Informacja wprowadzająca

Sesja V: W kierunku wzmocnienia zbiorowego wysiłku UE na rzecz poprawy cyberodporności i zwalczania dezinformacji

Wprowadzenie

W ciągu ostatnich kilku lat rozwój technologii cyfrowych osiągnął bardzo wysokie, niespotykane dotąd tempo, i zaczął wyraźnie oddziaływać na każdy właściwie aspekt życia codziennego oraz globalnej gospodarki i polityki. Dlatego też Unia Europejska stosunkowo szybko uznała, że jednym z jej celów powinno być zwiększenie zdolności technologicznych i umiejętności w dziedzinie cyberbezpieczeństwa, a także budowa silnego jednolitego rynku cyfrowego. Elementem istotnym w podejściu UE do kwestii cyberbezpieczeństwa było też zauważalne zbliżenie wojskowego i cywilnego sposobu rozumienia cybersfery oraz równoległe wzmocnienie utworzonej w 2004 r. Agencji Unii Europejskiej ds. Cyberbezpieczenstwa. Konsekwencją wzrastającej świadomości wagi cyberbezpieczeństwa były również decyzje Komisji Europejskiej z 2017 r., która przyjęła strategię trzech filarów cyberbezpieczeństwa w UE. Pierwszy z filarów budował odporność UE na ataki cybernetyczne, drugi kształtował skuteczną prewencję cybernetyczną, a trzeci wzmacniał współpracę międzynarodową w dziedzinie bezpieczeństwa cybernetycznego. Z uwagi na to, przyjętą strategię zwykło się określać jako: odporność, prewencja i obrona, które to założenia są stałym elementem polityki UE w dziedzinie bezpieczeństwa cybernetycznego.

Kluczowymi założeniami podejścia do cybernetyki są: 1) rozwój w kierunku jednolitego rynku bezpieczeństwa cybernetycznego; 2) efektywne wdrożenie i ewaluacja dyrektywy w sprawie bezpieczeństwa sieci i informacji; 3) odporność dzięki szybkiemu reagowaniu w sytuacji kryzysowej; 4) budowanie silnej unijnej bazy umiejętności cybernetycznych; 5) propagowanie cyberhigieny i świadomości zagrożeń; 6) identyfikacja podmiotów działających w złych intencjach; 7) publiczno-prywatna współpraca w zwalczaniu cyberprzestępczości; 8) doskonalenie reagowania politycznego w cybersferze; 9) budowanie zdolności w obszarze bezpieczeństwa cybernetycznego i 10) położenie akcentu na bezpieczeństwo cybernetyczne w stosunkach zewnętrznych. W tym ostatnim zakresie szczegółową strategię działania przedstawiła UE w 2018 r. poprzez m.in. utworzenie Europejskiego Obserwatorium Mediów Cyfrowych, które ma poprawić wykrywalność ataków cybernetycznych i dezinformacji, pracę z platformami internetowymi oraz podnoszenie świadomości i umożliwienie obywatelom reagowania na dezinformację w Internecie.

Funkcjonowanie Europejskiego Obserwatorium Mediów Cyfrowych udowadnia, że z ochroną cybersfery wiąże się zwiększenie świadomości UE na temat rozmaitego rodzaju działań dezinformujących w Internecie. UE przyjmuje, że dezinformacja to fałszywe lub

wprowadzające w błąd treści rozpowszechniane z zamiarem wprowadzenia w błąd lub zapewnienia korzyści gospodarczych lub politycznych, które mogą wyrządzić szkodę publiczną. UE zwraca uwagę, że dezinformacja to także treści wprowadzające w błąd, udostępniane co prawda bez złych intencji, ale wywołujące szkodliwe, z punktu widzenia społeczeństw UE, skutki. Rozpowszechnianie zarówno dezinformacji, jak i jej szczególnej kategorii jaką jest informacja nieintencjonalnie wprowadzająca w błąd (misininformacja) może zagrażać europejskim demokracjom i mieć wiele szkodliwych konsekwencji, takich jak promocja bądź nawet rozszerzenie wpływów wrogów zewnętrznych, narażanie zdrowia, bezpieczeństwa i środowiska UE na rozmaite ryzyka o niedających się przewidzieć ani policzyć skutkach. Należy mieć na względzie, że kampanie dezinformacyjne na dużą skalę stanowią poważne wyzwanie dla Europy i wymagają skoordynowanej reakcji ze strony państw UE, instytucji UE, platform internetowych, mediów informacyjnych i samych obywateli UE.

