Geopolitika podmořských komunikací

- CZ24 News | 4. září 2023

Svět je protkán komunikacemi všeho druhu – elektrické dráty, potrubí, dálnice a železnice vedou po zemi a jsou viditelné pouhým okem. Moře a oceány však slouží také k přepravě nejen zboží a zdrojů na lodích, ale také informací a energie pod vodou. Kromě potrubí k nim patří podmořské kabely, které spojují pevninské oblasti mezi kontinenty a ostrovy.

Podmořské kabely lze rozdělit do dvou hlavních kategorií – silové kabely, které přenášejí elektřinu, a komunikační kabely, které se používají pro internetovou komunikaci a nahradily zastaralé telegrafní (telefonní) linky. První napájecí kabel byl položen v roce 1965, aby spojil pevninskou část Kanady (Britskou Kolumbii) s několika ostrovy. Poslední byl položen mezi Peloponéským poloostrovem a ostrovem Kréta v roce 2021. Pokud jde o Rusko, v roce 2015 byl postaven energetický most na Krym, který se však klene nad vodou. Baltské, Severní a Středozemní moře ve svých hlubinách rozpouští elektrické dráty. Ale také v Tichém oceánu a Atlantiku existují podmořské komunikace a plánuje se zprovoznění nových. Přes Černé moře se plánuje kabel o výkonu 1 GW, který bude přenášet elektřinu z Ázerbájdžánu přes Gruzii do Rumunska, Moldavska a zemí EU. Jeho uvedení do provozu je plánováno na rok 2029 [1].

Dno moří a oceánů slouží především k přenosu dat: prochází jím přibližně 99 % internetového provozu. Zatímco před deseti lety se pokládáním podmořských internetových kabelů zabývaly specializované IT společnosti, nyní v tomto odvětví dochází k celosvětovému investičnímu boomu. Odhaduje se, že v příštích dvou letech bude do tohoto oboru investováno 10 miliard dolarů. Konkurence je obrovská, protože každý rok se velké i mladé firmy snaží přijít s novými projekty a uspokojit rostoucí poptávku po zajištění provozu.

Jen v roce 2022 vzrostla kapacita trans-pacifických kanálů meziročně o 35 % na něco málo přes 250 Tb/s. [2].

Nové technologie jsou stále účinnější. Například nejrychlejší, nedávno dokončený transatlantický kabel s názvem Amitié ad je silný jako zahradní hadice, financují ho společnosti Microsoft, Meta a další a dokáže přenášet 400 terabitů dat za sekundu [3].

Takzvaná temná vlákna se používají pro podmořské kabely k přenosu obrovského množství dat z kontinentu na kontinent. Tyto optické sítě obvykle vlastní konsorcia mezinárodních telekomunikačních společností a jednotliví velcí poskytovatelé cloudových a mediálních služeb. Například systém podmořských kabelů 2Africa, který má opásat africký kontinent, je výsledkem spolupráce společnosti Meta Platforms (dříve Facebook) a telekomunikačních společností včetně MTN GlobalConnect, Orange a Vodafone. Podmořský kabel 2Africa je navržen pro propojení až 16 párů vláken, přičemž některé tmavé nebo „nevyužité“ páry vláken jsou vyhrazeny pro budoucí rozšíření [4].

V současné době je na světě více než 552 podmořských internetových kabelů, ačkoli ještě před deseti lety jich bylo téměř třikrát více.

Moderní metody jejich pokládání se od doby v polovině 19. století, kdy byl položen první transatlantický telegrafní kabel, liší jen málo – jsou odvíjeny z lodí. Vzhledem k tomu, že většina kabelů leží v neutrálních vodách, jejich instalace a údržba s sebou nese určitá geopolitická rizika.

Mezi ně patří špionáž. Špionážní aktivity spojené s podmořskými kabely se oficiálně datují od tajné operace s krycím názvem Ivy Bells, kterou v roce 1971 provedla americká ponorka Halibut v Ochotském moři a při níž byl objeven vojenský telekomunikační kabel Sovětského svazu vedoucí po

dně Ochotského moře z Kamčatky na kontinent.

Mezi USA a EU vypukl vážný skandál poté, co se zjistilo, že se zpravodajské služby USA a Spojeného království podílely na průmyslové špionáži proti evropským koncernům. Jednalo se o využívání elektronického zpravodajského systému Echelon, který byl dříve zaměřen na SSSR a jeho spojence. Evropský parlament v roce 1999 zřídil zvláštní komisi pro tuto záležitost, neboť existovalo důvodné podezření, že americké a britské zpravodajské služby předávají důležité údaje konkurentům evropských firem, čímž jim způsobují mnohamilionové ztráty. 5] Komise vypracovala 194stránkovou zprávu, v níž vyjádřila obavy z porušování soukromí a různých důsledků takových systémů pro komerční organizace.

