PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 183 (2602), 25 LISTOPADA 2022 © PISM

BIULETYN

Działania hybrydowe Rosji przeciw państwom NATO i UE

Anna Maria Dyner

Dążąc do osiągnięcia celów na Ukrainie, Rosja będzie nasilała działania hybrydowe, w tym wojnę informacyjną, cyberataki lub akty sabotażu wymierzone w infrastrukturę krytyczną państw NATO i UE. Działania te mają spotęgować obawy europejskiej opinii publicznej przed niekontrolowaną eskalacją konfliktu i dalszym pogarszaniem sytuacji gospodarczej. W ten sposób Rosja chce osłabić jedność sojuszniczą, która jest niezbędna do dalszego wspierania Ukrainy, wdrażania nowych strategii Sojuszu i Unii oraz szybkiego reagowania na pojawiające się zagrożenia. Rośnie znaczenie budowania odporności państwowej i społecznej na poziomie poszczególnych państw i obu organizacji.

Rosja od lat rozwija koncepcję prowadzenia działań hybrydowych przeciw państwom zachodnim. Polega ona na używaniu całego spektrum instrumentów politycznych, ekonomicznych i społecznych w celu m.in. manipulowania poglądami ludności w państwach uznawanych za wrogie. Do najważniejszych obszarów rosyjskiej aktywności należą wojna informacyjna, cyberataki oraz instrumentalizacja migracji.

Wojna informacyjna. W przypadku rosyjskich działań dezinformacyjnych przeciw państwom UE i NATO szczególną rolę odgrywają media społecznościowe. Propagowanie rosyjskiego przekazu odbywa się za sprawą istniejących od lat kont i grup, w tym fałszywych, niejednokrotnie takich, które wcześniej głosiły hasła antysystemowe. Aktywność zwiększają też firmy zatrudniające pracowników do rozsiewania w sieci konkretnego rodzaju informacji, tzw. farmy trolli. Rosyjskie działania koncentrują się na kwestiach najbardziej wrażliwych społecznie i politycznie, a przekaz kształtowany jest w sposób mający wpływać na nastroje społeczne. Obecnie tematami są rosnąca inflacja oraz bezpieczeństwo energetyczne. W pierwszym przypadku uwypuklany jest fakt udzielania Ukrainie pomocy wojskowej przez państwa UE i NATO oraz zwiększanie wydatków obronnych przez część członków Sojuszu. Wskazuje się, że jest to jeden z czynników odpowiedzialnych za rosnące ceny. W drugim obszarze Rosja przekonuje, że przez lata była gwarantem niskich cen energii, a za ich obecny wzrost odpowiadają państwa UE, które wycofały się z dotychczasowej współpracy.

Rosja próbuje też wykorzystywać obecność uchodźców z Ukrainy na Zachodzie, wskazując, że rządy państw przyjmujących skupiają się na pomocy Ukraińcom kosztem własnych obywateli i ich zabezpieczenia zdrowotnego i edukacyjnego.

Celem Rosji jest zmniejszanie poczucia bezpieczeństwa mieszkańców państw zachodnich (np. co do dostaw paliw i energii), podważanie ich zaufania do władz krajowych, UE oraz NATO, a także zwiększanie polaryzacji społecznej – np. w sprawach związanych z ochroną zdrowia.

Zagrożenia dla infrastruktury krytycznej. Chociaż wojna na Ukrainie angażuje zasoby Rosji, wciąż dysponuje ona znacznym potencjałem do prowadzenia działań sabotażowanych i ataków w cyberprzestrzeni. Są one wymierzone w funkcjonowanie infrastruktury krytycznej (elektrownie, sieci przesyłowe, koleje) państw NATO i UE. Rosja finansuje też grupy hakerskie w państwach trzecich, np. UNC1151/Ghostwriter czy Digital Shadows/Conti. Z raportu Agencji UE ds. Cyberbezpieczeństwa (ENISA) wynika, że od wybuchu obecnej fazy wojny na Ukrainie wzrosło zagrożenie dla rządów, przedsiębiorstw i kluczowych sektorów, takich jak energetyka, transport, bankowość i infrastruktura cyfrowa. Raport Microsoft stwierdza z kolei, że w okresie luty–maj br. Rosja przeprowadziła cyberataki w 42 państwach (poza Ukrainą), których głównym celem były agencje rządowe (49%) oraz instytucje zarządzające

infrastrukturą krytyczną (19%). Najczęściej atakowana była Polska (8% przypadków) i państwa bałtyckie (w sumie 14%).

Mimo że państwa Sojuszu prowadzą nasilone działania mające na celu zwiększenie fizycznej ochrony infrastruktury krytycznej, Rosja nadal ma potencjał do prowadzenia sabotażu. Mogą na to wskazywać eksplozje rurociągów Nord Stream 1 i 2. W tym celu, podobnie jak w cyberprzestrzeni, Rosja może posługiwać się obywatelami państw trzecich.

