



NATO wobec potencjalnej rosyjskiej eskalacji hybrydowej

Filip Bryjka

Upublicznione informacje wywiadowcze państw NATO sugerują intensyfikację działań hybrydowych prowadzonych przez Rosję. Jej celem ma być przetestowanie reakcji i spójności Sojuszu, a także osłabienie pomocy dla Ukrainy w konsekwencji konieczności przeznaczenia zwiększonych zasobów na ochronę własnej infrastruktury krytycznej. W swoim planowaniu NATO uwzględnia różne scenariusze rosyjskiej eskalacji hybrydowej, która może nawet doprowadzić do uruchomienia art. 5 Traktatu północnoatlantyckiego. Państwa członkowskie różnią się poziomem gotowości do zwiększania kosztów, które Rosja będzie ponosić w wyniku potencjalnej eskalacji.

Przedstawiciele struktur wojskowych NATO podkreślają gotowość Sojuszu do reakcji na ewentualną [eskalację ze strony Rosji](#). Rosyjska strategia destabilizacji Zachodu w coraz większym stopniu wykorzystuje środki militarne, m.in. naruszenia przestrzeni powietrznej przez środki napadu powietrznego, cyberataki, zagłuszanie sygnału GPS/GNSS czy prowokacyjne manewry na morzu. Stanowi to poważne wyzwanie dla państw NATO, które są zmuszone do odpowiedzi w taki sposób, by utrzymać wiarygodność odstraszania, ale jednocześnie uniknąć niekontrolowanej eskalacji. Jednocześnie Rosja grozi – w przypadku odpowiedzi Sojuszu na jej prowokacje – rozszerzeniem działań wojennych na terytorium NATO i odwetem z wykorzystaniem wszystkich dostępnych środków [\(w tym broni nuklearnej\)](#). Wywierając w ten sposób presję psychologiczną na opinię publiczną i elity polityczne państw zachodnich, liczy na wstrzymanie pomocy dla Ukrainy, a także wznowienie selektywnej współpracy (np. w sferze gospodarczej).

Operacyjne podejście Sojuszu do zagrożeń hybrydowych. NATO definiuje zagrożenia hybrydowe jako połączenie środków wojskowych i cywilnych, a także tajnych i jawnych działań obejmujących dezinformację, cyberataki, presję gospodarczą, wykorzystywanie nieregularnych grup zbrojnych i sił regularnych. Aktywności te mogą być podejmowane w sposób skoordynowany na poziomie taktycznym i operacyjnym dla osiągnięcia celów strategicznych, a istotą ich użycia jest zacieranie granicy między wojną a pokojem. Działanie

w tzw. szarej strefie pozwala adwersarzom wykorzystywać systemowe podatności państw demokratycznych działających na podstawie procedur reagowania w czasie formalnego pokoju, co ogranicza spektrum możliwych odpowiedzi (zwłaszcza w zakresie użycia środków wojskowych). Operacje hybrydowe są przy tym prowadzone w sposób, który ma zapewnić atakującemu zdolność do tzw. wiarygodnego zaprzeczania, co utrudnia ocenę sytuacji, jednoznaczne przypisanie odpowiedzialności i wybór właściwej odpowiedzi.

Zgodnie z ustalonym w NATO konsensusem politycznym pierwszą linią obrony przed atakami hybrydowymi są narodowe siły i środki (służby wywiadowcze, policja, straż graniczna, wojsko itd.) państw, które stały się jego celem (zgodnie z art. 3). W czasie pokoju NATO zapewnia jednak wsparcie w zakresie świadomości sytuacyjnej – poprzez analizę zagrożeń i wymianę informacji wywiadowczych w ramach Joint Intelligence and Security Division (JISD), wsparcie zespołów NATO Counter-Hybrid Teams o charakterze doradczym i konsultacje polityczne (również z potencjalnym wykorzystaniem art. 4 Traktatu północnoatlantyckiego), co ma ułatwić decyzję o skoordynowanej kolektywnej odpowiedzi. Dla zapewnienia szybkiej i skutecznej reakcji w 2025 r. powołano specjalnego koordynatora ds. zagrożeń hybrydowych, który pełni rolę punktu kontaktowego wysokiego szczebla.