W nowym cyklu instytucjonalnym na lata 2024–2029 Komisja Europejska lansuje projekt tarczy demokracji, której jednym z priorytetów jest zwalczanie dezinformacji. Najnowszym celem UE jest w związku tym rozwój europejskiej sieci podmiotów weryfikujących fakty i mających zapewnić dostępność tej informacji we wszystkich państwach członkowskich UE i językach urzędowych. Inicjatywa wzmacniająca zdolności tych podmiotów będzie się opierać na pracach Europejskiego Obserwatorium Mediów Cyfrowych. Nowym działaniem jest też wdrożenie programu Cyfrowa Europa 2025-2027. Program ma się koncentrować na wdrażaniu sztucznej inteligencji (AI) i jej wykorzystaniu przez przedsiębiorstwa i administrację publiczną, chmurze obliczeniowej i danych, cyberodporności i umiejętnościach cyfrowych oraz zwalczaniu dezinformacji.

Aktualne wyzwania

Skalę wyzwań dotyczących cyberbezpieczeństwa pokazuje najlepiej najnowszy raport Agencji Unii Europejskiej ds. Cyberbezpieczenstwa przedstawiony w marcu 2025 r. Raport diagnozuje dojrzałość i odporność sektorów krytycznych, objętych dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2), wobec cyberzagrożeń. Ważne jest to, że analiza ujawnia istotne dysproporcje: podczas gdy sektor energetyczny, bankowy i telekomunikacyjny plasują się w czołówce, inne, jak administracja publiczna, zdrowie czy przestrzeń kosmiczna, pozostają w tzw. strefie ryzyka. Raport jest pierwszą kompleksową analizą, w której oceniono dojrzałość i odporność sektorów objętych dyrektywą NIS2, zapewniając zarówno przegląd porównawczy, jak i bardziej dogłębną analizę każdego sektora. Dokument ten ma pomóc państwom członkowskim i organom krajowym w identyfikowaniu luk i ustalaniu priorytetów w efektywnym wykorzystaniu zasobów dla zapewnienia wysokiego poziomu cyberbezpieczeństwa w całej Unii. Badanie opiera się na

danych pochodzących od organów krajowych, firm oraz instytucji unijnych, jak np. Eurostat. Raport nie tylko identyfikuje istniejące luki i zagrożenia, lecz także oferuje kompleksowy zestaw rekomendacji strategicznych skierowanych do państw członkowskich, organów nadzorczych i samych sektorów objętych dyrektywą NIS2. Sektory lepiej oceniane w badaniu skorzystały ze znacznego nadzoru regulacyjnego, globalnych inwestycji, ukierunkowania politycznego i solidnych partnerstw publiczno-prywatnych, a ich odporność ma kluczowe znaczenie dla stabilności społecznej i gospodarczej. Do sektorów posiadających dostateczny poziom dojrzałości zaliczono w raporcie m.in. infrastrukturę cyfrową, w tym podstawowe usługi internetowe, usługi zaufania, centra danych i usługi w chmurze. Co prawda, nadal istnieją tu wyzwania wynikające z nieodłącznej heterogeniczności, transgranicznego charakteru i włączenia w ich zakres wcześniej nieuregulowanych podmiotów, ale poziom odporności na zagrożenia cybernetyczne jest względnie wysoki.

