PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 79 (2700), 22 CZERWCA 2023 © PISM

BIULETYN

Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO

Filip Bryjka, Tomasz Zając

Nowe unijne regulacje dotyczące infrastruktury krytycznej mogą wzmocnić odporność państw UE na zagrożenia hybrydowe ze strony Rosji i Chin. Głównym wyzwaniem będzie jednak wypracowanie i implementacja wspólnych z NATO precyzyjnych standardów ochrony takiej infrastruktury. Konieczna będzie wymiana doświadczeń w tym zakresie między państwami oraz na linii państwo – sektor prywatny. Może to wywołać opór tych członków UE, którzy są niechętni do dzielenia się wrażliwymi informacjami.

Inwazja Rosji na Ukrainę zwiększyła ryzyko rosyjskich działań hybrydowych, w tym cyberataków, aktów dywersji i sabotażu wymierzonych w infrastrukturę krytyczną (IK) państw UE i NATO. Eksplozja gazociągów Nord Stream 1 i 2 ukazała podatność na takie zagrożenia infrastruktury położonej na dnie morza. Od początku 2023 r. służby wywiadowcze Norwegii, Danii i Holandii informują o wzmożonej aktywności Rosji ukierunkowanej na rozpoznanie portów morskich, rurociągów, kabli światłowodowych, platform wiertniczych i farm wiatrowych. Rosja prowadzi te działania za pomocą okrętów wojennych (w tym podwodnych), bezzałogowych platform latających i pływających, statków badawczych, a także sił specjalnych. Wzmożona aktywność wywiadowcza Rosji może świadczyć o przygotowaniach do ataków sabotażowych, których celem może być np. zakłócenie transportu surowców energetycznych lub transmisji danych, a w konsekwencji osłabienie gospodarki państw UE i NATO i wpływ na ich stanowisko w sprawie wspierania Ukrainy. Pośrednie zagrożenie dla IK stanowią także chińskie inwestycje w sektorze teleinformatycznym (sieć 5G) czy przejmowanie przez Chiny portów i terminali morskich. Istnieje ryzyko wykorzystania takiej infrastruktury do prowadzenia masowej inwigilacji cyfrowej lub blokowania łańcuchów dostaw.

Zmiany w podejściu UE do ochrony IK. Chociaż zarządzanie IK należy głównie do kompetencji państw członkowskich, także na poziomie unijnym istnieje szereg norm mających na celu jej ochronę. Są one zawarte m.in w dyrektywie dotyczącej IK z 2008 r., strategii UE w zakresie bezpieczeństwa morskiego z 2014 r. czy w rozporządzeniu ustanawiającym ramy monitorowania bezpośrednich inwestycji zagranicznych z 2019 r. Dodatkowe zasady wprowadzono po rosyjskiej agresji na Ukrainę, np. dziesiąty pakiet sankcji nałożonych na Rosję zakazuje obywatelom tego państwa zasiadania w organach zarządzających przedsiębiorstwami związanymi z IK.

Komisja Europejska (KE) postanowiła zastąpić kluczową w zakresie ochrony IK dyrektywę z 2008 r. nowym aktem prawnym, lepiej odpowiadającym na aktualne wyzwania bezpieczeństwa. Państwa członkowskie będą musiały go wdrożyć do swoich porządków prawnych do października 2024. Jego przepisy będą obejmować 11 sektorów (w tym infrastrukturę cyfrową oraz bankową), co jest znacznym rozszerzeniem w porównaniu z dyrektywą z 2008 r., gdzie wymieniono jedynie dwa takie obszary (energię i transport). Zmieniło się również podejście do samej koncepcji ochrony IK. Wcześniejsza dyrektywa kładła nacisk na prewencję – najważniejszym jej celem było nie dopuścić do wystąpienia niepożądanego zdarzenia dotyczącego IK, takiego jak np. atak terrorystyczny. Chociaż w aktualnym akcie prawnym nadal spory nacisk położony jest na ochronę infrastruktury przed niepożądanymi incydentami, to – ponieważ trudno jest im zapobiec – równie istotne jest przygotowanie się na ich wystąpienie oraz proces naprawy ich skutków (np. wcześniejsze zaplanowanie alternatywnych łańcuchów dostaw). Dyrektywa przewiduje także możliwość wymiany

najlepszych praktyk między państwami członkowskimi, co ma ułatwiać specjalnie utworzona Grupa ds. Odporności Podmiotów Krytycznych, w której zasiadać będą przedstawiciele państw UE oraz KE.

Innym sygnałem większego zaangażowania Unii w ochronę IK jest propozycja KE z marca br., aby znowelizować strategię w zakresie bezpieczeństwa morskiego. W ramach unijnej skoordynowanej obecności morskiej monitorowane będą teraz dodatkowe obszary, co ma zapobiegać takim wydarzeniom, jak eksplozja gazociągów NS 1 i 2.

Współpraca UE–NATO. Nowa unijna dyrektywa dotycząca IK wpisuje się w proces realizacji założeń zawartych w przyjętym w marcu 2022 r. Kompasie Strategicznym, w którym określono cele polityki bezpieczeństwa i obrony UE. W dokumencie tym podkreślono przede wszystkim potrzebę wzmocnienia ochrony IK przed cyberatakami, zabezpieczenia szlaków komunikacyjnych i łańcuchów dostaw. Cele te Unia zamierza osiągnąć we współpracy z NATO. W styczniu br. organizacje podpisały trzecią deklarację o współpracy i powołały wspólną grupę zadaniową ds. odporności infrastruktury krytycznej. Ma ona służyć wymianie informacji i dobrych praktyk w zakresie ochrony IK, a także opracowywać wytyczne w sprawie wzmocnienia odporności IK w czterech sektorach: energetyce, transporcie, infrastrukturze cyfrowej i przestrzeni kosmicznej.

