membro può sapere meglio della Commissione sovranazionale quali cavi è meglio proteggere e come. Allo stesso tempo, le infrastrutture digitali essenziali in Europa sono spesso strettamente interconnesse, per cui l'interdipendenza giustifica un ruolo speciale dell'UE nelle strutture transfrontaliere e nella loro protezione. Nel complesso, la panoramica evidenzia che le iniziative dell'UE sono comunque chiaramente troppo tardive e suggerisce che per lungo tempo ci si è dimostrati troppo ingenui.

3 Imparare dal passato

[18] Vgl. die Auswertung von TeleGeography-Daten in: Kirsch, S. (2018), Google und Co koppeln sich ab, WirtschaftsWoche 8.2.2018, https://www.wiwo.de/technologie/digitale-welt/tiefseekabel-google-und-co-koppeln-sich-ab/20916398.html.

[19] Commissione (2020), Proposta di direttiva del Parlamento europeo e del Consiglio sulla resilienza die soggetti critici, COM(2020) 829 final, Bruxelles, del 16.12.2020.

[20] I cavi Internet sottomarini non sono menzionati in modo specifico, poiché i cavi non possono essere di per sé strutture essenziali.

[21] Eckhardt, P. (2022), NIS-2 Directive: New EU rules on Cybersecutity, cepAdhoc del 18.10.2022, https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepAdhoc_NIS_2.0/cepAdhoc_NIS_2_Directive_New_EU_Rules_on_Cybersecurity.pdf ; Anzini, M. / Eckhardt, P. (2022), Digital Operational Resilience for financial Entities, cepPolicyBrief del 14.06.2021: https://www.cepitalia.eu/fileadmin/user_upload/cep.eu/cepPolicyBrief_Digital_Operational_Resilience_for_Financial_Entities_COM_2020__595.pdf

[22] Commissione (2022), „Kommission ruft Mitgliedstaaten zu besserem Schutz kritischer Infrastrukturen auf“, Comunicato stampa del 18.10.2022, https://germany.representation.ec.europa.eu/news/kommission-ruft-mitgliedstaaten-zu-besserem-schutz-kritischer-infrastrukturen-auf-2022-10-18_de.

In linea di principio, la vulnerabilità digitale dell'Europa è nota da molti anni. L'idea di intercettare i cavi risale alla Guerra Fredda e i cavi sottomarini erano già stati deliberatamente disturbati durante la Prima Guerra Mondiale.[23] Nel 2015, gli ambienti militari statunitensi hanno riferito che i sottomarini e le navi russe erano sempre più attivi in prossimità dei cavi sottomarini ed hanno espresso il timore che la Russia potesse tagliare i cavi per escludere da Internet le nazioni ostili.[24] Due anni prima, le rivelazioni di Edward Snowden, whistleblower della NSA, avevano mostrato che le agenzie di intelligence statunitensi, oltre a cooperare con gli operatori e i sistemi di *hacking*, potevano anche accedere direttamente alle linee in fibra ottica del mondo[25]. E già nel 2010 Wikileaks aveva pubblicato una lista segreta di importanti infrastrutture che, secondo gli Stati Uniti, avrebbero dovuto essere protette da attacchi terroristici, nominando esplicitamente la città della Frisia orientale di Norden e Sylt, dove ancora oggi arrivano rispettivamente gli importanti cavi sottomarini SEA-ME-WE 3 e AC-1[26]. Attualmente ci sono sedici cavi sottomarini che toccano l'Irlanda, la cui interruzione avrebbe un impatto critico sul traffico internet europeo per diverse ore o addirittura giorni.[27]

