Cyfrowa dźwignia Teheranu – jak Iran może zagrozić rozwojowi opartemu na danych i nowych technologiach?

Jakub Kukulski
Analityk The Opportunity

25.05.2026

Cieśnina Ormuz to nie tylko kluczowy szlak eksportu ropy i gazu, ale także jeden z najważniejszych węzłów globalnej infrastruktury danych. Zakłócenia w funkcjonowaniu podmorskich kabli światłowodowych oznaczałyby uderzenie w sektor cyfrowy gospodarek GCC – kolejny, po węglowodorach, filar ich modelu rozwoju.

Instytucjonalizacja kontroli nad Cieśniną

9 maja należące do Korpusu Strażników Rewolucji kanały Fars i Tasnim opublikowały dwa podobne artykuły. Twierdziły w nich, że skoro „hiperskalery" (hyperscalers) Amazona, Google'a i Microsoftu w Państwach GCC (Gulf Coooperation Council) są zależne od kabli przebiegających po kontrolowanym przez Iran dnie morskim Cieśniny, Teheran powinien pobierać od amerykańskich firm opłaty licencyjne, a także zmusić je do formalnego działania zgodnie z irańskimi przepisami.

Agencja Tasnim powołała się na art. 34 Konwencji Narodów Zjednoczonych o prawie morza (UNCLOS)[1] , argumentując, że prawa do tranzytu przyznane żegludze [w Cieśninie Ormuz] nie wygaszają suwerenności Iranu nad samym dnem morskim. Agencja pomija art. 79, który wyraźnie chroni prawo do układania i utrzymywania kabli podmorskich.

Ze względu na obowiązujące sankcje, nie istnieje legalna możliwość uiszczania opłat przez amerykańskie firmy. Jednak sposób sformułowania argumentów wskazuje na to, że celem Iranu mogą nie być same opłaty a instytucjonalizacja kontroli nad Cieśniną i kablami.

Okablowany region

Przez podmorskie kable przechodzi do 98% danych na świecie, reszta jest obsługiwana przez satelity. Połączenie kablowe jest nie tylko stabilniejsze, ale też wielokrotnie szybsze niż poprzez satelitę (średnio 340 terabitów na sekundę w przypadku kabla podmorskiego i średnio 100–200 gigabitów na sekundę w przypadku połączenia satelitarnego). Kable są niezbędne dla funkcjonowania współczesnej gospodarki opartej na informacji.

Przez Cieśninę Ormuz, która w najwęższym punkcie ma 54 km szerokości i średnią głębokość 50 metrów, przechodzą obecnie cztery kable: FALCON (FLAG Alcatel-Lucent Optical Network), GBICS/MENA (Gulf Bridge International Cable System/Middle East North Africa Cable System), AAE1 (Asia Africa Europe-1), oraz OMRAN/EPEG (Oman-Iran/Europe-Persia Express Gateway). Planowana jest także budowa trzech kolejnych kabli: FIG (Fiber in Gulf), łączącego kraje GCC i Irak, odnogi Khaleej kabla SEA-ME-WE-6 (South East Asia–Middle East–Western Europe 6), a także odnogi Pearls od obiegającego Afrykę kabla 2Africa.

W promieniu 200 km od irańskiej strony Cieśniny znajdują się istotne stacje lądowania (*landing station*) - miejsca, w których kable podmorskie wychodzą z wody i łączą się z infrastrukturą naziemną: Dubaj, będący stacją lądowania dla trzech kabli, oraz Fudżajra, port leżący nad Zatoką Omańską, w której z infrastrukturą lądową łączy się dwanaście różnych kabli. Dla porównania, największą stacją pod względem ilości kabli w Europie jest Marsylia, gdzie na ląd wychodzi jedenaście kabli.

Operatorzy wykupują zazwyczaj pojemność (*capacity*) przepływu danych na wielu kablach jednocześnie, dzięki czemu w przypadku awarii lub zerwania jednego z nich, dane mogą być przekierowane. Ruch internetowy podlega zasadom protokołu BGP (Border Gateway Protocol). Pakiet danych nie wybiera najkrótszej fizycznej trasy, ale optymalizuje ją w oparciu o dostępną przepustowość, komercyjne umowy o wymianie ruchu oraz koszty dostarczania pakietów. Dopóki istnieje alternatywne fizyczne połączenie, z dostępną przepustowością, na której operator wykupił licencje na przepustowość, dane mogą podróżować nawet jeśli jest to trasa wokół globu.

