Komentarz KBN

Nr 2 (113) / 2024 12 stycznia 2024 r.

Mechanizm Talliński – istotne wsparcie cybernetyczne dla ukraińskiej infrastruktury krytycznej

Adrian Tyszkiewicz

W dniu 20 grudnia 2023 r. przedstawiciele resortów spraw zagranicznych jedenastu państw (Dania, Estonia, Francja, Niemcy, Niderlandy, Polska, Szwecja, Ukraina, Wielka Brytania, Kanada, Stany Zjednoczone) ogłosili utworzenie platformy wsparcia w zakresie cyberbezpieczeństwa dla odpierającej rosyjską agresję Ukrainy. Zasadnicze elementy planu pomocowego nazwanego Mechanizmem Tallińskim (MT) zostały uzgodnione w stolicy Estonii już 30 maja 2023 r. i przewidywały utworzenie trzech filarów instytucjonalnych: (1) biura prowadzonego przez Estonię w Kijowie, oficjalnie reprezentującego i kierującego inicjatywą (*front–office*); (2) biura organizacyjnego w Warszawie, zajmującego się gromadzeniem informacji o ukraińskim zapotrzebowaniu oraz rozdzielającego zgromadzone zasoby (*back–office*); oraz (3) grupy koordynacyjnej gromadzącej wszystkie zainteresowane strony, w tym Ukrainę. Zadaniem tej ostatniej jest regularne opracowywanie zaleceń i rekomendacji związanych z funkcjonowaniem całego mechanizmu.

Działania grupy, w skład której wchodzą zarówno same państwa sojusznicze, jak i wywodzące się z nich podmioty prywatne – firmy technologiczne oraz organizacje pozarządowe reprezentujące branże IT, określa deklaracja, która zakłada wsparcie dla zdolności obronnych oraz rozwojowych ukraińskiej cywilnej infrastruktury cyfrowej, zagrożonej rosyjskimi operacjami w cyberprzestrzeni. Mechanizm, deklarując podejmowanie decyzji na zasadzie konsensu za wiedzą i przy udziale przedstawicieli strony ukraińskiej, przewiduje wsparcie ujęte w trzech równoległych perspektywach działania: (1) krótkookresowej, zorientowanej na konieczne, celowe wsparcie;

(2) wzmacniającej tendencje rozwojowe perspektywy średniookresowej oraz (3) utrwalającej efekty pomocy i rozwoju opcji długookresowej. Jest to zbieżne z oczywistą i powszechną oceną charakteru konfliktu, którą przy okazji ogłaszania powstania Mechanizmu przypomniał szef MSZ Estonii Margus Tsahkna twierdząc m.in., że do wojennych celów Rosji należą ukraińskie cywilne i militarne zdolności w przestrzeni cyfrowej, stąd wymienione kompleksowe działania są kluczowe dla Ukrainy.

Ważnym postanowieniem w ramach inicjatywy stały się założenia zarówno o komplementarności MT względem budowania wojskowych zdolności obronnych w cyberprzestrzeni, jak i wsparcia wysiłków związanych z rozwojem cyfryzacji Ukrainy w sferze cywilnej. Wreszcie całość działań spełniających kryteria pomocy, odbudowy i wzmacniania ma być zbieżna ze współpracą partnerską ze strukturami NATO, Unii Europejskiej oraz innymi krajami wspierającymi wysiłek wojenny Ukrainy. Chodzi w szczególności o szeroką, gromadzącą ponad 50 państw, koalicję tworzącą tzw. Grupę Ramstein (*Ramstein framework*), której głównym celem jest zapewnienie regularnej pomocy wojskowej dla Kijowa, polegającej na finansowaniu, dostawach uzbrojenia, szkoleniu kadr oraz modernizacji i naprawie sprzętu. To właśnie w ramach Grupy Ramstein w dniu 19 sierpnia 2023 r. powołano Koalicję IT (*IT Coalition*), której głównym zamierzeniem wspartym przez budżet w początkowej wysokości 10 milionów euro przekazanych przez Luksemburg stało się zapewnienie solidnej infrastruktury informatycznej służącej celom obronnym Ukrainy. W grupie partnerów Koalicji znalazły się także wszystkie państwa bałtyckie oraz Dania i Belgia. W szczególności należy zwrócić uwagę na rolę Estonii, która podobnie jak w przypadku MT stała się współinicjatorem utworzenia Koalicji, będącej owocem wcześniejszego namysłu w ramach Grupy Kontaktowej ds. Obrony Ukrainy. Pamiętając przy okazji o roli gospodarza, jaką odgrywa Estonia w ramach cyklicznych, natowskich ćwiczeń z zakresu obrony cybernetycznej (*Cyber Coalition*), gromadzących corocznie 28 aliantów z Paktu, 7 krajów partnerskich, państwa członkowskie UE oraz przedstawicieli przemysłu i ośrodków akademickich, nie sposób nie odczytać fundamentalnego zaangażowania Tallinna w obronę przed zagrożeniami cybernetycznymi jako wniosków wyciągniętych z przypisywanego Rosji kompleksowego ataku hakerskiego na Estonię na przełomie kwietnia i maja 2007 roku. W czasie niespełna miesiąca rosyjscy hakerzy poprzez ataki typu DDoS sparaliżowali m.in. strony wszystkich ministerstw, kilku banków oraz ugrupowań politycznych, a także główny serwer poczty elektronicznej estońskiego parlamentu.