Współpraca UE i NATO w zakresie ochrony IK ma kluczowe znaczenie m.in. z uwagi na członkostwo tylko w jednej z tych organizacji takich państw, jak Wielka Brytania, Norwegia czy oczekująca na akcesję do Paktu Szwecja. Na wodach terytorialnych tych państw znajdują się elementy podmorskiej infrastruktury krytycznej, które są kluczowe dla bezpieczeństwa transatlantyckiego. Sojusznicy zobowiązali się do ochrony IK w ramach wzmacniania tzw. odporności (*resilience*). Sojusz ma istotne doświadczenie instytucjonalne w tym obszarze, sięgające lat 50. XX w., gdy w NATO utworzono Cywilny Komitet Planowania Kryzysowego. W 2022 r. został on przekształcony w Komitet Odporności, który podlega bezpośrednio Radzie Północnoatlantyckiej oraz wyznacza główne kierunki strategii i polityki państw członkowskich w obszarze wzmacniania odporności. Komitetowi podlega sześć wyspecjalizowanych grup planistycznych i Euroatlantyckie Centrum Koordynacji Reagowania na Katastrofy (EADRCC), które jest odpowiedzialne za wsparcie państw członkowskich i partnerów w sytuacjach kryzysowych spowodowanych katastrofami naturalnymi. W 2023 r. w strukturach Sojuszu utworzono także specjalną komórkę ds. podmorskiej infrastruktury krytycznej. Jest ona platformą wymiany doświadczeń i praktyk między państwami członkowskimi, instytucjami cywilnymi i wojskowymi oraz sektorem prywatnym (zwłaszcza w zakresie wykorzystania innowacyjnych technologii do ochrony IK). Za ochronę podwodnej IK w wymiarze operacyjnym będzie odpowiadać Morskie Centrum Ochrony Podwodnej Infrastruktury Krytycznej utworzone przy Sojuszniczym Dowództwie Morskim w Northwood. W odpowiedzi na rosnącą aktywność wywiadowczą Rosji na morzu NATO zwiększyło liczbę okrętów wojennych i samolotów patrolujących obszary wokół kluczowych elementów morskiej IK.

Wnioski i perspektywy. Decyzja UE o stopniowym uniezależnianiu się od rosyjskich surowców i wzmożona aktywność wywiadowcza Rosji znacznie zwiększają ryzyko rosyjskich ataków sabotażowych na IK. Potencjalnym celem mogą być transporty gazu z Norwegii, która stała się największym dostawcą tego surowca dla państw Unii. Dywersyfikacja źródeł pozyskiwania przez Polskę energii w znacznym stopniu opiera się na dostawach drogą morską, dlatego potencjalnym celem rosyjskich ataków hybrydowych może być infrastruktura na Bałtyku. Rosja może być skłonna do tego rodzaju działań, by wywrzeć negatywny wpływ na sytuację gospodarczą państw UE i NATO, a w ten sposób zniechęcić ich społeczeństwa do wspierania Ukrainy.

Nasilenie zagrożeń dla IK i ich ponadnarodowy charakter wymagają wzmocnienia regulacji na poziomie unijnym i koordynacji działań między NATO i UE. Dotychczasowe decyzje słusznie zmieniają całościowe podejście Unii do IK, przesuwając punkt ciężkości z jej ochrony (*protection*) na odporność (*resilience*). Oznacza to, że w swoich działaniach państwa nie tylko starają się nie dopuścić do uszkodzenia IK, ale muszą również przygotować plany całego procesu reagowania na jej potencjalne uszkodzenie, w celu zminimalizowania negatywnych konsekwencji.

By przeciwdziałać wrogim działaniom hybrydowym wymierzonym w IK, UE i NATO powinny dokonać wspólnej charakterystyki słabości sektorów kluczowych dla ich bezpieczeństwa energetycznego i cybernetycznego oraz zaproponować dodatkowe rozwiązania, które podwyższą poziom jej ochrony (np. system wymiany doświadczeń związanych z IK). Dodatkowo powinny one przygotować wspólne, ponadnarodowe standardy oceny odporności IK. Poważnym wyzwaniem i ograniczeniem współpracy między NATO i UE może być niechęć poszczególnych państw członkowskich do dzielenia się wrażliwymi informacji na temat własnych słabości, a także współpraca z sektorem prywatnym, na który zostaną nałożone dodatkowe obowiązki sprawozdawcze, np. prowadzenie cyklicznej oceny ryzyka. Kluczowa dla nowych planów Komisji będzie również kwestia zasobów finansowych, jakie państwa członkowskie będą chciały przeznaczyć na rzeczywiste zaangażowanie się w ochronę IK w UE.

Redakcja: Sławomir Dębski, Łukasz Kulesa, Rafał Tarnogórski,
Jędrzej Czerep, Wojciech Lorenz, Łukasz Maślanka, Patrycja Sasnal, Justyna Szczudlik, Daniel Szeligowski, Jolanta Szymańska, Marcin Terlikowski, Damian Wnukowski, Szymon Zaręba, Tomasz Żornaczuk