Ponadto, wskazuje się cztery sektory i dwa podsektory będące w „strefie ryzyka". Są nimi: 1) zarządzanie usługami ICT; 2) przestrzeń kosmiczna, 3) administracja publiczna; 4) sektor morski; 5) zdrowie i 6) gaz. Sektory te wymagają szczególnej uwagi, aby zapewnić, że zidentyfikowane luki w poziomie dojrzałości są eliminowane w sposób umożliwiający podmiotom wchodzącym w ich skład skuteczne radzenie sobie z dodatkowymi wyzwaniami. Raport dowodzi, że wszystkie sektory stoją przed wyzwaniami związanymi z budowaniem własnej dojrzałości i spełnianiem wymogów dyrektywy NIS2. Dla lepszego ich wspierania, zaleca się ściślejszą współpracę w ramach sektorów i między nimi, a także wydanie wytycznych dla poszczególnych sektorów, dotyczących wdrażania środków zarządzania ryzykiem.

W rekomendacjach wskazano konieczność rozwoju krajowych zdolności w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem sektorów znajdujących się w tzw. strefie ryzyka. Jedną z możliwości jest stworzenie specjalnych programów wsparcia technicznego i merytorycznego dla organów regulacyjnych oraz organizacji sektora publicznego. Ważne jest również zwiększenie dostępności specjalistycznych szkoleń, ćwiczeń z zakresu cyberbezpieczeństwa oraz narzędzi wspierających analizę ryzyka i reagowanie na incydenty. Poza tym, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa kładzie silny nacisk na potrzebę promowania wymiany informacji i współpracy międzysektorowej. Sugeruje się rozszerzenie roli struktur takich jak ISAC (*Information Sharing and Analysis Centres*), które powinny funkcjonować nie tylko na poziomie krajowym, ale również europejskim. W raporcie wskazano, że wspólne ćwiczenia, współdzielenie scenariuszy zagrożeń oraz rozwój platform wymiany informacji są kluczowe dla zwiększenia świadomości i gotowości. Wreszcie kluczowe znacznie dla zapewnienia cyberbezpieczeństwa ma integracja analiz ryzyka sektorowego z procesami decyzyjnymi na poziomie polityk publicznych. Niektóre sektory – jak energetyka czy bankowość – już korzystają z takich podejść, jednak potrzebne jest rozszerzenie tej praktyki na kolejne branże, szczególnie w sektorach wrażliwych, takich jak zdrowie, administracja

publiczna czy usługi ICT. Powinno to prowadzić do lepszego planowania zasobów, inwestycji oraz skuteczniejszego wdrażania strategii bezpieczeństwa cyfrowego. Raport zawiera też zalecenie dalszego rozwijania ćwiczeń z obszaru cyberbezpieczeństwa na poziomie ogólnoeuropejskim. Ćwiczenia typu Cyber Europe, obejmujące scenariusze awarii międzysektorowych, powinny być rozszerzane o komponenty technologii operacyjnych, łańcuchów dostaw oraz krytycznych zależności międzysektorowych. Szczególne znaczenie ma tu integracja sektorów, które dotychczas rzadko brały udział w tego typu wydarzeniach, jak np. przestrzeń kosmiczna, ciepłownictwo czy wodór.

W przypadku dezinformacji wyzwania są funkcją złożoności samego tego zjawiska. Co do zasady ma ona trzy postaci: 1) dezinformacja rozpowszechniana przez zewnętrzne podmioty (państwa czy np. organizacje); 2) dezinformacja lokalna, która w wielu przypadkach replikuje dezinformację zewnętrzną, ale wcale nie musi to być regułą i 3) misinformacja, która obejmuje rozpowszechnianie manipulacyjnych lub fałszywych treści przez osoby prywatne, często nieświadomie, za pomocą rozmaitych komunikatów (tik tok, platforma X, Facebook). Aby skutecznie walczyć z dezinformacją i misinformacją potrzebnych jest wiele działań i środków, do których należy zaliczyć: 1) finansowanie i wspieranie podmiotów, które identyfikują i ewidencjonują konkretne przypadki dezinformacji np. „fake newsy" (*fact-checking*); 2) rozwój zasobów ludzkich, głównie pozyskiwanie wykwalifikowanych kadr; 3) efektywne komunikowanie, w tym tworzenie prawdziwych, interesujących narracji i skuteczne przekazywanie komunikatów trafiających do odbiorców; 4) budowanie relacji i zaufania, ponieważ podmioty działające na rzecz walki z dezinformacją muszą stale umacniać swoją wiarygodność i podejmować pozytywne kampanie mające na celu budowanie zaufania i zaangażowania obywateli, przy jednoczesnym zrozumieniu ich potrzeb, a zarazem delikatnej równowagi w pluralistycznym społeczeństwie demokratycznym, w którym funkcjonują różne opinie i poglądy (walka z dezinformacją nie może być bowiem sposobem narzucania jednej wizji świata: jeżeli tak będzie postrzegana, sama stanie się rodzajem dezinformacji); 5) transformacja cyfrowa, która zapewni dostęp do skutecznych narzędzi cyfrowych w celu pozyskiwania i wizualizacji danych, projektowania graficznego i edycji wideo, co pozwoli na weryfikację treści i tym samym zapewni umiejętność krytycznego myślenia.