Bezpośrednią przyczyną wszczęcia działań w zakresie Mechanizmu Tallińskiego stał się kolejny, bezprecedensowy, przypisywany rosyjskiej grupie Solntsepek atak hakerski na infrastrukturę jednego z ukraińskich potentatów telefonii komórkowej oraz łączności cyfrowej – firmy Kyivstar, do którego doszło 12 grudnia 2023 r. W wyniku potwierdzonych finalnie przez samą grupę hakerską rosyjskich działań, abonenci sieci, czyli ponad połowa obecnej ukraińskiej populacji, przez dwa dni byli całkowicie pozbawieni łączności telefonicznej i internetowej. Grupa Solntsepek najprawdopodobniej jest powiązana ze znaną z agresywnych działań formacją Sandworm, uznawaną za jednostkę podporządkowaną rosyjskiemu wywiadowi wojskowemu GRU, która przeprowadziła w 2022 r. porównywalny co do skali atak na infrastrukturę łączności satelitarnej oferowanej przez firmę Viasat, skutkujący czasowym wyłączeniem modemów satelitarnych w wielu krajach europejskich oraz zakłóceniem działania turbin wiatrowych na terenie Niemiec.

Rosyjskie działania tym razem nie wpłynęły bezpośrednio na systemy komunikacji wojska ukraińskiego, niemniej jednak zakłóciły system ostrzegania przed nalotami i atakami z powietrza. Na-

tomiast na kilka przynajmniej dni wyłączyły z prawidłowego działania istotne elementy infrastruktury finansowo–handlowej, tzn. kilka systemów bankowych, szereg bankomatów oraz terminali płatniczych. Skalę wrogich działań przybliżają dane mówiące o tym, że ponad dziesięć tysięcy komputerów, cztery tysiące serwerów oraz całe systemy pamięci wirtualnej (*cloud storage*) oraz kopii zapasowych zostały pozbawione danych. Ze względu na domniemany, co najmniej kilkumiesięczny dostęp do serca systemu informatycznego firmy Kiyvstar, zakłada się ponadto, że pozyskane w wyniku włamania dane mogą być wykorzystywane w przyszłości nie tylko ze szkodą dla abonentów operatora, ale także dla innych systemów walczącego z najazdem rosyjskim państwa.

Do kwestii ochrony domeny cyfrowej nadzwyczajną rolę przykłada także sama Ukraina. Obok działań kierowanych przez specjalnie powołane instytucje centralne, jak np. Narodowe Centrum Koordynacji Cyberbezpieczeństwa przy Radzie Bezpieczeństwa Narodowego i Obrony Ukrainy, które w połowie grudnia 2023 r. przeprowadziło strategiczne ćwiczenia z zakresu cyberobrony, Ukraina wdrożyła w ramach systemu szkolnictwa powszechnego służący bezpieczeństwu przedmiot „Obrona Ukrainy", w ramach którego przewidziano m.in. szkolenia z zakresu sterowania dronami, elektroniki oraz prowadzenia komunikacji.

Potrzebom zmagającego się z rosyjskim najazdem państwa w domenie cyberbezpieczeństwa i utrzymania struktury informatycznej próbują w ramach kontaktów bilateralnych sprostać także pojedyncze kraje sojusznicze. Jest to zgodne z literą deklaracji tallińskiej, która uznaje bez zastrzeżeń taką pierwotną formę współpracy. Za przykład może posłużyć zaangażowanie rządu polskiego, który celem wsparcia defensywnych wysiłków Ukrainy zawarł z władzami w Kijowie w sierpniu 2022 r. porozumienie dotyczące współpracy w zakresie cyfryzacji i cyberbezpieczeństwa, które skutkowało m.in. budową mobilnego centrum przetwarzania danych skarbowych. Natomiast już od początków pełnoskalowej inwazji rosyjskiej staraniami rządu polskiego Ukraina otrzymała około dwudziestu tysięcy terminali łączności satelitarnej Starlink, z których pokaźna liczba (około czterech tysięcy) została spożytkowana w tzw. centrach niezłomności, czyli punktach na terenie całej Ukrainy zapewniających niezależną od stanu naziemnej infrastruktury i miejsca usytuowania łączność.

Niewątpliwie Mechanizm Talliński jako inicjatywa grupy państw Paktu Północnoatlantyckiego, Unii Europejskiej oraz prywatnych podmiotów branży technologicznej wzmacnia oraz stabilizuje instytucjonalnie i funkcjonalnie zachodnie wsparcie dla walczącej Ukrainy w zakresie ochrony i rozwoju domeny cyfrowej. Otwarta formuła MT oraz dopuszczenie przedstawicieli świata nauki i prywatnego biznesu stwarza szansę na elastyczne podejście do potrzeb zagrożonej atakami, zapewniającej łączność, cywilnej infrastruktury Ukrainy. Zasada działań zgodnych z prawem międzynarodowym, z każdorazową zgodą strony ukraińskiej, podejmowanych na zasadzie konsensu, w różnych zależnie od potrzeb i sytuacji perspektywach czasowych, wzmacnia także szerszą demokratyczną koalicję państw i innych podmiotów partycypujących w wysiłku obronnym zaatakowanego państwa. Mechanizm, poprzez swoje powiązania z działaniami zainteresowanych stron w sferze wojskowej, ma szanse stać się komplementarną odpowiedzią za rosyjskie ataki mogące nie tylko wpłynąć na deficyty łączności i informacji, także w siłach zbrojnych Ukrainy, ale i na postawę ukraińskiego społeczeństwa, od której zależy w zasadniczym wymiarze wola polityczna kontynuowania wojny obronnej w starciu z agresywnym mocarstwem.