La Russia è già in grado di interferire con questa infrastruttura digitale essenziale in qualsiasi momento da diversi anni. Gli esperti di intelligence tedeschi dichiarano apertamente che l'esercito russo dispone di sottomarini e unità "il cui compito originario è quello di intercettare le comunicazioni attraverso i cavi sottomarini, di manipolare le linee e, se necessario, anche di danneggiarle irreparabilmente"[28]. Si tratta probabilmente della nave russa Yantar, che maschera regolarmente il suo itinerario esatto disabilitando il segnale di localizzazione e che si dice abbia due sottomarini orientati a intercettare e tagliare cavi in fibra ottica in profondità.[29] Non sorprende che il guasto del vitale cavo in fibra ottica tra l'arcipelago artico e la terraferma norvegese alla fine dello scorso anno sia stato attribuito allo spionaggio russo,[30]anche se non è possibile (finora) trarre una conclusione definitiva. Gli esperti dell'Atlantic Council, un *think tank* statunitense, avevano avvertito poco prima della guerra in Ucraina che l'esercito russo avrebbe attaccato uno dei cavi sottomarini europei in futuro, oltre a danneggiare fisicamente o interrompere le strutture dei fornitori di servizi Internet e dei punti di scambio Internet. I punti di scambio Internet potrebbero essere fisicamente danneggiati o tagliati fuori dalla rete elettrica.[31]

---

[23] Grunert, F. (2012), Drohnen und SWIFT unter Wasser – Die Relevant von Unterseekabeln, sicherheitspolitik-blog 6.11.2012, https://d-nb.info/1063995795/34.

[24] Gruber, A. (2015), Wenn die Tiefseekabel reißen, SZ 26.10.2015, https://www.sueddeutsche.de/digital/datenverbindungen-im-meer-wenn-die-tiefseekabel-reissen-1.2708619.

[25] Meister, A. (2013), Glasfaserkabel und Spionage-U-Boote, Netzpolitik.org 20.6.2013, https://netzpolitik.org/2013/glasfaserkabel-und-spionage-u-boote-wie-die-nsa-die-nervenzentren-der-internet-kommunikation-anzapft/.

[26] DPA (2010), Wikileaks pubblicò una lista di potenziali obiettivi terroristici, da “Stern” 6.12.2010, https://www.stern.de/politik/ausland/enthuellungsplattform-wikileaks-veroeffentlicht-liste-potenzieller-terrorziele-3873034.html. Documento consultabile (in data 18/10/22) a: https://wikileaks.org/plusd/cables/09STATE15113_a.html

[27] Sherman, J. (2022), Cord-cutting, Russian style, Atlantic Council 31.1.2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/.

[28] Zitiert nach: Sawall, A. (2022), Sicherheitspolitiker warnen vor Angriffen auf Seekabel, Golem.de 4.10.2022, https://www.golem.de/news/geheimdienst-sicherheitspolitiker-warnen-vor-angriffen-auf-seekabel-2210-168688.html.

[29] FutureZone, Russisches Spionageschiff in der Karibik unterwegs, 08.12.2019, https://futurezone.at/netzpolitik/russisches-spionageschiff-in-der-karibik-unterwegs/400697507

[30] Staalesen, A. (2022), 'Human activity' behind Svalbard cable disruption, The Barents Observer 11.2.2022, https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption.

[31] Sherman, J. (2022), Cord-cutting, Russian style, Atlantic Council 31.1.2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/.

Anche se l'UE riuscirà a posare rapidamente un numero sufficiente di cavi e altre infrastrutture digitali essenziali per creare “ridondanza” e quindi maggiore resilienza, la loro protezione rimane una questione difficile. Gli operatori di rete stiano già compiendo enormi sforzi per rendere più resilienti le loro linee in fibra ottica e le stazioni dei cavi attraverso una progettazione specifica dei cavi e dei relativi condotti con l'uso di una tecnologia di sensori e di monitoraggio specializzata[32]. Tuttavia, secondo gli esperti, una protezione completa dei cavi di profondità richiederebbe enormi investimenti in sorveglianza, sottomarini e fregate[33]. Mentre il Regno Unito ha nel frattempo commissionato una seconda nave da guerra per proteggere i cavi sottomarini,[34] gli Stati membri dell'UE non dispongono di tali tipi imbarcazioni. A giugno, uno studio interno per il Parlamento europeo ha identificato numerosi punti "altamente vulnerabili" sui cavi sottomarini in fibra ottica dell'Europa ed ha chiesto un’adeguata protezione militare.[35]