V roce 2005 uvedlo americké námořnictvo do provozu ponorku s jaderným pohonem USS Jimmy Carter (SSN-23), jejíž funkce podle analytiků americké zpravodajské komunity zahrnují také identifikaci podmořských kabelů a jejich odposlech.

Americká armáda je zase znepokojena činností ruských výzkumných lodí. Konkrétně v říjnu 2015 kontradmirál William Marks uvedl, že „došlo ke zvýšené aktivitě ruského námořnictva v blízkosti podmořských kabelových tras, které jsou žilou globální elektronické komunikace a obchodu“ [6]. [6].

USA byly obzvláště znepokojeny trasou ruské lodi Jantar, která na podzim 2015 pomalu plula podél východního pobřeží USA na Kubu. Loď byla neustále monitorována americkými špionážními satelity, loděmi a letadly. Představitelé amerického námořnictva uvedli, že ruská loď měla na palubě speciální podvodní vozidla, která mohla být spuštěna na dno, aby přeřízla podmořský kabel.

Nedávno se podobná tvrzení objevila v souvislosti s internetovými kabely u evropského pobřeží, nyní se však hypotetická aktivita Ruska zdůvodňuje snahou pomstít se za podkopání plynovodu Nord Stream.

Po zahájení speciální vojenské operace začala EU diskutovat o kritické infrastruktuře [7]. 7] Útok na Nord Stream v září 2022 přiměl Evropskou radu, aby v říjnu téhož roku zveřejnila pětibodový plán na zvýšení informovanosti [8]. 8] Následovala směrnice Evropské rady z prosince 2022 o „zvýšení odolnosti kritické infrastruktury“, včetně podmořských kabelů.

Žádná organizace EU však v této oblasti nevede a nemá výslovný mandát k ochraně podmořských kabelů. Námořní bezpečnost v EU obecně zajišťují tři technické agentury, které nejsou součástí ozbrojených sil členských států: Evropská agentura pro kontrolu rybolovu (EFCA), Evropská agentura pro námořní bezpečnost (EMSA) a Evropská agentura pro pohraniční a pobřežní stráž FRONTEX, přičemž pouze poslední jmenovaná agentura má významné donucovací pravomoci. Evropský systém ostrahy hranic (EUROSUR), který provozuje agentura FRONTEX, kombinuje prostředky, jako jsou bezpilotní letadla, radary a letadla, které se však používají především k potírání nelegální migrace.

Nedostatek politických mechanismů v tomto směru vedl k militarizaci tématu bezpečnosti podmořských kabelů v EU. V červnu 2023 otevřelo NATO v anglickém Northwoodu nové středisko, které se věnuje speciálně infrastruktuře podmořských kabelů [11]. 11] Místo samozřejmě nebylo vybráno náhodně, protože Británie je ostrovní stát (Sea Power) a je závislá na spolehlivosti podmořské infrastruktury.

Obecně se anglosaské země v minulosti odvolávaly na tyto umělé hrozby. Například v roce 2012 zveřejnilo Belferovo centrum při Harvardově univerzitě ve Spojených státech studii, podle níž by se moderní technologie mohly využít při přetržení hlubokomořských kabelů. Vzhledem k tomu, že transoceánské kabely, které byly položeny relativně nedávno, vedou prakticky po stejných trasách

jako jejich předchůdci, nebylo by pro příslušné orgány obtížné odhalit jejich hlavní trasy [12].

Zatímco v minulosti docházelo k poškození v mělkých vodách a několik námořních mil od pobřeží v důsledku náhodného lovu vlečnými sítěmi, lodních kotev nebo přírodních katastrof (byli zaznamenáni i žraloci, kteří kabely rozkousali), hlubokomořská sabotáž může způsobit potíže s opravou a může vést ke značným nákladům.

Podmořské transoceánské kabely jsou v hloubkách větších než 300 metrů obvykle pokládány přímo na dno oceánu (dodatečnou ochranu mají pouze v blízkosti břehu). V důsledku toho je lze poměrně snadno poškodit a k jejich čtení jsou zapotřebí pouze speciální přístroje.

Přestože podmořské kabely vedou vysokonapěťový proud, mohou je poškodit nejen speciálně vycvičení sabotéři, ale i „amatéři". V březnu 2013 neznámí útočníci v Egyptě přeřízli podmořský kabel SMW4 750 metrů od pobřeží města Alexandrie [13]. V důsledku přerušení klesla rychlost internetu v Egyptě o 60 %, dokud nebylo vedení obnoveno.