System posiada więc redundacje, jednak jest ona geograficznie ograniczona do kilku sieci, które nie przebiegają pod wodami Cieśniny Ormuz i w jej pobliżu:

[1] Której Iran nigdy nie ratyfikował

- Do Morza Czerwonego – poprzez naziemną sieć kabli SNFN (Saudi National Fiber Network). Od portu Al-Chubar nad Zatoką Perską do Janbu i Dżeddy nad Morzem Czerwonym. W tych saudyjskich miastach znajdują się stacje lądowania m.in. kabli FLAG Europe-Asia, SE-ME-WE 4 i 5 oraz 2Africa (głównej części);
- Przez Irak do Europy – poprzez iracką sieć naziemną Silk Route i dalej przez turecką EWTC (East West Turkey Connect Fiber Cable System);
- Poprzez OMRAN/EPEG (Europe-Persia Express Gateway), który biegnie od Barki w Omanie, po dnie Zatoki Omańskiej do Iranu, a następnie Azerbejdżan, Rosję, Ukrainę aż do Polski i Niemiec;
- Poprzez omańskie stacje lądowania nad Zatoką Omańską (Barka, Al-Seeb, Al-Bustan, Kalhat) i dalej do Indii;
- Oraz lądowo przez kabel MEETS (Middle East-Europe terrestrial system), który łączy wszystkie państwa GCC z sobą;

Najlepszą redundację posiadają Oman i Arabia Saudyjska. W najgorszej pozycji są Katar i Bahrain, które w wypadku uszkodzenia kabli biegnących przez Cieśninę, muszą zdać się na sieć saudyjską i lądowy MEETS.

Kable – łatwy cel, wymagająca naprawa

Podmorskie kable trudno ochronić, można przerwać niskim kosztem, bez jednoznacznego przypisania odpowiedzialności. Sprawia to, że są idealnym celem dla irańskich działań w „szarej strefie".

Łodzie rybackie i ciągnięcie kotwicy po dnie odpowiadają za około 86% z średnio 200 awarii kabli podmorskich rocznie na świecie. Iran mógłby użyć do przerwania kabli nurków, dronów podwodnych, ale również łodzi o niejasnej przynależności. Skalę trudności w wykrywaniu i jednoznacznym przypisywaniu działań w „szarej strefie" pokazuje przypadek rosyjskiego tankowca Eagle S pływającego pod banderą Wysp Cooka, który uszkodził kable telekomunikacyjne i energetyczne w Zatoce Fińskiej w grudniu 2024 roku. Mimo uznania incydentu przez Estonię i Finlandię za poważną ingerencję w infrastrukturę krytyczną, fiński sąd uniewinnił załogę z powodu braku dowodów na celowe działanie.

Naprawa kabla może trwać od jednego dnia do kilku miesięcy (średnio 44 dni) i kosztować łącznie od 1 do 3 mln USD za całą operację. W warunkach konfliktu wydłuża się czas naprawy, rośnie jej koszt, a także stawka ubezpieczeń statków. Po atakach jemeńskich Hutich na Morzu Czerwonym w 2024 r. koszty ubezpieczeń statków kładących kable w akwenie wzrosły dwukrotnie, nawet do 150 tys. USD za dzień. Cztery firmy odpowiadają za większość (82,7% długości kabli położonych po 2020 r. na świecie) instalacji i naprawy kabli podmorskich : francuska ASN, amerykański SubCom, japoński NEC, oraz chiński HNM Tech (który jednak nie obsługuje, żadnych sieci w regionie). SubCom posiada 8 statków, ASN 7, a NEC nie posiada własnych jednostek, jedynie czarteruje norweski statek Normand Clipper. Obecnie w regionie znajdują się tylko dwie jednostki, obie należą do ASN: uwięziony w saudyjskim porcie Dammam Ile de Batz, oraz Ile de Bréhat na Morzu Arabskim.

Uszkodzenie kabla w Cieśninie Ormuz wiązałoby się nie tylko z kosztami naprawy, ale uszczupliłoby ograniczone możliwości naprawy w innych rejonach świata.

Wpływ fizycznego przecięcia kabla na lokalną architekturę cyfrową

Choć całkowite odcięcie państw GCC od internetu jest mało prawdopodobne ze względu na redundację i ilość alternatyw, to przerwanie kabla spowoduje wysokie koszty dla gospodarek regionu.

