PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 112 (2922), 29 LIPCA 2024 © PISM

BIULETYN

Rosyjskie działania dywersyjne wobec państw NATO

Filip Bryjka

Od początku br. Rosja nasila ofensywne działania o charakterze hybrydowym przeciwko państwom NATO. Rosyjskie służby wywiadowcze coraz częściej rekrutują pośredników do prowadzenia ataków dywersyjno-sabotażowych skierowanych m.in. przeciwko infrastrukturze cywilnej i wojskowej, politykom, dziennikarzom i przedstawicielom przemysłu zbrojeniowego. Ich celem jest zastraszanie zachodnich społeczeństw i decydentów, a tym samym osłabienie ich woli dalszego udzielania pomocy wojskowej Ukrainie.

Na początku lipca br. w części amerykańskich baz wojskowych w Europie podwyższono stopień alarmowy do poziomu CHARLIE, który wprowadza się w przypadku wystąpienia incydentu lub otrzymania informacji wywiadowczych wskazujących na prawdopodobieństwo ataków na obiekty i personel. Wzmocnienie środków bezpieczeństwa jest związane ze wzmożoną aktywnością dywersyjno-sabotażową Rosji. W kwietniu br. w Niemczech zatrzymano dwie osoby (obywateli Niemiec rosyjskiego pochodzenia), które na zlecenie rosyjskiego wywiadu przygotowywały ataki na obiekty wojskowe, fabryki uzbrojenia, obiekty przemysłowe i infrastrukturę transportową wykorzystywaną do zaopatrywania Ukrainy. Miały mieć one postać podpaleń i detonacji ładunków wybuchowych, a jednym z planowanych celów były instalacje sił zbrojnych USA w Bawarii, gdzie szkoleni są ukraińscy żołnierze.

Metody rosyjskiej dywersji. Operacje hybrydowe prowadzone przez Rosję wobec państw NATO mają coraz bardziej agresywny charakter. Nie ograniczają się do działań niekinetycznych (np. kampanii dezinformacyjnych, malowania graffiti czy cyberataków), lecz przybierają też postać akcji dywersyjno-sabotażowych (w tym podpaleń), aktów przemocy i wandalizmu czy prowokacji na granicy z wykorzystaniem zinstrumentalizowanej migracji.

Dotychczas w wyniku rosyjskiej inspiracji sabotażyści atakowali głównie tzw. miękkie cele cywilne (np. hale przemysłowe, sklepy, magazyny), m.in. na Litwie, Łotwie, w Estonii, Wielkiej Brytanii i Polsce. We Francji seria podpaleń sparaliżowała funkcjonowanie szybkich linii kolejowych w dniu otwarcia igrzysk olimpijskich, co wywołało trudności komunikacyjne i podważyło zdolność francuskich władz do zapewnienia bezpieczeństwa. Z informacji Agencji Bezpieczeństwa Wewnętrznego (ABW) wynika, że zleceniodawcą dywersji w Polsce jest rosyjski wywiad wojskowy GRU. Pod koniec lipca br. Służba Bezpieczeństwa Ukrainy (SBU) zatrzymała kolejną grupę dywersantów przygotowywaną do działań w Polsce i państwach bałtyckich przez rosyjską Federalną Służbę Bezpieczeństwa (FSB). Chociaż dotychczasowe ataki nie doprowadziły do zakłócenia funkcjonowania państwa i nie wywołały poważnej sytuacji kryzysowej, niektóre z nich dokonywano w miejscach, gdzie składowane są różnego rodzaju tworzywa sztuczne i chemikalia, co niesie za sobą ryzyko skażenia środowiska i ofiar wśród ludności cywilnej – takiemu zdarzeniu ABW zapobiegło w lutym br. we Wrocławiu. Przez takie działania rosyjski wywiad próbuje wywołać atmosferę strachu i sygnalizować gotowość do nakładania kosztów i generowania ryzyka wobec państw wspierających Ukrainę, co ma obniżyć poparcie zachodnich społeczeństw wobec takiej polityki.

Ważnym celem rosyjskiej dywersji są też obiekty infrastruktury wojskowej i należące do przemysłu zbrojeniowego. Ataki na nie mają ograniczyć tempo i skalę zachodniego wsparcia dla Ukrainy. Dotychczas Rosji nie udało się przeprowadzić skutecznej akcji dywersyjnej skierowanej przeciw infrastrukturze wojskowej (na wzór wysadzenia przez oficerów GRU magazynów uzbrojenia

w Czechach w 2014 r.), jednak w fabrykach zbrojeniowych na Łotwie, w Niemczech, Wielkiej Brytanii i Polsce doszło do incydentów, które mogły być efektem celowego sabotażu. Obiekty militarne są przedmiotem intensywnego rozpoznania ze strony rosyjskiej agentury. W maju 2022 r. na Łotwie zatrzymano osoby przygotowujące atak na lotnisko wojskowe Lielvārde, z kolei w połowie 2023 r. w Polsce ABW rozbiła kilkunastoosobową siatkę szpiegowską, która przygotowywała ataki dywersyjne na linie kolejowe, porty morskie i bazy wojskowe.

W celu zminimalizowania kosztów i ryzyka rosyjski wywiad do działań dywersyjnych rekrutuje niewyszkolonych agentów. Pozwala to Rosji zaprzeczać związkom z incydentami i unikać odpowiedzialności. Werbunki są prowadzone m.in. w mediach społecznościowych (np. Telegram), a zapłata realizowana w formie kryptowalut, co utrudnia wykrycie zleceniodawców. Bazę rekrutacyjną stanowią migranci z Europy Wschodniej i rosyjskojęzyczni obywatele państw, w których prowadzone są akcje dywersyjne. Często są to osoby z przeszłością kryminalną lub problemami finansowymi, a ich główną motywacją do współpracy z obcym wywiadem są korzyści materialne. Przyjęty przez Rosjan sposób działania jest spowodowany także wydaleniem ponad 600 dyplomatów (w tym oficerów wywiadów) z Europy.

