Rosyjskie okręty podwodne penetrują morskie szlaki, którymi biegną światłowody łączące informacyjnie kontynenty

FOT. ADOBE STOCK

ROSYJSKIE OPERACJE PODWODNE

Chociaż sytuacja na granicy polsko-białoruskiej jest ciągle niebezpieczna i wymaga ciężkiej pracy naszych służb granicznych, to już trochę przyzwyczailiśmy się do tego stanu rzeczy. To, że jest ona tylko jednym elementem dużo szerszej wojny hybrydowej, jaką rozpoczęła Rosja, zaczyna powoli docierać do coraz większej części społeczeństwa. Widzimy przecież w ostatnich dniach gazowy szantaż Rosji – skierowany przeciwko wszystkim krajom europejskim – który rozpoczął się w bardzo konkretnym momencie, gdy pierwsze rezultaty utopijnej polityki ekologicznej dotyczącej redukcji emisji gazów cieplarnianych zaczęły być odczuwalne.

W tym krytycznym momencie okazuje się, że ceny uprawnień do emisji bardzo wzrosły przez inwestycje spekulacyjne różnych inwestorów, być może powiązanych z rosyjską oligarchią. Dokładnie w tym samym czasie Rosja koncentruje potężne siły wojskowe na granicy z Ukrainą, próbując wymusić szybszą zgodę na uruchomienie rurociągu Nord Stream 2, a także licząc na rozłam w polityce obronnej Unii Europejskiej. Poza tym pojawiają się coraz liczniejsze doniesienia o aktywnym rosyjskim udziale w wojnie informacyjnej dotyczącej trwającej już drugi rok pandemii koronawirusa.

Analizując te wszystkie fakty, otrzymamy pełniejszy obraz tej wojny hybrydowej, jaka toczy się dosłownie na naszych oczach, chociaż jest zupełnie inna niż wszystkie inne konflikty międzynarodowe, z jakimi mieliśmy do tej pory do czynienia. Jej celem są przede wszystkim dezinformacja społeczeństw europejskich, dokonanie rozłamów wewnętrznych, osłabienie rządów narodowych, a nade wszystko ich destabilizacja przez wzniecanie manifestacji i protestów ulicznych. Ma to doprowadzić do osłabienia zaufania społeczeństw do rządów aktualnie sprawujących władzę w poszczególnych państwach, co Rosji ułatwi realizację jej geopolitycznych celów.

Newralgiczne światłowody

O współczesnych metodach, które są stosowane w wojnach informacyjnych, pisałem już na łamach „Naszego Dziennika" („Nowe wojny informacyjne", 12.10.2021 r.), dzisiaj jednak chciałbym zwrócić uwagę na nowy element tej wojny, na który bardzo rzadko zwracają uwagę dziennikarze i analitycy, a społeczeństwo prawdopodobnie zupełnie nie zdaje sobie z niego sprawy. Jest to istotny element infrastruktury informatycznej, który rzeczywiście trudno zauważyć, ponieważ znajduje się on setki, a nawet tysiące metrów pod powierzchnią światowych mórz i oceanów. Są to położone na dnie morskim tysiące kilometrów światłowodów, którymi przesyła się informacje widoczne dla nas, użytkowników, na ekranach telefonów komórkowych i komputerów.

Pomimo olbrzymich inwestycji w inne technologie przesyłania informacji, takie jak: łączność satelitarna, telefonia 5G, czy też łącza radiowe, cały czas ponad 90 proc. dostępnych w internecie informacji przesyłanych jest między krajami a kontynentami za pomocą kabli światłowodowych. Jeśli ktoś chciałby uzyskać bezpośredni dostęp do tej najważniejszej infrastruktury informatycznej i przesłać olbrzymie ilości treści dezinformacyjnych albo „podsłuchać" zawartość przesyłanych informacji, to powinien w odpowiedni sposób podłączyć się do któregoś z kabli za pomocą specjalistycznych urządzeń. Jest to technologia absolutnie niedostępna dla jakichkolwiek grup cyberprzestępców niezależnie od tego, czy pracują dla prywatnych zleceniodawców, czy też pracują na rzecz służb dowolnego kraju. Poza tym kable światłowodowe można po prostu przeciąć albo zniszczyć, i w ten sposób przerwać łączność między różnymi krajami, a w szczególności odciąć Europę od infrastruktury informatycznej Stanów Zjednoczonych. To już bardzo poważne zagrożenie, które spowoduje paraliż gospodarczy, ekonomiczny i społeczny na skalę globalną.