Rizikem jsou také přírodní katastrofy, zejména ve vulkanických oblastech. V roce 2006 způsobilo zemětřesení u pobřeží Tchaj-wanu výpadky internetu na Tchaj-wanu, v Jižní Koreji a v celé jihovýchodní Asii. Opravy tehdy trvaly téměř dva měsíce. A v roce 2021 erupce sopky a následné zemětřesení přerušily podmořské kabely táhnoucí se až na Tongu. Země byla více než tři týdny bez vysokorychlostního internetu a téměř výhradně se spoléhala pouze na mobilní telefonní sítě.

Západ se obává nejen o bezpečnost podmořských komunikací, ale také o bezpečnost Číny. I když kontext je poněkud odlišný, a sice konkurenční. 14] Americké ministerstvo spravedlnosti vydalo prohlášení o kabelové síti Pacific Light, v němž uvedlo, že přítomnost čínských státních příslušníků mezi možnými dodavateli a investory je nežádoucí. Byly vyjádřeny obavy ohledně přístupu k údajům a soukromí. Faktem je, že zákony na ochranu soukromí se v jednotlivých zemích liší a přístupy Pekingu a Washingtonu, stejně jako EU, které jsou největšími hráči v daném odvětví, se liší.

A konečně, samotný zájem Číny o podmořské komunikace a její aktivní účast na jejich pokládce již vyvolává obavy Spojených států, které ztrácejí svůj monopol.

Skupina Hengtong je největší čínskou firmou vyrábějící kabely a vlastní více než 70 různých dceřiných společností. V roce 2020 skupina Hengtong Group koupila společnost Huawei Marine Networks a přejmenovala ji na HMN Technologies. V roce 2021 zařadilo americké ministerstvo obchodu firmu na černou listinu amerických subjektů za podporu „vojenské modernizace Lidové osvobozenecké armády". To skupině Hengtong Group zakazuje přijímat určité zboží podléhající pravidlům správy vývozu bez licence. Protože však má mnoho dceřiných společností, bylo pro USA obtížné sledovat transfery technologií.

Huawei je také na sankčním seznamu USA. Z projektů podmořských kabelů, na kterých se podílela ČLR, se společnost Huawei podílela na přibližně 45 %. Zbývajících 55 % kabelových projektů v ČLR si rozdělily společnosti China Unicom, China Telecom a China Mobile [15].

Rusko není v oblasti podmořské internetové komunikace příliš zastoupeno. Sachalin, stejně jako Kurilské ostrovy, Severní mořská cesta a Kaliningradská oblast jsou spojeny s pevninou. Přitom první autonomní kabel do Kaliningradské oblasti byl položen relativně nedávno, v roce 2021 [16]. Z mezinárodních linek má Rusko kabelové spojení s Finskem, Gruzií a Japonskem. To je vzhledem k velikosti naší země relativně málo, ale zároveň to výrazně snižuje možná rizika. Ačkoli ostatní země v tomto odvětví prakticky nemají naše zastoupení, s vlastními technologickými znalostmi bychom mohli v tomto perspektivním odvětví vytlačit západní společnosti, přinejmenším ve spřátelených zemích.

Před více než deseti lety se diskutovalo o mezikontinentálním kabelu BRICS, ale pak toto téma zmizelo z programu jednání. Možná na tak velkolepý projekt nebyl dostatek finančních prostředků – nebo politické vůle. S rozšiřováním tohoto klubu a se stále větším počtem zemí, které mají zájem na vytvoření multipolárního světového uspořádání [17], však bude téma podmořských komunikací a zajištění jejich bezpečného provozu zcela aktuální.

[1], [2] – news.cn

[3] – cnet.com

[4] – dgtlinfra.com

[5] – zpráva komise : Zpráva o existenci globálního systému pro odposlech soukromých a komerčních komunikací (ECHELON odposlechový systém) (2001/2098(INI))

[6] – David E. Sanger a Eric Schmitt, Ruské lodě v blízkosti datových kabelů jsou pro pohodlí USA příliš blízko // The New York Times , OCT. 25, 2015

[7] – europarl.europa.eu

[8] – ec.europa.eu

[9] – consilium.europa.eu

[10] – dgap.org

[11] – pbs.org

[12] – Michael Sechrist, Nové hrozby, Stará technologie: Zranitelnost v systémech správy sítí podmořských komunikačních kabelů. Diskusní dokument Belfer Center, No. 2012-03, Harvard Kennedy School, únor 2012.

[13] – Al-Masry Al-Youm, internetový sabotér dopaden, říká CEO Telecom Egypt // Egypt Independent , 27. 3. 2013

[14] – justice.gov

[15] – thediplomat.com

[16] – ria.ru

[17] – Leonid Savin. Ordo Pluversalis. Oživení multipolárního světového řádu". PDF

AUTOR: Leonid Savin

Překlad: zvedavec.news

ZDROJ