Zgodnie z informacjami funkcjonującymi w obiegu publicznym od 2016 r. w planowaniu operacyjnym NATO została

uwzględniona sytuacja, gdy działania hybrydowe prowadzone poniżej otwartego konfliktu zbrojnego osiągają poziom zbrojnej napaści, co może doprowadzić do uruchomienia art. 5 Traktatu północnoatlantyckiego mówiącego o kolektywnej obronie. Sojusz nie określa przy tym warunków, jakie musiałyby zostać spełnione, by taka decyzja – mająca zawsze charakter ściśle polityczny – została podjęta. Pozostawienie ich w sferze niejednoznaczności umożliwia każdorazową ocenę sytuacji (m.in. pod względem szkodliwości ataku) i dostosowanie odpowiedzi. Uwarunkowania te są jednak wykorzystywane przez Rosję do stopniowej eskalacji metodami hybrydowymi w celu zdiagnozowania, jak daleko może się posunąć bez ponoszenia przy tym znaczących kosztów.

Możliwe warianty odpowiedzi państw NATO. Szczegóły dotyczące kolektywnej reakcji Sojuszu na zbrojną napad z wykorzystaniem metod hybrydowych miały być uwzględnione w [trzech planach regionalnych](#) przyjętych w 2023 r. Podobnie jak zaktualizowana w 2025 r. strategia NATO wobec zagrożeń hybrydowych, mają one charakter niejawni. Jednocześnie narzędzia wojny hybrydowej (tajne operacje, dywersja, sabotaż, wtargnięcia, infiltracja, wrogie działania o zasięgu lokalnym czy ograniczona agresja zbrojna) uwzględniano w planowaniu operacyjnym i strategiach NATO już w czasach zimnej wojny (m.in. w strategii elastycznej odpowiedzi).

W najbliższych miesiącach NATO może się zmierzyć z rosyjską eskalacją hybrydową obejmującą m.in. intensyfikację [kampanii dywersyjno-sabotażowej](#) (jest to scenariusz o wysokim prawdopodobieństwie). Istnieje także rosnące ryzyko kolejnych ataków powietrznych z wykorzystaniem dronów, pocisków manewrujących, a nawet rakiet balistycznych, na terytorium lub w pobliżu państw Sojuszu. Mniej prawdopodobna jest ograniczona rosyjska operacja wojskowa, polegająca np. na wysłaniu nieoznakowanych grup zbrojnych w celu zajęcia części jednego z państw bałtyckich (np. obszarów zamieszkałych przez społeczność rosyjskojęzyczną) lub ataku „pod fałszywą flagą” z terytorium NATO na Rosję, co miałoby uzasadnić podjęcie przez nią działań militarnych.

W reakcji na wystąpienie jednego lub kombinacji powyższych scenariuszy państwa NATO – na poziomie narodowym lub sojuszniczym – mają do dyspozycji cały wachlarz odpowiedzi, by podnieść koszty działań Rosji, wpłynąć na jej kalkulacje i zniechęcić do dalszej eskalacji. W pierwszej kolejności członkowie Sojuszu powinni zwiększyć swoją odporność na rosyjską eskalację, m.in. poprzez ochronę obiektów infrastruktury krytycznej (zwłaszcza z sektora energetycznego i przemysłu zbrojeniowego) przed uderzeniami dronów i pocisków balistycznych. W tym celu na poziomie NATO może zostać podjęta decyzja o wzmocnieniu zdolności operacyjnych misji „Eastern Sentry” (powołanej we wrześniu 2025 r. w odpowiedzi na rosyjski atak dronów na Polskę) i rozmieszczeniu w Polsce, państwach bałtyckich i Rumunii dodatkowych systemów obrony przeciwlotniczej, antydronowych (w tym dronów przechwytyjących), rozpoznawczych, walki radioelektronicznej, a także śmigłowców i samolotów bojowych. Niezmiennie istotne jest też kontrolowanie narracji w domenie informacyjnej, w której Rosja