Kable światłowodowe można po prostu przeciąć albo zniszczyć, i w ten sposób przerwać łączność między różnymi krajami, a w szczególności odciąć Europę od infrastruktury informatycznej Stanów Zjednoczonych

Zauważmy, że telefony komórkowe nie korzystają już z niezależnej infrastruktury, ale wykorzystują właśnie ową sieć światłowodową. Zdecydowana większość transakcji handlowych i finansowych przeprowadzana jest właśnie przez tę infrastrukturę. Dokumentacja dyplomatyczna, wojskowa i polityczna również z niej korzysta. Na temat ważnych aspektów rozwoju sieci światłowodowej z punktu widzenia prób chińskiej dominacji pisałem już na łamach „Naszego Dziennika" („Brama do Europy", 4.11.2019 r.). Dzisiaj jednak globalne problemy, które obserwowaliśmy do tej pory raczej na kierunku azjatyckim, dotarły dosłownie do naszego bałtyckiego wybrzeża.

Jak podaje brytyjski „Daily Mail" w artykule z 10 stycznia: Putin chce odłączyć Wielką Brytanię od kontynentu europejskiego poprzez zniszczenie podmorskich kabli światłowodowych. Niektóre z tych światłowodów przez cieśniny duńskie biegną również do Polski. Admirał sir Anthony Radakin, który od listopada ubiegłego roku pełni funkcję szefa brytyjskiego sztabu obrony, uważa, że Rosja postanowiła zaatakować sieć światłowodową. Zwraca on uwagę, że Rosja stała się wrogim mocarstwem, które realizuje najbardziej niszczycielski scenariusz – poza użyciem broni jądrowej – zniszczenia krytycznej brytyjskiej infrastruktury światłowodowej.

W wywiadzie podkreślił on, że obserwowana jest bardzo wysoka aktywność rosyjskich łodzi podwodnych – zarówno w rejonie Morza Północnego, jak i Bałtyku. Według admirała Rosja już tak wysoko rozwinęła swoje możliwości, że może zagrozić podmorskim kablom światłowodowym i wykorzystać je w wojnie informacyjnej. Jednocześnie ostrzegł on Rosję, że każda taka ingerencja będzie traktowana z najwyższą powagą, a naruszenie infrastruktury światłowodowej zostanie uznane za akt wojny równoznaczny z jej wypowiedzeniem. To bardzo poważne stwierdzenie. Tylko czy powstrzyma ono ewentualne zaplanowane działania rosyjskiej floty podwodnej?

NATO w gotowości

Niestety, od października 2020 r. znany jest raport ministerstw obrony

Zakłócenia w działaniu svalbardzkiego podmorskiego systemu kablowego (SUCS) miały już miejsce między 130 a 230 km od Svalbardu

FOT. WIKIMEDIA/J. STRZELECKI

państw sojuszniczych NATO, który wyciekł już do publicznej sieci internetowej. Podkreśla on strategiczne znaczenie infrastruktury dla działalności militarnej NATO oraz stwierdza, że nie ma dotychczas skutecznych sposobów ochrony podmorskich światłowodów. Rosja natomiast dysponuje dwoma podstawowymi środkami, które mogą być wykorzystane bezpośrednio do ataku na podmorskie światłowody. Są to okręty podwodne i specjalistyczne okręty nawodne. Szczególnie te ostatnie są bardzo niebezpieczne, gdyż dysponują autonomicznymi łodziami podwodnymi przystosowanymi do skomplikowanych prac podwodnych.