W wypadku przekierowania danych zwiększają się opóźnienia i zmniejsza się przepustowość. Ma to szczególne znaczenie dla rynków finansowych państw Zatoki Perskiej, które należą do najbardziej zinformatyzowanych i zintegrowanych z globalnym systemem kapitałowym. W regionie funkcjonują kluczowe giełdy papierów wartościowych, takie jak Dubai Financial Market (DFM) i Abu Dhabi Securities Exchange (ADX) w Zjednoczonych Emiratach Arabskich (ZEA), Saudi Exchange (Tadawul) w Arabii Saudyjskiej – największa giełda na Bliskim Wschodzie pod względem kapitalizacji – a także Qatar Stock Exchange (QSE) w Dosze. Rynki te są silnie uzależnione od algorytmicznego obrotu oraz infrastruktury kolokacyjnej, gdzie przewaga

konkurencyjna liczona jest w mikro- i milisekundach. Nawet minimalne opóźnienia w transmisji danych mogą zaburzać mechanizmy arbitrażu pomiędzy giełdami regionu a centrami globalnymi (Londyn, Nowy Jork, Singapur), prowadząc do strat wynikających z nieefektywnej wyceny aktywów, opóźnionych aktualizacji oraz zmniejszonej płynności.

Zakłócenia mają również bezpośredni wpływ na systemy rozliczeń i płatności, w tym na infrastrukturę SWIFT oraz lokalne systemy RTGS (Real-Time Gross Settlement) wykorzystywane przez banki centralne GCC. Opóźnienia w synchronizacji danych mogą zakłócać rozliczenia transgraniczne, instrumenty pochodne powiązane z ropą i gazem, a także automatyczne systemy zarządzania płynnością.

Degradacja łączności wpływa również na systemy logistyczne, operacje lotnicze, handel elektroniczny oraz infrastrukturę energetyczną, gdzie coraz częściej stosuje się cyfrowe systemy zarządzania siecią i automatyzację w czasie rzeczywistym.

Podnoszenie kosztów bez odcinania kabli

Iran może podnosić koszt funkcjonowania cyfrowej gospodarki Zatoki bez jej fizycznego niszczenia.

Trwający konflikt ma wpływ na planowane inwestycje. Iracko-emiracki WorldLink Transit Cable Project miał być podmorskim przedłużeniem istniejącego kabla łączącego Turcję z Irakiem do Abu Zabi. Koncepcja wycenianego na 700 mln USD projektu opierała się na przedstawieniu Zatoki Perskiej jako bezpieczniejszego połączenia miedzy Europą a Azją. Kontynuacja projektu zapowiedzianego w 2024 r. stoi obecnie pod znakiem zapytania.

Ryzyko i koszty związane z kładzeniem kabli powodują także opóźnienia w instalacji planowanej infrastruktury. Dotyczy to wspomnianej odnogi Khaleej/SEA-ME-WE 6, FIG, oraz Pearl/2Africa. To ostatnie finansuje konsorcjum złożone m.in. z saudyjskiego stc i emirackiego e&, oraz Meta. W SEA-ME-WE 6 udziały ma Microsoft, saudyjska Mobily i Batelco. FIG z kolei jest projektem katarskiej, państwowej spółki Ooredoo.

Obecna sytuacja utrudnia także naprawę i konserwacje podmorskich kabli, które mogą ulec zniszczeniu od niecelowych uszkodzeń.

Iran uderza w rozwój cyfrowy

Każde z państw GCC w ramach odpowiedniej strategii odchodzenia od gospodarki opartej na ropie, rozwija długofalowy program gospodarczy, w którym kluczowym filarem dywersyfikacji jest gospodarka cyfrowa, rozwój sztucznej inteligencji i infrastruktury danych.

W ZEA proces ten jest najbardziej zaawansowany. Kraj posiada 52 aktywne centra danych z czego 34 w Dubaju i 14 w Abu Zabi. Rozwija także megakampusy AI, w tym projekt "Stargate UAE" w Abu Zabi, o planowanej mocy obliczeniowej 1 GW w pierwszej fazie i docelowo do 5 GW, co plasuje go wśród największych planowanych kompleksów obliczeniowych na świecie. Arabia Saudyjska w ramach przetransformowanej strategii Saudi Vision 2030, zaczęła priorytetyzować sektor AI oraz rozbudowę chmur obliczeniowych od 2023 roku. Założona w maju 2025 r. państwowa spółka AI - HUMAIN nawiązała współprace z NVidią, AWS i Google w celu budowy centrów danych o łącznej mocy 2 GW w okolicach Rijadu. Aktywne saudyjskie centra danych skupione są wokół Rijadu (9) i Dammamu nad Zatoką Perską (6). Katar w ramach Qatar National Vision 2030 zbudował 7 centrów danych, Bahrajn posiada ich 8, a 12 omańskich centrów danych jest zlokalizowanych nad Zatoką Omańską, w promieniu 300 km od Iranu.

