aut. Andrzej Kozłowski 04.12.2020

PRZYSZŁOŚĆ NATO POD ZNAKIEM NOWOCZESNYCH TECHNOLOGII

Zmiana komunikacji strategicznej oraz znaczne inwestycje w walkę z zagrożeniami hybrydowymi i cyberatakami to rekomendacje ekspertów, którzy z polecenia sekretarza generalnego NATO sporządzili raport o przyszłości Sojuszu.

NATO opublikowało raport „NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General", w którym przedstawiono rekomendacje dotyczące przyszłości Sojuszu. Dokument został sporządzony na polecenie sekretarza generalnego Jensa Stoltenberga i stanowi on odpowiedź na komentarz prezydenta Francji Emmanuela Macrona o „śmierci mózgu" NATO. W dużej mierze skupia się na wyzwaniach ze strony Rosji i Chin, zmianach w podejmowaniu decyzji przez Sojusz, ale nie zapomniano również o kwestiach cyberbezpieczeństwa i dezinformacji.

Czytaj też: Amerykanie „odbijają" Europę Chinom. Polska między „młotem a kowadłem" [WYWIAD]

Dokument wyróżnia w oddzielnych podrozdziałach zagadnienia związane z działaniami hybrydowymi i cyberatakami oraz kwestie związane z komunikacją strategiczną oraz przeciwdziałaniem dezinformacji.

Cyberbezpieczeństwo i zagrożenia hybrydowe

Autorzy dokumentu twierdzą, że cyberataki oraz działania hybrydowe są podejmowane przez wrogich Sojuszowi aktorów państwowych i niepaństwowych. Podkreślają, ze trudno jest wykryć kto je przeprowadził, ponieważ często używa się różnorodnych grup pośredniczących, niezwiązanych bezpośrednio z rządami państw zainteresowanych osłabieniem NATO. Głównym celem takich działań jest podważenie międzynarodowego porządku, osłabienie Sojuszu oraz państw demokratycznych. Autorzy podkreślają również, że te metody często są wykorzystywane przeciwko najsłabszym członkom NATO oraz tym, którzy ze względu na swoją sytuację są szczególnie podatni na takie operacje.

Od 2016 roku Sojusz podjął wiele cennych inicjatyw, które były ukierunkowane na zwiększenie ochrony przed cyberatakami i zagrożeniami hybrydowymi. Na szczycie w Warszawie uznano cyberprzestrzeń jako przestrzeń prowadzenia działań wojennych na równi z lądem, morzem i przestrzenią powietrzną. Wprowadzono również inicjatywę Cyber Defence Pledge, aby zwiększyć przygotowanie państw do obrony przed zagrożeniami w cyberprzestrzeni.

Czytaj też: Wielka Brytania z jednostką do zadań cyberofensywnych. „Przełom w dziedzinie

obronności”

W 2018 roku stworzono zespoły Country Hybrid Support, aby zapewnić wsparcie państwom członkowskim w walce z zagrożeniami hybrydowymi. Rok później zatwierdzono raport na temat wzmacniania odpowiedzi NATO na zagrożenia hybrydowe. Eksperci postulują dalsze zmiany i sugerują stworzenie wspólnych ram politycznych, w których zostanie zdefiniowana kwestia jak Sojusz ocenia, przypisuje odpowiedzialność i reaguje na incydenty hybrydowe oraz „cyberincydenty" w czasie kryzysu. Takie rozwiązanie przyniosłoby większą przejrzystość oraz pozwoliłoby na jaśniejsze zdefiniowanie odpowiedzialności i zadań dla NATO, Unii Europejskiej oraz państw członkowskich. Autorzy raportu zauważają, że ciągnące się w nieskończoność polityczne dyskusje na temat atrybucji danego ataku i tego jak NATO powinno reagować utrudniały skuteczną reakcję na zagrożenia we właściwym czasie oraz zwiększały ryzyko pomyłki i niezamierzonej eskalacji.

Eksperci radzą również, że NATO powinno określić poziom swoich ambicje w walce z zagrożeniami hybrydowymi oraz zintegrować dyskusję na ten temat włączając w pracę komórki odpowiedzialne m.in. za dyplomację publiczną w Sojuszu, co pozwoli przezwyciężyć obecną fragmentacją zadań i obowiązków wśród wielu różnych komórek organizacji. Rekomenduje się także wzmocnienie potencjału NATO do pomocy swoim członkom w obronie przez cyberatkami i atakami hybrydowymi. Sugeruje się tutaj częstsze wykorzystanie Artykułu 4 jako platformy dialogu w sprawie ustalenia atrybucji danego ataku co pozwoli zademonstrować jedność Sojuszu.