Oltre alla protezione fisica dei cavi, la loro sicurezza informatica risulta pure una questione sempre più importante. Degli atti dolosi contro la sicurezza delle telecomunicazioni europee di cui si è venuti a conoscenza nel periodo tra il 2012 e il 2021, solo circa un terzo riguardava danni fisici, come quelli generati da incendi dolosi o dal taglio deliberato dei cavi, mentre il 64% di queste interruzioni poteva essere attribuito ai cosiddetti attacchi *denial-of-service* (DoS).[36] Con un attacco DoS è possibile distruggere non solo singoli siti web, ma anche intere reti, bombardandole con un numero estremamente elevato di richieste. Nel maggio di quest'anno, il governo tedesco ha ammesso che tali attacchi DoS erano stati condotti contro autorità e ministeri tedeschi, di cui il gruppo di hacker russi Killnet ha successivamente rivendicato la responsabilità[37]. Tuttavia, va sottolineato che nel contesto della guerra in Ucraina, gli scenari di minaccia "*cyber Pearl Harbor*" inizialmente temuti non si sono finora concretizzati[38].

Per i dati particolarmente sensibili nel settore militare, la comunicazione satellitare è generalmente preferibile al trasferimento via cavo via terra o via mare, ma anche in questo caso è possibile individuare una forte vulnerabilità potenziale. Pochi giorni fa, il capo del dipartimento di sicurezza della Federazione delle industrie tedesche ha riferito che la comunicazione satellitare europea è ancora più vulnerabile agli attacchi rispetto ai cavi sottomarini.[39] È quindi positivo che il Parlamento europeo abbia recentemente approvato il piano della Commissione per le comunicazioni satellitari sicure (il relativo trilogo è programmato per la fine di ottobre)[40] - ma il tempo è fondamentale, come

---

[32] Ermert, M. (2022), Missing Link: Angriffe auf Backbones – Wie gut sind Glasfaserkabel geschützt?, Heise Online 29.05.2022, https://www.heise.de/hintergrund/Missing-Link-Informationsgesellschaft-Wie-sicher-sind-die-Glasfaserkabel-7123783.html?seite=all.

[33] Gsteiger, F. (2021), Tiefseekabel, SRF 15.8.2021, https://www.srf.ch/news/international/kuenftige-ziele-im-cyber-krieg-tiefseekabel-sehr-verletzlich-und-wie-geschaffen-fuer-sabotage.

[34] Anonym (2022), Protecting seabed infrastructure, Navy Lookout 3.10.2022, https://www.navylookout.com/protecting-seabed-infrastructure-uk-multi-role-ocean-surveillance-ship-to-be-in-service-by-2023/.

[35] Citazione da: Sawall, A. (2022), Sicherheitspolitiker warnen vor Angriffen auf Seekabel, Golem.de 4.10.2022, https://www.golem.de/news/geheimdienst-sicherheitspolitiker-warnen-vor-angriffen-auf-seekabel-2210-168688.html.

[36] ENISA (2022), Telecom Security Incidents 2021. Annual Report, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021, S. 22.

[37] Bundesregierung bestätigt Hacker-Angriffe, Tagesschau 9.5.2022, https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html.

[38] Schulze, M. (2022), Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022, Stiftung Wissenschaft und Politik 02.05.2022 (Ukraine-Analysen Nr. 267), S. 2-13.

[39] Sawall, A. (2022), Industrieverband hält Satellitennetz für verwundbarer, Golem.de 6.10.2022, https://www.golem.de/news/bdi-industriebverband-haelt-satellitennetz-fuer-verwundbarer-2210-168758.html.

[40] Kabelka, L. (2022), Grünes Licht für EU-Programm für sichere Konnektivität, Euractiv 13.10.2022, https://www.euractiv.de/section/innovation/news/parlamentarischer-hauptausschuss-genehmigt-eu-programm-fuer-sichere-konnektivitaet/.

dimostrano anche le invenzioni sulle decisioni discrezionali di Elon Musk sull'uso del suo sistema satellitare *Starlink* da parte dell'esercito ucraino. Ma anche mettendo da parte i lunghi tempi di preparazione per mandare in orbita i satelliti, questi sistemi non sono una panacea. A partire dagli anni '90 sono stati resi noti casi in cui i criminali sono riusciti ad accedere alle comunicazioni satellitari o addirittura alle loro traiettorie. Inoltre, è poco noto che non tutti i flussi di dati rilevanti dal punto di vista militare possono essere spostati dai cavi sottomarini alla trasmissione satellitare, poiché, ad esempio, il controllo dei droni richiede una trasmissione in tempo reale ed un'elevata larghezza di banda.[41] Questo non è garantito dalla trasmissione satellitare, che ha una latenza ancora troppo elevata[42].