będzie wykorzystywała każdy incydent, nawet o relatywnie niewielkiej szkodliwości, do podsycania podziałów i polaryzacji społecznej. Istotne dylematy pojawiają się w Sojuszu w bardziej niebezpiecznym, ale też mniej prawdopodobnym scenariuszu przejścia Rosji do selektywnych uderzeń powietrznych, tłumaczonych np. [działaniem ukraińskich systemów WRE](#). Nawet jeśli w wyniku takich ataków nie będzie ofiar, część sojuszników może żądać symetrycznej odpowiedzi wobec Rosji, a część uznać to za zbyt ryzykowne.

Wobec perspektywy napięć w NATO, na których wywołanie obliczona jest rosyjska taktyka, sojusznicy powinni już teraz uzgodnić zestaw działań będących alternatywą dla symetrycznego odwetu. Pierwszym wyborem mogłoby być zapewnienie Ukrainie zasobów niezbędnych do zwiększenia skali i skuteczności jej [kampanii uderzeń dalekiego zasięgu na cele strategiczne w Rosji](#). Mogłoby to objąć transfery większej ilości i nowych rodzajów uzbrojenia a także dzielenie się danymi wywiadowczymi o potencjalnych celach. Państwa Sojuszu mogą też kontynuować i wzmacniać egzekwowanie dotychczasowych środków odpowiedzi o charakterze dyplomatycznym (np. wydalenia rosyjskich dyplomatów i zamykanie placówek dyplomatycznych), informacyjnym (komunikacja strategiczna wobec Rosji), wojskowym (misje „Baltic” i „Eastern Sentry”) i ekonomicznym (sankcje), a także rozszerzać je o działania ofensywne (w tym realizowane we współpracy z ukraińskim wywiadem i siłami specjalnymi). Warte rozważenia byłyby np. cyberoperacje ukierunkowane na manipulowanie rosyjską domeną informacyjną czy też na zakłócanie funkcjonowania rosyjskiej infrastruktury krytycznej. Ich niekinetyczny charakter obniży ryzyko dalszej eskalacji militarnej.

Wnioski. Z perspektywy państw wschodniej flanki NATO – najbardziej narażonych na agresywne działania Rosji – kluczowym elementem odstraszenia jest kolektywny wymiar odpowiedzi na rosyjskie operacje hybrydowe, co nie tylko pozwoli dzielić ryzyko związane z potencjalnym odwetem, ale także zwiększy psychologiczny efekt oddziaływania na rosyjskich decydentów politycznych i wojskowych. By osiągnąć ten cel, niezbędne jest podejmowanie wobec Rosji ofensywnych odpowiedzi podnoszących koszty jej eskalacji, przy zachowaniu ich niekinetycznego charakteru ze względu na wagę jedności sojuszniczej. W NATO nie ma jednak politycznego konsensusu nawet w tej kwestii, co osłabia sojuszniczą zdolność do odstraszenia ataków hybrydowych. Rosyjska strategia destabilizacji wykorzystuje przy tym słabe punkty systemów bezpieczeństwa państw NATO, absorbuje ich zasoby i podwyższa koszty ochrony. Testuje reakcje na poziomie narodowym i sojuszniczym oraz bada „czerwone linie”, których przekroczenie spotka się ze zdecydowaną odpowiedzią. Ze względu na wzrost częstotliwości używania przez Rosję środków wojskowych państwa NATO powinny więc pilnie dostosować swoje procedury reagowania do neutralizacji tych zagrożeń na zasadach podobnych do czasu wojny (np. w kwestii zestrzeliwania środków napadu powietrznego) mimo formalnego pokoju. To z kolei pozwoliłoby na wzmocnienie odporności państw i zwiększenie potencjału odstraszenia poprzez odmowę.