> *Strony będą się konsultowały, ilekroć zdaniem którejkolwiek z nich zagrożona będzie integralność terytorialna, niezależność polityczna lub bezpieczeństwo którejkolwiek ze Stron*
>
> *Artykuł 4 Traktatu Waszyngtońskiego*

Eksperci sugerują również podniesienie świadomości w obszarze zagrożeń hybrydowych oraz kampanii przeprowadzonych z wykorzystaniem takich środków. Rekomenduje się stworzenie jednolitej terminologii oraz poprawienie świadomości sytuacji poprzez lepsze monitorowanie, wykrywanie i analizowanie zagrożeń hybrydowych na poziomie operacyjnym i strategicznym. Można w tym celu wykorzystać metody prognozowania, analizy trendów, najlepsze praktyki, gry i symulacje oraz włączyć zagadnienia związane z konfliktami hybrydowymi w trening i ćwiczenia.

Ponadto autorzy raportu przewidują, że NATO powinno wesprzeć członkowi w stworzeniu kompleksowego programu odpowiedzi na zagrożenia hybrydowe zarówno na poziomie strategicznym jak i taktyczno-operacyjnym. Podkreśla się także potrzebę współpracy wojskowo-cywilnej w tym obszarze, jak również konieczność wzmacniania odporności społeczeństw państw członkowskich. Powinno się to odbywać poprzez różne mechanizmy odpowiedzi na dezinformację wymierzoną w NATO i indywidualnych członków (zasada dziel i rządź). W środowisku hybrydowym, komunikacja strategiczna nie powinna być uruchamiana w związku z kryzysem, ale być prowadzona w sposób ciągły i jest to kluczowe, jeżeli chodzi o wiarygodność odstraszania NATO. Konieczne będzie znalezienie odpowiednich środków odpowiedzi na zastraszanie ze strony innych państw, które jednak powinny nie eskalować napięć. Eksperci rekomendują, żeby było ono koordynowane w wielu domenach jednocześnie.

Sojusz powinien rozważyć i rozwinąć dyplomatyczne środki deeskalacji napięć związanych z

zagrożeniem hybrydowym, takie jak wizyty międzynarodowe, konferencje prasowe czy konsultacje w ramach Artykułu 4 oraz rozwinąć toolbox oferujący różnorodne narzędzia do neutralizacji takiego rodzaju zagrożeń.

Czytaj też: Gen. Molenda: „Tak jak inne wojska, tak i cyberżołnierze muszą mieć swój poligon”

Według rekomendacji ekspertów NATO i państwa muszą rozwinąć zdolności operowania w przestrzeni wirtualnej oraz kognitywnej na poziomie taktycznym. Będą one niezbędne do wykrywania dezinformacji oraz mitygowania jej negatywnych skutków. Wymaga to lepszego poznania potrzeb społecznych, zrozumienia sieci społecznościowych, a także metod przekazywania informacji online oraz powiązanych narracji. NATO i sojusznicy muszą również stworzyć prawne i etyczne ramy działania w tych przestrzeniach. Rekomenduje się również przeprowadzanie cyklicznych ćwiczeń walki z zagrożeniami hybrydowymi, które oparte są na realistycznych scenariuszach. Muszą one mieć charakter interdyscyplinarny i uwzględniać podmioty z obszaru DIMEFIL (diplomatic, informatiom, military, economic, financial, intelligence i law enforcement). Trening oraz ćwiczenia muszą odbyć się na poziomie taktyczno-operacyjnym jaki i poziomie polityczno-strategicznym. Eksperci podsumowują, że konieczne jest zwiększenie zdolności w obszarze przeciwdziałania zagrożeniom hybrydowym poprzez przeznaczenie większych ilości pieniędzy, zatrudnienie dodatkowych osób oraz wdrożenie odpowiednich politycznych i prawnych ram pozwalających na sprostanie tym wyzwaniom.

Komunikacja strategiczna, dyplomacja publiczna i walka z dezinformacją

Komunikacja strategiczna jest niezwykle istotna jeżeli chodzi o odstraszanie i obronę, w zwłaszcza dzisiaj, kiedy informacja jest jednym z obszarów rywalizacji - wskazują eksperci. Środowisko informacyjne jest pełne dezinformacji, fake newsów oraz oszustw pochodzących od wielu aktorów, co jest szczególnie groźne w dobie dynamicznego postępu technologicznego. Celem takich działań jest podważenie zaufania do instytucji demokratycznych oraz zmiana postrzegania NATO wśród społeczeństw państw członkowskich. Eksperci zauważają, że przeciwnicy Sojuszu demonstrują rosnące zdolności oraz przejawią coraz większe chęci do wykorzystywania nowoczesnych rozwiązań technologicznych przeciwko NATO i ich sojusznikom w sferze informacyjnej.

