PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 106 (2727), 7 SIERPNIA 2023 © PISM

BIULETYN

Ograniczone zdolności UE do cyberobrony

Aleksandra Kozioł

UE opracowała nową politykę w zakresie cyberobrony po napaści Rosji na Ukrainę, co zwiększyło poziom zagrożeń w przestrzeni cyfrowej. Wytyczne kładą nacisk na odpieranie cyberataków, a także na rozwój zdolności wojskowych i ich koordynację ze sferą cywilną. Duże rozdrobnienie podmiotów odpowiedzialnych za cyberbezpieczeństwo na poziomie UE i brak zachęt dla państw członkowskich utrudniają jednak osiąganie zamierzonych rezultatów.

Polityka UE w zakresie cyberobrony, zaprezentowana w listopadzie 2022 r. przez Komisję Europejską i Wysokiego Przedstawiciela, jest wdrażana z trudnością. Zakłada ona budowę zdolności do odpierania cyberataków i poprawę stanu europejskiego sektora cyfrowego. Realizuje więc założenia Kompasu Strategicznego oraz unijnej strategii cyberbezpieczeństwa z 2020 r., która wyznaczyła cele w zakresie ochrony przed cyberatakami i poprawy zabezpieczeń usług cyfrowych. W UE wciąż trwają ponadto prace nad przyjęciem tzw. aktu w sprawie cyberodporności, który ma określić wymogi cyberbezpieczeństwa produktów, oraz dwóch regulacji zwiększających bezpieczeństwo cyfrowe i informacyjne w instytucjach UE.

Wyzwania cyberbezpieczeństwa. Rosyjskie wojska w lutym 2022 r. wkroczyły na Ukrainę m.in. przy zastosowaniu cyberataku na jedną z działających w Europie sieci satelitarnych. Potwierdza to, że przestrzeń cyfrowa jest domeną działań wojennych, a zabezpieczenie przed cyberatakami musi obejmować podmioty i usługi ze sfery wojskowej i cywilnej. Cyberataki uważane są przeważnie za działania poniżej progu wojny, mimo że w przypadku infrastruktury krytycznej, takiej jak sieci elektroenergetyczne czy satelitarne, mogą spowodować nie tylko paraliż ich funkcjonowania, ale także uszkodzenia fizyczne. Według raportu Agencji UE ds. Cyberbezpieczeństwa (ENISA) z 2022 r. w UE wzrasta zarówno liczba, jak i wpływ cyberataków, inwigilacji cyfrowej oraz kampanii dezinformacyjnych. Coraz częściej wykorzystują je też państwa, wspomagając realizację swoich celów politycznych.

Rosnąca sieć powiązań w przestrzeni cyfrowej wymaga mechanizmów wspólnego przeciwdziałania oraz budowy zdolności nie tylko do ochrony, ale także odpierania cyberataków. Obecnie za te kwestie odpowiadają głównie państwa członkowskie, których zdolności są zróżnicowane, natomiast UE wspiera je w ograniczonym zakresie, obejmującym przede wszystkim sferę cywilną. Ze względu na przekrojowy charakter walki z cyberzagrożeniami na poziomie unijnym odpowiedzialne są za nią cztery podmioty: ENISA, zespół reagowania CERT-EU, centrum zwalczania cyberprzestępczości w Europolu (EC3) i Europejska Agencja Obrony (EDA). W 2018 r. podpisały one porozumienie o współpracy, jednak zdolności UE do odpierania cyberataków pozostają niewystarczające, a współpraca państw – szczególnie w kwestiach wojskowych – ograniczona. Większą rolę w tym kontekście odgrywa NATO.

Wdrażanie polityki cyberobrony w UE. Założenia unijnej polityki obejmują rozbudowę zdolności i pogłębienie współpracy między państwami członkowskimi, ponieważ to do ich kompetencji należą wojskowe działania w przestrzeni cyfrowej. UE pełni w tym procesie rolę wspierającą i koordynującą, a za podstawę kompleksowego podejścia przyjmuje współpracę podmiotów wojskowych i cywilnych, co jest szczególnie istotne wobec zwiększającego się poziomu zależności między siłami zbrojnymi a sektorem cywilnym.

Główny cel polityki – budowa wspólnych zdolności do odpierania cyberataków – miał zostać zrealizowany dzięki powołaniu nowych jednostek odpowiedzialnych za

cyberobronę i włączeniu ich w istniejący cywilny system cyberbezpieczeństwa. Kluczową rolę w nowym systemie cyberobrony przypisano Centrum Koordynacji UE ds. Cyberobrony (EUCDCC), aby zapewnić świadomość sytuacyjną państwom członkowskim oraz misjom i operacjom zagranicznym UE. Przy wsparciu EDA miały działać ponadto sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET) oraz unijna konferencja dowódców ds. obrony cyberprzestrzeni – platforma dyskusji na temat cyberincydentów w siłach zbrojnych. Podnoszeniu praktycznych zdolności do cyberobrony miał natomiast służyć projekt wspólnych ćwiczeń CyDef-X oraz rezerwa ds. cyberbezpieczeństwa działająca na bazie usług świadczonych przez dostawców prywatnych. W praktyce utworzenie tak wielu nowych jednostek i sprecyzowanie ich kompetencji okazało się trudne. W lutym 2023 r. EDA z opóźnieniem utworzyła zaproponowany w polityce cyberobrony MICNET, a w jego skład weszło tylko 18 z 27 państw UE.