Nel complesso, questi esempi dimostrano che la protezione dei cavi essenziali non può essere gestita solo dagli operatori privati, ma deve essere considerata, nell'attuale contesto geopolitico, un compito cruciale degli Stati membri europei che richiede investimenti coordinati e rapidi. Anche se l'UE ha competenze limitate in questo settore, deve inviare un segnale forte svolgendo un ruolo di coordinamento e fornendo sufficienti capitali di investimento, poiché la protezione delle infrastrutture digitali essenziali può avere successo solo per l'UE nel suo complesso. La catena digitale è infatti forte quanto il suo anello più debole. Anche per questo motivo, sarebbe urgente una maggiore sintonia con le iniziative statunitensi degli ultimi anni. Infine, poiché è difficile garantire una protezione fisica e digitale assoluta dell'infrastruttura dei dati, è essenziale una crittografia adeguata di tutte le informazioni rilevanti.

4 Conclusioni e raccomandazioni

Anche se le attuali iniziative dell'UE riconoscono sempre più l'importanza della sicurezza delle infrastrutture digitali, mancano misure concrete varate in tempo per garantire la protezione. I fondi stanziati per la *Global Gateway Strategy*, che oltre al digitale mira a finanziare progetti nel settore del clima e dell'energia, dei trasporti, della salute, dell'istruzione e della ricerca, devono quindi concentrarsi con urgenza sulla protezione delle infrastrutture digitali essenziali. In seguito all'azione del governo statunitense "*Clean Cable*" lanciata nel 2020[43], un programma europeo di investimenti in *Clean Cable* ed una protezione militare immediata garantirebbero che i cavi sottomarini essenziali che collegano il continente a Internet non possano essere intercettati o sabotati. Inoltre, occorre accelerare drasticamente l'adozione e l'attuazione degli attuali piani della Commissione per le infrastrutture essenziali e le comunicazioni satellitari sicure, e applicare una crittografia adeguata di tutti i dati pertinenti per proteggere meglio i dati particolarmente sensibili. Per questo, il ruolo di coordinamento rivendicato dalla Commissione il 18 ottobre è indispensabile. Senza un'azione rapida, decisa e congiunta da parte degli europei, infatti, la riporta tata distopia di Rumaan Alam rischia di diventare realtà fin troppo presto.

---

[41] Grunert, F. (2012), Drohnen und SWIFT unter Wasser – Die Relevant von Unterseekabeln, sicherheitspolitik-blog 6.11.2012, https://d-nb.info/1063995795/34.

[42] La latenza in questo contesto descrive il tempo di ritardo che i pacchetti di dati impiegano dalla sorgente alla destinazione.

[43] Moss, S. (2020), US 'Clean Network' program seeks to build clouds, cables, and apps free of China, DCD 6.8.2020, https://www.datacenterdynamics.com/en/news/us-clean-network-program-seeks-build-clouds-cables-and-apps-free-china/.

Autore:

Dr. Anselm Küsters, LL.M., Capo dipartimento Digitalizzazione e nuove tecnologie
kuesters@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin
Tel. + 49 761 38693-0

Traduzione (dalla versione in lingua tedesca):

Dott. Andrea De Petris, Direttore scientifico cep Italia
depetris@cep.eu

Centro Politiche Europee ROMA
Via G. Vico, 1 | I-00196 Roma
Tel. +390684388433
cepitalia@cep.eu

Centrum für Europäische Politik FREIBURG|BERLIN,
Centre de Politique Européenne PARIS
Centro Politiche Europee ROMA
Costituiscono il **Centres for European Policy Network** FREIBURG|BERLIN|PARIS| ROMA.

Gli istituti della rete CEP sono specializzati nell'analisi e nella valutazione degli atti promossi dalle istituzioni dell'Unione europea nell'ambito delle politiche di loro competenza e nel quadro d'insieme del processo di integrazione. Il lavoro scientifico, riflesso in particolare nelle proprie pubblicazioni, viene portato avanti indipendentemente da qualsiasi interesse di parte e in favore di una Unione europea che rispetti lo stato di diritto ed i principi dell'economia sociale di mercato.