Jednym z takich okrętów, który jest uznawany za potencjalnie niebezpieczny, jest „Jantar". Oficjalnie nazywany jest okrętem badawczym i przewozi on dwie małe łodzie podwodne typu AS-37 „Russia" przeznaczone do specjalistycznych misji inżynieryjnych. Łodzie mogą zanurzyć się na głębokość prawie 6 kilometrów i wykonywać tam skomplikowane prace. Ten „okręt badawczy" na co dzień stacjonuje w tajnej rosyjskiej bazie morskiej Olenya Guba niedaleko Siewieromorska, siedziby rosyjskiej Floty Północnej w obwodzie murmańskim.

Olenya Guba to baza, w której stacjonują rosyjskie okręty specjalne. Należy do nich m.in. słynny szpiegowski atomowy okręt podwodny rosyjskiej marynarki wojennej AS-12 „Łoszarik", oficjalnie również nazywany okrętem badawczym, wyposażony w specjalne systemy przeznaczone do niszczenia instalacji na dużych głębokościach. Kiedy „Jantar" pierwszy raz w 2015 r. wypłynął w rejs, wywołał panikę amerykańskich służb wywiadowczych. Został wykryty w pobliżu amerykańskiej bazy Guantanamo na Kubie, dokładnie w miejscu, gdzie znajdowała się podwodna instalacja kabli światłowodowych łącząca strategiczną bazę z Florydą.

Później odnotowano jego aktywność u wybrzeży Syrii i w Zatoce Perskiej, zawsze w czasie największego napięcia na arenie międzynarodowej. We wrześniu 2021 r. jego obecność odnotowano w okolicach Irlandii, gdzie poruszał się równolegle do kabla podmorskiego Celtic Norse oraz AEConnect-1, który łączy Irlandię ze Stanami Zjednoczonymi (pełną mapę północno atlantyckich kabli światłowodowych można znaleźć na stronie: https://www.infrapedia.com).

„Jantar" jest częścią rosyjskiej struktury okrętów szpiegowskich w ramach wojskowego projektu głównego zarządu badań podwodnych. Wyposażony jest również w holowane systemy sonarowe przystosowane do dokładnego mapowania dna morskiego w poszukiwaniu kabli i innych elementów podwodnej infrastruktury informatycznej. Do zderzenia z podobnym sonarem używanym przez brytyjski okręt doszło w 2020 r. na północnym Atlantyku, kiedy uderzył on w niezidentyfikowany okręt podwodny, prawdopodobnie rosyjski, co potwierdziło niedawno brytyjskie ministerstwo obrony. Kolizja została zarejestrowana przez ekipę filmową dla brytyjskiej stacji telewizyjnej Channel 5 na potrzeby serii dokumentalnej „Warship: Life at Sea".

Powinniśmy zachować szczególną ostrożność w korzystaniu z nieznanych nam lub niepewnych stron internetowych, a także niezwykle krytycznie podchodzić do wszystkich informacji pojawiających się zarówno w mediach społecznościowych, jak i na portalach o wątpliwej wiarygodności

Eksperci ds. bezpieczeństwa na całym świecie wielokrotnie już ostrzegali przed możliwością podsłuchiwania podmorskich kabli w celach szpiegowskich. Zagrożenia mogą polegać również na wprowadzaniu specjalnych elementów w procesie produkcji kabli (backdoorów), atakowaniu stacji lądowych i urządzeń łączących kable z sieciami na lądzie lub podsłuchiwaniu kabli na morzu. A przecież producentami i właścicielami podwodnych kabli światłowodowych są firmy prywatne, nad którymi bezpośredni nadzór wojskowy dotyczący cyberbezpieczeństwa jest raczej niemożliwy.

Rosyjskie okręty specjalne

Wojska obrony cyberprzestrzeni są właściwie zupełnie bezradne wobec fizycznej ingerencji w funkcjonowanie infrastruktury światłowodowej. Natomiast Rosja posiada skuteczne „okręty specjalne", które służą właśnie do takich celów. Dostępne informacje na temat aktywności okrętu „Jantar" są niewątpliwie jedynie niewielką częścią dużo większej operacji rosyjskiej floty, która prowadzi bardzo aktywne działania dotyczące światowej infrastruktury światłowodowej. Jeśli uda im się przerwać większość połączeń między Europą a Stanami Zjednoczonymi, to będziemy mieli do czynienia z bardzo krytyczną sytuacją.