Czytaj też: Russia is simply the best! Narracje Kremla pod lupą NATO StratCom

Priorytetem dla Sojuszu powinno być zwiększenie odporności społeczeństw na takie działania. Niestety państwa nie inwestują dostatecznie dużych środków w ten obszar bezpieczeństwa. Żadne z nich nie traktuje odpowiednio priorytetowo proaktywnej i spójnej komunikacji wspierającej cele Sojuszu. Eksperci podkreślają, że zagrożenie jest stwarzane zarówno przez aktorów państwowych jak i niepaństwowych, którzy używają agresywnej taktyki poniżej progu użycia konwencjonalnych sił. Dlatego NATO musi być świadome tych działań oraz reagować na nie, dostarczając precyzyjnych, opartych na faktach informacji. Eksperci, którzy przygotowali raport dla sekretarza stanu radzą, aby NATO przyspieszyło transformację swoich zasobów komunikacji strategicznej, co umożliwi skuteczną rywalizację w środowisku informacyjnym. Musi się to wiązać z inwestycjami w budżet, osoby, technologie oraz wdrożeniem podejścia ukierunkowanego na osiągnięcie konkretnego celu i odpowiednich mechanizmów ewaluacji działań. Kluczowym elementem będzie utrzymanie przez NATO pozytywnego wizerunku oraz podkreślanie spójności i jedności, co pozwoli na zwiększanie rozpoznawalności Sojuszu oraz wsparcia.

Eksperci podkreślają również konieczność nadania priorytetu cyfrowym elementom w proponowanych reformach komunikacji strategicznej, co pozwoli na lepsze wykorzystanie danych i pogłębienie

zrozumienia złożonego środowiska. Umożliwi także bardziej efektowne zaangażowanie się w dialog z tą częścią społeczeństwa, która ma priorytetowe znaczenie dla Sojuszu. NATO nie może jednak się skupić tylko i wyłącznie na komunikacji w świecie cyfrowym, równie ważne jest bezpośrednie dotarcie do społeczeństwa poprzez takie inicjatywy jak Zgromadzenie Parlamentarne NATO czy Atlantic Treaty Association oraz bardziej proaktywne podeście do tłumaczenia i wyjaśniania polityk, operacji, a także działań podejmowanych przez Sojusz.

Czytaj też: NATO na wojnie z „pandemią fake newsów". Jak walczyć, by wygrać?

Eksperci rekomendują też większą dyscyplinę w publikowaniu deklaracji ze szczytu i spotkań. Powinny one też być krótsze tak, aby miały praktyczne znaczenie oraz stanowiły istotne narzędzie przekazywania informacji. Od 2011 rozrosły się jeżeli chodzi o swoją wielkość i straciły praktyczne znaczenie komunikacyjne, co według ekspertów należy to zmienić tak, aby lepiej wyjaśniać społeczeństwom cele Sojuszu i podejmowane przez niego działania. Eksperci rekomendują, żeby NATO wróciło do praktyki krótkich i zwięzłych komunikatów ministrów, co pozwoli szerszej publiczności, a nie tylko ekspertom, lepiej zrozumieć podejmowane działania.

Autorzy raportu zauważają również rosnące znaczenie nowoczesnych technologii, które z jednej strony mogą stanowić wyzwanie i zagrożenie dla NATO, ale również szansę dla Sojuszu, który powinien odgrywać rolę instytucji koordynującej i odpowiedzialnej za dzielenie się informacjami. Eksperci rekomendują zwołanie szczytu cyfrowego pomiędzy rządami i sektorem prywatnym w celu zidentyfikowania problemów dla obrony kolektywnej, które mogą powstać ze względu na rozwój sztucznej inteligencji i jej zastosowanie do działania wymierzonych w NATO.

Czytaj też: Czy grozi nam cyfrowe Pearl Harbour? [OPINIA]

Raport rekomenduje też utworzenie centrów analitycznych prowadzących badania nad nowymi technologiami oraz zastosowanie sztucznej inteligencji tak, aby Sojusz zwiększył swój potencjał i ochronę przed cyberatakami oraz lepiej przygotował się na wyzwania konfliktów hybrydowych.

Większość propozycji ekspertów zawarta w raporcie jest sformułowana ogólnikowo, co jest charakterystyczne dla tego typu dokumentów. Wyodrębnienie i podkreślenie obszarów takich jak cyberbezpieczeństwo, dezinformacja oraz kwestii związanych z nowoczesnymi technologiami pokazuje, jak istotne znaczenie będą one miały w przyszłości. Z pewnością część rekomendacji jest godna uwagi. Chociażby jak stałe prowadzenie komunikacji strategicznej tak, aby promować własną narrację, jak również wspieranie brandu NATO i skuteczniejsze wyjaśnianie celów oraz działań Sojuszu. Istotne jest też podkreślenie znaczenie artykułu 4 i rozszerzenie jego zastosowania w celu przeciwdziałania zagrożeniom hybrydowym. Raport przygotowany przez ekspertów jest oczywiście zbiorem rekomendacji i potrzeba teraz działań politycznych, aby je wdrożyć w życie.