Rosyjskie służby wywiadowcze zlecają również dokonywanie aktów przemocy i zamachów w celu zastraszenia i wpłynięcia na aktywność zawodową konkretnych osób. Dzięki pozyskaniu przez USA informacji wywiadowczych udało się zapobiec m.in. planowanemu zabójstwu Armina Pappergera – dyrektora niemieckiej firmy Rheinmetall, która produkuje dostarczaną Ukrainie amunicję artyleryjską 155 mm. Wcześniej opłaceni przez rosyjskie służby sprawcy pobili na Litwie rosyjskiego opozycjonistę Leonida Wołkowa, a także zniszczyli samochód ministra spraw wewnętrznych Estonii Lauriego Laanemetsa. Udaremnione zamachy na przedstawicieli sektora zbrojeniowego wskazują, że intencją Rosji jest zastraszanie zachodnich rządów i ich społeczeństw metodami terrorystycznymi, co ma doprowadzić do zmniejszenia skali pomocy dla Ukrainy.

Cyberataki i walka radioelektroniczna. Od początku inwazji na Ukrainę rosyjskie grupy hakerskie APT prowadzą wobec państw NATO intensywne operacje w cyberprzestrzeni, skierowane m.in. przeciw sieciom administracji państwowej i wojskowym systemom teleinformatycznym. Celem cyberataków jest m.in. infrastruktura kolejowa, morska i lotnicza, a w latach 2022–2024 ich ofiarą były m.in. czeskie, łotewskie, litewskie, polskie, rumuńskie i estońskie spółki kolejowe. 15 lipca br. hakerzy z grupy NoName057(16) przeprowadzili serię ataków typu DDoS (odmowa usługi) na polski przemysł zbrojeniowy i infrastrukturę lotniczą, co miało być reakcją na inicjatywę Polski dotyczącą potencjalnego zestrzeliwania rosyjskich rakiet na terytorium Ukrainy przez państwa NATO. Rosyjscy hakerzy usiłują przede wszystkim podważyć zdolności logistyczne państw Sojuszu do zaopatrywania Ukrainy w uzbrojenie i sprzęt wojskowy.

Coraz częściej Rosja stosuje wobec państw NATO elementy walki radioelektronicznej (WRE). Od końca 2023 r. z obwodu królewieckiego, Petersburga i Moskwy okresowo zagłuszany jest sygnał GPS na terytorium państw regionu bałtyckiego. Doprowadziło to do zakłócenia tysięcy lotów cywilnych i wojskowych. Od stycznia do kwietnia br. doświadczyło ich 28% lotów transportowych i obserwacyjnych Królewskich Sił Powietrznych Wielkiej Brytanii nad Europą Wschodnią i 16% nad Północno-Zachodnią. Rosja prowadzi podobne działania na Bliskim Wschodzie (z baz na terytorium Syrii) i Oceanie Atlantyckim (z okrętów marynarki wojennej), zagłuszając sygnał GPS w strategicznym obszarze GIUK między zachodnim wybrzeżem Szkocji i Irlandii a południowo-zachodnim wybrzeżem Islandii. Na udział Rosji w tworzeniu zagrożenia w zakresie kontroli ruchu lotniczego Luksemburga, Szwecji, Francji i Holandii wskazują także ustalenia Międzynarodowego Związku Telekomunikacyjnego. Prócz zagłuszania nawigacji ingerencje polegały na przerywaniu programów telewizyjnych i emitowaniu materiałów propagandowych na temat wojny na Ukrainie. Rosja generuje w ten sposób dodatkowe koszty po stronie państw, które próbują jej utrudnić osiągnięcie celów strategicznych.

Wnioski i perspektywy. Rosja będzie nasilać działania hybrydowe przede wszystkim wobec państw, które mają największy wpływ na wsparcie Ukrainy. Stosując coraz bardziej ofensywne metody – niosące ze sobą ryzyko ofiar, Rosja testuje, jak daleko może się posunąć. Brak zdecydowanej reakcji może ją zachęcać do dalszego nasilania agresji. Choć NATO podkreśla, że działania hybrydowe mogą prowadzić do uruchomienia art. 5 (mówiącego o obronie zbiorowej), wzmocnienie odstraszania wymaga gotowości politycznej do podjęcia proaktywnych działań w odpowiedzi na rosyjską dywersję. Dlatego Sojusz powinien przygotować warianty elastycznego reagowania na rosyjskie akty dywersji i sabotażu, które będą nakładać koszty na atakującego.

Polska pełniąca rolę hubu logistycznego, przez który przechodzi ok. 80% zachodniej pomocy dla Ukrainy, jest szczególnie narażona na rosyjskie ataki dywersyjne. By wzmocnić odporność na tego rodzaju zagrożenia, państwa NATO mogą zwrócić się o wsparcie doradczo-konsultacyjne antyhybrydowych zespołów doradczych NATO (CHST). Odpowiedzialność za przeciwdziałanie i reagowanie na tego rodzaju zagrożenia jest jednak przede wszystkim kompetencją krajową. Chociaż istnieje możliwość uzyskania wsparcia od sojuszników w reakcji na atak hybrydowy, nadużywanie takich mechanizmów (konsultacje na podstawie art. 4 czy art. 5) może osłabiać ich polityczne znaczenie. Dlatego priorytetem powinno być przede wszystkim wzmacnianie narodowej odporności, w tym zwiększenie budżetów służb kontrwywiadowczych i wywiadowczych.