PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 115 (2313), 14 CZERWCA 2021 © PISM

BIULETYN

Wzmacnianie roli UE w zakresie cyberbezpieczeństwa

Aleksandra Kozioł

Trwająca pandemia zwiększyła skalę wykorzystania technologii cyfrowych i nasiliła związane z nimi zagrożenia. UE stanęła więc przed koniecznością wzmocnienia swojego potencjału wykrywania i reagowania na wrogie działania w sieci. Nowe inicjatywy powinny przede wszystkim wpłynąć na usprawnienie współpracy instytucji unijnych z państwami członkowskimi i podmiotami prywatnymi. Skuteczność działań ograniczać będzie jednak niskie i rozproszone finansowanie.

Strategia na cyfrową dekadę. W grudniu ub.r. Komisja Europejska i wysoki przedstawiciel ds. zagranicznych zaprezentowali nową strategię w zakresie cyberbezpieczeństwa, która ma na celu wzmocnienie zbiorowej odporności na cyberzagrożenia oraz zapewnienie ochrony usług i narzędzi cyfrowych w UE. Jej wdrożenie ma także zapewnić Unii czołową rolę w wyznaczaniu międzynarodowych norm i standardów w cyberprzestrzeni.

Publikacji strategii towarzyszyły dwie propozycje legislacyjne, obejmujące tzw. dyrektywę NIS 2, która dotyczy podniesienia cyberodporności Unii i dyrektywę ws. odporności podmiotów krytycznych. Nowe przepisy mają usprawnić współpracę i wymianę informacji na poziomach krajowym i unijnym, rozszerzają także katalog sektorów o istotnym znaczeniu dla cyberbezpieczeństwa, m.in. o usługi cyfrowe, zdrowie i przestrzeń kosmiczną. Zaletą propozycji jest kompleksowe podejście, łączące ochronę przed cyberatakami z zapobieganiem tradycyjnym zagrożeniom, jak przestępczość i klęski żywiołowe.

Wzrost zagrożenia. Funkcjonowanie systemów teleinformatycznych w coraz większym stopniu wpływa na unijne gospodarki, instytucje i działania zewnętrzne. Zależność od technologii cyfrowych szczególnie uwidoczniła się podczas pandemii, gdy 40% pracowników w UE przeszło na pracę zdalną, a wzrost ruchu w sieci (nawet o 60%) nasilił ataki na użytkowników. Stworzyło to zagrożenie nie tylko dla bezpieczeństwa systemów i informacji, ale spowodowało także straty finansowe – szacuje się, że koszt ataków w skali globalnej wyniósł w ub.r. 5,5 bln euro.

Zapewnienie otwartego dostępu do internetu i bezpieczeństwa technologii cyfrowych wymaga współpracy międzynarodowej, co utrudniają działania państw autorytarnych. Wspierają one często inicjatywy grup hakerskich lub używają własnych specjalnych sił wojskowych do walki w sieci. W grudniu ub.r. zaatakowana została np. Europejska Agencja Leków, z której hakerzy – prawdopodobnie powiązani z Rosją i Chinami – wykradli dane nt. szczepionek przeciw COVID-19. Trudności w ustaleniu sprawców utrudniają jednak reagowanie, przez co sankcje za cyberataki UE nałożyła dotąd tylko dwukrotnie, obejmując nimi kilka podmiotów z Rosji, Chin i Korei Płn.

Nowe inicjatywy współpracy. Skuteczność walki z cyberzagrożeniami opiera się przede wszystkim na zdolności wczesnego wykrywania i reagowania przed wystąpieniem szkody. Państwa członkowskie, dostrzegając korzyści ze współpracy, zainicjowały w tym obszarze kilka projektów PESCO, np. zespoły szybkiego reagowania na zagrożenia w cyberprzestrzeni. Obrona przed atakami w sferze cyfrowej wymaga jednak skoordynowania działań na szerszą skalę, czemu ma służyć utworzenie unijnej sieci centrów monitorowania bezpieczeństwa. Zostaną one wsparte przez technologie sztucznej inteligencji, które usprawnią wykrywanie i przyspieszą analizę incydentów. Lepsze przewidywanie ma zapewnić także powołanie grupy roboczej ds. cyberwywiadu przy Centrum Analiz Wywiadowczych UE. Przełamanie sceptycyzmu państw członkowskich wobec przenoszenia kompetencji krajowych na poziom UE będzie jednak wymagało precyzyjnego określenia roli grupy w unijnym systemie, m.in. uwzględnienia zadań Europejskiego Centrum ds. Walki z Cyberprzestępczością w Europolu.

Skala incydentów cyfrowych sprawia, że w ich zwalczanie zaangażowana jest coraz większa liczba podmiotów z państw członkowskich oraz UE. Powoduje to trudności z wymianą zebranych informacji, a także z podejmowaniem współpracy na poziomie operacyjnym i technicznym. Do poprawy zdolności reagowania kryzysowego i koordynacji działań przywracających funkcjonowanie zaatakowanych systemów ma przyczynić się planowana wspólna jednostka ds. cyberprzestrzeni. Jej zadania nie są na razie precyzyjnie określone, co rodzi obawy o powielanie już istniejących kompetencji, m.in. organów unijnych – Agencji UE ds. Cyberbezpieczeństwa (ENISA) czy Zespołu reagowania na incydenty komputerowe (CERT-EU).