Big Tech posiada podstawową infrastrukturę właśnie na terytorium Stanów Zjednoczonych i zapewne funkcjonowanie globalnej sieci internetowej jest również silnie uzależnione od serwerowych centrów przetwarzania danych, które właśnie tam zbudowano. Zniszczenie połączeń transatlantyckich spowoduje potężne zakłócenia w działalności systemów internetowych w Europie. I nie chodzi tu tylko o problemy z usługami poczty internetowej, wyszukiwarek, serwisów społecznościowych, czy też sklepów internetowych, ale przede wszystkim z prawidłowym funkcjonowaniem europejskiej infrastruktury krytycznej. Tej militarnej w szczególności, a o niej z oczywistych powodów wiemy bardzo mało. Na ile jest ona uzależniona od amerykańskich serwerów? Czy amerykańska broń będąca na wyposażeniu europejskich armii będzie odporna na całkowite zerwanie transferu danych przebiegającego w światłowodach na dnie Atlantyku? A co z wojskami amerykańskimi stacjonującymi w Europie, czy pozostała łączność satelitarna wystarczy im do prowadzenia skutecznych działań wojskowych?

Uszkodzone połączenia

Niestety, obserwujemy pojawienie się kolejnych problemów. Brytyjski Total Telecom 12 stycznia podał informację zatytułowaną: „Sabotaż podmorski? Najbardziej wysunięty na północ kabel na świecie wyłączony przez nieznane zdarzenie". Opisuje w nim zakłócenia w działaniu svalbardzkiego podmorskiego systemu kablowego (SUCS), który miał miejsce między 130 a 230 km od Svalbardu.

W poniedziałek 10 stycznia firma Space Norway, operator najbardziej wysuniętego na północ kabla podmorskiego na świecie, poinformowała o uszkodzeniu kabla SUCS z nieznanej przyczyny. Space Norway twierdzi, że incydent jest szczegółowo badany, ale aby naprawić uszkodzoną część kabla, konieczny będzie specjalistyczny statek naprawczy. System SUCS łączy Svalbard Satellite Station (SvalSat), bardzo ważny, strategiczny system satelitarny znajdujący się na tej norweskiej wyspie, z norweskim brzegiem. SvalSat zawiera ponad 100 anten satelitarnych i jest kluczowym centrum pobierania danych z satelitów.

Poza tym tajemnicza awaria SUCS wywołała fale spekulacji ze strony europejskich mediów, które zwracają uwagę na geopolityczne znaczenie Svalbardu i lokalizacji SUCS, która obejmuje korytarz ważny dla rosyjskiej marynarki wojennej, między Morzem Barentsa a Atlantykiem. Rosja od dawna sugerowała, że SvalSat może być wykorzystywany przez Norwegię do pobierania danych również z satelitów wojskowych, co byłoby zgodnie z prawem nielegalne, ponieważ Svalbard należy do traktatowo wyznaczonej strefy zdemilitaryzowanej.

Rosja obawiała się również, że SUCS jest wykorzystywany do monitorowania aktywności okrętów podwodnych na tym obszarze. Na razie nie ma oficjalnego norweskiego stanowiska, ale możemy przypuszczać, że to kolejna rosyjska akcja, w której tym razem dokonano nie tylko rozpoznania, lecz także uszkodzenia.

A więc wojna o światłowody trwa, czy jest ona przygotowaniem do większej, konwencjonalnej operacji militarnej, czy tylko kolejnym elementem wojny informacyjnej prowadzonej coraz aktywniej przez Rosję, tego na razie nie wiemy. Ale tym bardziej powinniśmy zachować szczególną ostrożność w korzystaniu z nieznanych nam lub niepewnych stron internetowych, a także niezwykle krytycznie podchodzić do wszystkich informacji pojawiających się zarówno w mediach społecznościowych, jak i na portalach o wątpliwej wiarygodności. Korzystajmy ze sprawdzonych źródeł informacji, najlepiej rządowych, bo one odpowiednio zabezpieczone przez służby zapewniają nam dostęp do weryfikowalnych treści. A to właśnie te treści są jednym z najważniejszych elementów wojny informacyjnej.●

Dr Grzegorz Osiński