Wagę problematyki bezpieczeństwa podkreślono w „Warsaw Call", tj. wspólnym oświadczeniu przyjętym przez ministrów UE ds. cyberbezpieczeństwa w dniu 5 marca 2025 r. podczas nieformalnego spotkania zorganizowanego przez Ministerstwo Cyfryzacji. Apel Warszawski stanowi ważny punkt odniesienia dla przyszłych działań Unii Europejskiej w zakresie ochrony przestrzeni cyfrowej w dobie rosnących wyzwań geopolitycznych. Zawraca się w nim uwagę na konkretne działania UE w następujących obszarach: 1) wzmocnienie zarządzania kryzysowego poprzez sprawne przyjęcie Cybersecurity Blueprint; 2) wzmocnienie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa, w tym również UE-NATO; 3) przyjęcie

mapy drogowej nowych technologii oraz prognozowania strategicznego w obszarze cyberbezpieczeństwa; 4) zwiększenie wysiłków na rzecz zwalczania niedoboru specjalistów ds. cyberbezpieczeństwa w UE.

Szczególnym wyzwaniem w obszarze cyberbezpieczeństwa i dezinformacji jest budowanie odporności społeczeństw demokratycznych na sytuacje krytyczne. Szczególnej ochronie powinny być poddane wszystkie demokratyczne procedury, takie jak wybory czy referenda, które z założenia stają się celem wzmożonych ataków oraz manipulacji. Praktyka podpowiada, że są to szczególne momenty, w których aktywizują się podmioty zewnętrze zainteresowane wywarciem wpływu na sceny polityczne państw członkowskich UE. Z kolei instytucje stojące na straży demokracji muszą w tym przypadku działać w sposób szczególnie ostrożny i wyważony, żeby nie naruszyć zaufania publicznego oraz by same instytucje nie zaczęły być postrzegane jako uczestnik szerokiego i złożonego procesu dezinformacji.

Pytania do dyskusji

1. Jaka jest rola Unii Europejskiej i jej instytucji w budowaniu odporności UE na zagrożenia związane z infrastrukturą cybernetyczną i działania dezinformacyjne?
2. Jak wzmocnić odporność cybernetyczną sektorów z tzw. obszaru ryzyka, tj. zarządzanie usługami ICT, administracja czy zdrowie?
3. Jaka powinna być rola platform cyfrowych w zapewnieniu bezpieczeństwa cybernetycznego społeczeństwom UE?
4. Jak wzmocnić organizacje społeczeństwa obywatelskiego w skutecznej walce z dezinformacją?
5. Jak modyfikować narzędzia walki z dezinformacją, kiedy ta zmienia się i dostosowuje do zmian społeczno-politycznych?
6. Jak budować efektywne kanały komunikacji, których celem jest generowanie zaufania do informacji, co będzie zwiększało u odbiorców świadomość możliwości dezinformacji lub misinformacji?
7. Jakie są możliwości zastosowania sztucznej inteligencji (AI) dla zapewnienia odpowiedniego poziomu cyberbezpieczeństwa i skutecznej walki z dezinformacją?