Budowa pozycji międzynarodowej. Bezpieczeństwo w sferze cyfrowej stanowi istotny element działań zewnętrznych Unii. Cyberprzestrzeń jako sfera operacyjna wpływa na prowadzenie misji i operacji UE, ma także znaczenie dla bezpieczeństwa w wymiarze globalnym. Główne cele i zadania mają zostać określone w programie na rzecz budowania zewnętrznych zdolności cyfrowych UE, którego realizację wspierać będzie unijna Rada ds. Budowania Zdolności Cyfrowych. Unia rozważa także powołanie nieformalnej sieci dyplomacji cyfrowej, która służyłaby promocji bezpiecznej cyberprzestrzeni. Działania skupiłyby się na pogłębianiu współpracy z partnerami, m.in. NATO, oraz promocji standardów bezpieczeństwa w sferze cyfrowej w ramach organizacji międzynarodowych, np. ONZ i Rady Europy.

Zapewnienie sobie roli lidera w zakresie cyberbezpieczeństwa będzie wymagało od UE poprawy innowacyjności i konkurencyjności technologicznej na globalnym rynku. W tym celu w kwietniu br. Rada wydała zgodę na utworzenie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych. Ma ono połączyć ośrodki publiczne i prywatne zajmujące się kwestiami cyberbezpieczeństwa na poziomie UE, a także zapewnić współpracę z siecią specjalnie powołanych krajowych ośrodków koordynacji.

Poważnym wyzwaniem dla spójności i efektywności unijnych działań w zakresie cyberbezpieczeństwa będzie jednak przezwyciężenie ograniczeń związanych z finansowaniem. Przede wszystkim środki przeznaczone na ten cel są zbyt niskie w stosunku do potrzeb – na lata 2021–2027 wyniosą ok. 2 mld euro na poziomie UE i ok. 2 mld euro rocznie na poziomie państw członkowskich, podczas gdy USA tylko w ub.r. wydały ok. 17 mld dolarów. Dodatkowo unijne finansowanie odbywa się w ramach kilku różnych instrumentów, co utrudnia planowanie inwestycji w tym obszarze.

Wnioski. Poprawa świadomości sytuacyjnej i wymiany informacji między państwami członkowskimi a organami unijnymi jest niezbędna wobec skali zagrożeń w sferze cyfrowej. Zwiększenie odporności UE na cyberataki wymaga m.in. zabezpieczenia infrastruktury i sposobów komunikacji. Propozycje nowych instrumentów częściowo odpowiadają na te potrzeby. Państwa członkowskie powinny jednak zadbać o doprecyzowanie podziału zadań i aktywnie włączyć się w usprawnienie współpracy, a także zwiększyć finansowanie. Pozycja lidera w zakresie cyberbezpieczeństwa wymagać będzie inwestycji w badania i rozwój oraz stworzenia inicjatyw przyciągających i utrzymujących ekspertów na unijnym rynku pracy. Obecnie branża notuje duże braki kadrowe, co świadczy także o braku odpowiedniej edukacji w zakresie cyberbezpieczeństwa i niskiej świadomości społecznej co do zagrożeń w sieci.

Wobec rosnącej podatności na ataki kluczowe będzie szybkie przyjęcie rozporządzeń dotyczących bezpieczeństwa informacji i zasad cyberbezpieczeństwa, jakie mają obowiązywać organy UE (ich wdrażanie ma wspierać wzmocniony CERT-EU). Większą uwagę należy zwrócić także na koordynację cywilnych, obronnych i kosmicznych aspektów cyberbezpieczeństwa. Obecnie w UE rozwijane są oddzielne projekty, np. system bezpiecznej rządowej łączności satelitarnej GOVSATCOM.

Bezpieczne funkcjonowanie systemów teleinformatycznych oraz otwarty dostęp do internetu będą wymagały zwiększonych wysiłków dyplomatycznych na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni. Są one szczególnie istotne ze względu na agresywne działania m.in. Rosji i Chin, które podważają międzynarodowe standardy w tym zakresie. Ze względu na globalną skalę cyberzagrożeń ich skuteczne zwalczanie będzie sprzyjało zacieśnianiu współpracy z partnerami, np. Wielką Brytanią i USA, które posiadają zdolności ofensywne w sferze cyfrowej.

Podatność na działania hybrydowe np. ze strony Rosji – cyberataki i dezinformację w najbliższym sąsiedztwie – negatywnie wpływa na bezpieczeństwo wewnątrz UE. Polska może więc odegrać aktywną rolę w procesie rozbudowy unijnej cyberodporności, wysuwając propozycje specjalnych programów dla państw stowarzyszonych Partnerstwa Wschodniego i Bałkanów Zachodnich. Ważnym elementem będzie także podtrzymanie polskiego zaangażowania w rozwój projektu obserwacji i śledzenia przestrzeni kosmicznej (SST), który zapewni bezpieczne i stabilne funkcjonowanie technologii wykorzystujących dane satelitarne.