Instrumentalizacja migracji. Interesom UE i NATO zagrażają też rosyjskie działania prowadzone w Afryce, Bliskim Wschodzie i Ameryce Łacińskiej. Rosja szerzy tam propagandę na temat odpowiedzialności Zachodu za lokalne problemy gospodarcze. W tym celu, obok mediów społecznościowych, wykorzystuje rozwijane przez siebie media tradycyjne, w tym telewizję RT i portal Sputnik. Działania te, których nasilenie obserwowane jest od ubiegłego roku, są elementami procesu instrumentalizacji migracji i próbą wywołania dodatkowych ruchów ludności w kierunku Europy. Wskazują na to m.in. statystyki Straży Granicznej pokazujące, że osoby próbujące nielegalnie przekroczyć granicę białorusko-polską posiadają rosyjskie wizy.

Rosyjskie władze umożliwiły też lądowanie samolotów m.in. z Turcji, Syrii i Białorusi w obwodzie kaliningradzkim, co wskazywało na możliwość podjęcia próby destabilizacji granicy z Polską i Litwą.

Groźba nasilenia rosyjskich działań. Rosja zaangażowana w wojnę na Ukrainie będzie się starała osiągać cele polityczne w relacjach z UE i NATO relatywnie niskim kosztem, głównie poprzez działania hybrydowe. Szczególnie narażone będą państwa najbardziej wspierające Ukrainę, kluczowe dla podejmowania decyzji w obu organizacjach, oraz te, gdzie w najbliższych miesiącach odbędą się wybory prezydenckie bądź parlamentarne (w 2023 r. m.in. w Czechach, Estonii, Finlandii i Polsce). Rosja skupi się na prowadzeniu i intensyfikowaniu wojny informacyjnej wymierzonej w proces podejmowania decyzji o dozbrajaniu Ukrainy. Będzie też próbowała podważać spójność NATO, niezbędną do wdrażania nowej strategii Sojuszu, która zakłada wzmocnienie mechanizmów kolektywnej obrony.

Możliwe jest nasilenie cyberataków oraz aktów sabotażu i terrorystycznych wymierzonych w infrastrukturę krytyczną oraz teleinformatyczną, które będą miały na celu sparaliżowanie usług kluczowych w zaatakowanym państwie. Tego rodzaju działania będą miały m.in. zwiększać poczucie zagrożenia wojennego i testować zdolności obronne państw UE i NATO.

Rosja będzie nadal instrumentalizowała ruchy migracyjne oraz podsycała nastroje antyimigranckie i antyuchodźcze. Jej celem będzie wywieranie presji na państwa europejskie, testowanie systemu ochrony granic zewnętrznych UE i NATO oraz wywołanie poważnych sporów politycznych i w kwestii polityki migracyjnej wewnątrz państw członkowskich.

Wnioski i rekomendacje. Państwa NATO i UE muszą się liczyć z nasileniem działań hybrydowych, które w zamierzeniu Rosji mają osłabić ich poparcie dla Ukrainy. Obie organizacje powinny rozpocząć szerokie kampanie informacyjne skierowane do społeczeństw państw członkowskich, budujące odporność na dezinformację i kształtujące społeczne kompetencje w zakresie weryfikowania źródeł informacji. W ramach takich działań warto wskazać mechanizmy najbardziej popularnych rozwiązań stosowanych w rosyjskiej wojnie informacyjnej, np. tworzenie łańcucha pozornie wiarygodnych informacji, które mogą doprowadzić do niekorzystnych zjawisk społecznych (np. do paniki w efekcie informacji o sfabrykowanym zagrożeniu).

Jednym ze szczególnie niebezpiecznych scenariuszy działań hybrydowych Rosji będzie wywołanie kolejnej fali migracji skierowanej do Europy. Wynika stąd konieczność podjęcia przez UE we współpracy z innymi państwami działań pomocowych dla państw szczególnie dotkniętych kryzysem żywnościowym (również w ramach ONZ, co utrudni Rosji wykorzystywanie tej organizacji). Niezbędne będzie też zwiększenie współpracy wywiadowczej i kontrwywiadowczej między państwami UE i NATO w celu rozpoznawania zagrożeń związanych z nielegalną migracją. Konieczne będzie również poszerzenie kooperacji między służbami granicznymi państw UE w celu zwiększenia ochrony granicy zewnętrznej.

Istotne będzie też rozwijanie kompetencji społecznych i instytucjonalnych w zakresie reagowania na cyberzagrożenia, zwłaszcza związane z funkcjonowaniem infrastruktury krytycznej. Warto też rozważyć wprowadzenie i przetestowanie modeli zarządzania taką infrastrukturą bez dostępu do internetu. Podczas poważnej awarii spowodowanej np. przez cyberatak czy akt sabotażu będzie wówczas możliwe utrzymanie dostępu do kluczowych usług.

Polska może również rozważyć wprowadzenie zmian legislacyjnych ułatwiających walkę z zagrożeniami hybrydowymi. Rosyjskie ataki cybernetyczne lub fizyczne ułatwia fakt, że obrona państw UE i NATO polega jedynie na działaniach reaktywnych. Jednym z elementów naprawczych może być zatem zwiększenie uprawnień instytucji odpowiedzialnych za bezpieczeństwo państwa, które w określonych sytuacjach – wskazujących na bardzo duże zagrożenie atakiem hybrydowym – mogłyby podjąć działania prewencyjne.