Pozostałe założenia polityki, które m.in. za pośrednictwem stałej współpracy strukturalnej (PESCO) i Europejskiego Funduszu Obronnego (EDF) mają przyczynić się do poprawy stanu europejskiego przemysłu, wymagają natomiast szybkiego przeprowadzenia strategicznej oceny nowych i przełomowych technologii z uwzględnieniem sektora cyfrowego. W polityce nie zidentyfikowano pożądanych inwestycji dla państw członkowskich, tymczasem np. uniezależnienie od krytycznych cybertechnologii z państw trzecich i podniesienie atrakcyjności sektora cyberobrony dla wykwalifikowanych ekspertów, których brakuje na europejskim rynku, są niezbędne do wzmacniania międzynarodowej pozycji UE.

Perspektywy współpracy. Publikacja polityki cyberobrony nie zwiększyła istotnie świadomości państw na temat wagi współpracy w świetle bieżących cyberzagrożeń ani nie przełożyła się na wzrost ich zaangażowania w budowę wspólnych zdolności do cyberobrony, o czym świadczy m.in. charakter projektów PESCO. W prace Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji (CIDCC), na którego bazie ma powstać Centrum Koordynacji ds. Cyberobrony, zaangażowały się dotąd tylko cztery państwa (Francja, Niemcy, Holandia i Węgry), a największy projekt, czyli Zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa (CRRT), tworzy zaledwie osiem państw (Belgia, Estonia, Chorwacja, Holandia, Litwa, Polska, Rumunia i Słowenia). Chociaż w maju 2023 r. państwa zgłosiły dwa nowe cyberprojekty PESCO, biorą w nich udział odpowiednio trzy i cztery państwa. Współpraca w zakresie cyberobrony jest ograniczona szczególnie w porównaniu z rozwojem konwencjonalnych zdolności wojskowych w Europie. W ramach projektu PESCO Mobilność wojskowa (MM) oprócz 25 unijnych państw (poza Danią i Maltą) współpracę podjęło czterech partnerów globalnych – Kanada, Norwegia, Stany Zjednoczone i Wielka Brytania.

Mimo to ambicje UE w zakresie cyberbezpieczeństwa na poziomie międzynarodowym zwiększyły się od początku rosyjskiej pełnoskalowej agresji. Głównym celem stała się wymiana doświadczeń i wspieranie zdolności najbardziej narażonych na cyberataki państw Partnerstwa Wschodniego i Bałkanów Zachodnich. Za pośrednictwem Europejskiego Instrumentu na rzecz Pokoju (EPF) Unia sfinansowała np. oprogramowanie i sprzęt dla Sił Zbrojnych Ukrainy, co umożliwiło otwarcie w Kijowie w grudniu 2022 r. centrum szkolenia w zakresie cyberobrony. Zgodnie z wytycznymi nowej polityki na dalsze wsparcie będą mogły w szczególności liczyć państwa kandydujące, które dostosują się do unijnej wspólnej polityki bezpieczeństwa i obrony. UE konsekwentnie podejmuje również temat cyberbezpieczeństwa w relacjach dwustronnych – w 2022 r. odbył się m.in. ósmy dialog ze Stanami Zjednoczonymi i drugi z Ukrainą. Ustanowienie stałego mechanizmu wymiany informacji pozostaje jednak wyzwaniem w stosunkach amerykańsko-unijnych, mimo że np. w 2016 r. unijny CERT-EU i natowski NCIRC zawarły porozumienie techniczne umożliwiające wymianę informacji w sprawach cyberobrony, a obie organizacje współpracują w kwestiach cyberbezpieczeństwa od 2010 r.

Wnioski. Transgraniczny charakter i skutki cyberataków zwiększają potrzebę wspólnych działań, na co odpowiadają założenia polityki UE w zakresie cyberobrony. Rozdrobnienie instytucjonalne i niejasny podział kompetencji między podmiotami wojskowymi a cywilnymi utrudniają jednak współpracę i obniżają zaangażowanie państw członkowskich, mimo że dokument odwołuje się do klauzuli wzajemnej pomocy (art. 42 ust. 7 Traktatu o UE), która działa podobnie do art. 5 w NATO. Większą atrakcyjnością – ze względu na uznane doświadczenie – cechuje się obecnie współpraca w ramach Centrum Doskonalenia Cyberobrony NATO (CCDCOE), do którego dołączają kolejne państwa spoza Sojuszu, m.in. Korea Płd. w 2022 r. i Ukraina w 2023 r.

Rozwój zdolności do odpierania cyberataków na poziomie UE powinien odpowiadać bieżącym zagrożeniom hybrydowym, m.in. ze strony Rosji. Jako niewłaściwe należy w tym kontekście ocenić zatem takie wdrażanie polityki cyberobrony, które rozgranicza działalność podmiotów wojskowych i cywilnych – współpraca MICNET z CERT-EU ma rozpocząć się dopiero po sformowaniu jego zdolności. Ujednolicanie terminologii czy wymiana doświadczeń w kwestiach technik operacyjnych przyniosłyby więcej korzyści, gdyby prowadzone były równolegle z tworzeniem nowej jednostki. Polska, która wydzieliła na poziomie krajowym trzy zespoły reagowania – rządowy, wojskowy i badawczy – będzie nie tylko mogła łatwo włączyć się w prace na poziomie UE, ale także zaoferować własne doświadczenie w zakresie ich funkcjonowania. Warto przy tym, by w sytuacji zagrożenia ze strony Rosji i Białorusi zwiększała inwestycje w sektor cyberobrony z użyciem unijnych środków, m.in. EDF i Cyfrowa Europa.

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