Ich zagęszczenie oraz waga dla modelu rozwoju sprawia, że stają się celem irańskich ataków. 1 marca drony Shahed uszkodziły dwa centra danych AWS Amazon w ZEA powodując unieruchomienie aplikacji bankowych dla ok. 50 milionów użytkowników.

Iran poprzez blokadę zwiększa także koszt energii w państwach GCC, który jest podstawą konkurencyjności tamtejszych centrów danych. Średni koszt energii elektrycznej dla dużych odbiorców w państwach GCC wynosi około 0,05–0,10 USD/kWh, podczas gdy w Europie może przekraczać 0,15–0,25 USD/kWh. W przypadku eskalacji napięć w regionie i zakłóceń infrastruktury energetycznej, wzrost kosztów energii bezpośrednio przekłada się na koszty operacyjne centrów danych, które stanowią nawet 30–60% całkowitego kosztu ich utrzymania.

Wnioski

Irańska groźba pokazuje, że infrastruktura gospodarki cyfrowej staje się nowym elementem w rywalizacji międzynarodowej. Podmorskie kable, stacje lądowania i centra danych zaczynają pełnić podobną rolę strategiczną jak rurociągi, terminale LNG czy elektrownie. Ich uszkodzenie nie prowadzi do całkowitego „wyłączenia internetu", ale pozwala podnosić koszt funkcjonowania gospodarki cyfrowej przeciwnika, destabilizować przepływy finansowe i zniechęcać inwestorów.

Iran posiada ograniczone możliwości konwencjonalnej projekcji siły wobec państw GCC i Stanów Zjednoczonych, jednak infrastruktura cyfrowa Zatoki daje Teheranowi relatywnie tani i asymetryczny instrument nacisku, którym można operować nie przekraczając progu wojny. W praktyce nawet częściowe uszkodzenie kabli lub podniesienie ryzyka wystarcza, by zwiększyć koszty ubezpieczeń i opóźniać inwestycje. Szczególnie narażone są ZEA, których infrastruktura cyfrowa i finansowa znajduje się w bezpośrednim sąsiedztwie Iranu. Arabia Saudyjska posiada większą głębię strategiczną. Znaczna część jej infrastruktury cyfrowej znajduje się wokół Rijadu. Bahrajn i Katar mają najmniejszą redundacje sieci, a Oman – z wyjściem na Zatokę Omańską i Morze Arabskie – znacznie większą. Te rozbieżności w percepcji zagrożenia mogą dodatkowo rozbijać współpracę między państwami GCC.

Mimo ryzyka „Big Techy" póki co nie wycofują się z regionu. Państwa Zatoki pozostają jednym z najatrakcyjniejszych miejsc rozwoju infrastruktury AI ze względu na tanią energię, dostęp do kapitału państwowych funduszy majątkowych oraz położenie między Europą a Azją. W przypadku dalszych inwestycji w centra danych, budowy podmorskich i naziemnych sieci oraz kampusów AI wzrosną koszty ich ochrony, obsługi i ubezpieczenia.

Wnioski dla Polski i UE

Przypadek państw Zatoki pokazuje, że odporność cyfrowa nie zależy wyłącznie od liczby kabli, ale także od możliwości ich szybkiej naprawy w warunkach kryzysu. W czasie pokoju uszkodzenia infrastruktury podmorskiej są relatywnie łatwe do usunięcia, jednak w środowisku wysokiego ryzyka gwałtownie rosną koszty ubezpieczeń, czas reakcji i ograniczenia logistyczne. Dotyczy to również Europy i Morza Bałtyckiego. Państwa UE są dobrze połączone i całkowite odcięcie regionu od internetu jest mało prawdopodobne, jednak percepcja zagrożenia pozostaje nierówna – Finlandia czy państwa bałtyckie są bardziej zależne od ograniczonej liczby połączeń niż np. Polska.

W praktyce oznacza to konieczność inwestycji nie tylko w redundancję kabli, ale także w zdolności naprawcze: flotę wyspecjalizowanych statków, monitoring infrastruktury podmorskiej oraz technologie pozwalające szybciej identyfikować miejsca uszkodzeń. Obecnie globalne możliwości naprawy kabli pozostają bardzo ograniczone, a większość rynku kontrolują cztery firmy. Wraz z rozwojem AI i gospodarki opartej na danych podmorskie kable będą stawały się coraz bardziej strategicznym zasobem, a konflikty coraz częściej będą wymierzone właśnie w te cyfrowe arterie gospodarki światowej.