ZDOLNOŚCI CYBERWYWIADOWCZE UE – WYZWANIA I OGRANICZENIA [ANALIZA]

Unia Europejska stworzyła wspólne ramy umożliwiające podejmowanie skoordynowanych działań w celu wzmocnienia cyberbezpieczeństwa, w tym rozwój zdolności cyberwywiadu.

Skomputeryzowane systemy sieciowe, wspierane przez technologie sztucznej inteligencji, w coraz większym stopniu stają się platformą rozprzestrzeniania zagrożeń ładu publicznego i bezpieczeństwa wewnętrznego, a także bezpośrednich ataków na cele żywotne dla interesów bezpieczeństwa narodowego. W celu obniżenia poziomu ryzyka, skali zagrożeń oraz prawdopodobieństwa cyberataku, współczesne państwa tworzą systemy wykrywania, ostrzegania, przeciwdziałania i obrony przed cyberzagrożeniami. Włączają w te działania służby wywiadowcze, rozwijając ich specjalistyczne zdolności oraz umieszczając je w odrębnych ramach organizacyjno-instytucjonalnych, określanych jako „cyberwywiad".

Cyberwywiad obejmuje zespół zorganizowanych czynności pozyskiwania, gromadzenia, przetwarzania i analizowania danych i informacji generowanych i/lub przesyłanych w sieciowych systemach teleinformatycznych w celu wytworzenia wiedzy o źródłach i podmiotach działań zagrażających bezpiecznemu funkcjonowaniu infrastruktury teleinformatycznej, a przez to wspomagania procesów decyzyjnych zmierzających do zapobiegania, przeciwdziałania i zwalczania takich zagrożeń. Ponieważ infrastruktura teleinformatyczna ma istotne, w części krytyczne, znaczenie dla bezpieczeństwa państw oraz ich obywateli, cyberwywiad jest domeną władzy państwowej, w szczególności wyspecjalizowanych organów i służb, choć nie wyklucza to rozwoju prywatnych zdolności rozpoznawczo-analitycznych przez podmioty gospodarcze traktujące „cyberwywiad" jako formę usługi rynkowej. Ze względu na transgraniczne powiązania między elementami infrastruktury technicznej oraz zdeterytorializowane, zwirtualizowane interakcje wykreowane przez oprogramowanie sterujące skomputeryzowanymi systemami urządzeń, cyberbezpieczeństwo wykroczyło poza obszar interesów narodowych i stało się przedmiotem międzynarodowej rywalizacji i współpracy.

Instytucje i organizacje międzynarodowe, których cele obejmują także bezpieczeństwo, stabilność międzynarodową i ład wewnętrznych, takie jak NATO i Unia Europejska, od pewnego czasu podejmują skoordynowane działania na rzecz wzmocnienia zdolności cyberwywiadowczych. W przypadku Unii Europejskiej, formalne kroki w kierunku poprawy stanu cyberbezpieczeństwa podjęte zostały już na początku bieżącego stulecia, choć dopiero w 2013 r. przyjęta została unijna strategia cyberbezpieczeństwa. We wrześniu 2017 r. strategia została zaktualizowana i uzupełniona o elementy wzmacniające odporność infrastruktury teleinformatycznej państw członkowskich na zagrożenia i ataki, a także polepszające koordynację między organami cyberbezpieczeństwa państw członkowskich oraz działania na poziomie UE. Rok później, na szczycie UE w Brukseli, uzgodniono „zwalczanie nielegalnych i prowadzonych w złej wierze działań w cyberprzestrzeni i wykorzystujących cyberprzestrzeń oraz budowanie silnego cyberbezpieczeństwa." W kontekście nasilenia cyberataków, a także kampanii dezinformacji w internecie, przywódcy państw członkowskich oznajmili: „Takie

zagrożenia i ataki zwiększają naszą wspólną determinację do dalszego umacniania wewnętrznego bezpieczeństwa UE oraz naszych zdolności i możliwości w zakresie wykrywania wrogich działań obcych służb wywiadowczych i innych podmiotów działających w złej wierze na naszych terytoriach, a także online, jak również do zapobiegania takim wrogim działaniom, zakłócania ich i reagowania na nie." To stanowisko współbrzmiało z wcześniejszymi oświadczeniami dotyczącymi zagrożeń hybrydowych, wśród których na czołowym miejscu znajdowały się cyberzagrożenia.

Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym obejmowały inicjatywę powołania Komórki UE ds. syntezy informacji o zagrożeniach hybrydowych (Hybrid Fusion Cell – HFC). Co istotne, komórka ta miała powstać w obrębie Centrum Wywiadowczego i Sytuacyjnego UE (INTCEN) – organu współpracy wywiadowczej państw członkowskich w zakresie analizy problemów i zagrożeń bezpieczeństwa Unii Europejskiej. Zadania HFC, działającej od maja 2017 r., obejmują analizę na podstawie informacji niejawnych od państw członkowskich oraz rozpoznania jawnoźródłowego różnych aspekty zagrożeń hybrydowych, określanie poziomu ryzyka, regularna ocena zagrożeń oraz formułowanie ostrzeżeń dla Europejskiej Służby Działań Zewnętrznych (ESDZ), Komisji Europejskiej i państw członkowskich.

HFC została także uwzględniona w zaleceniach Komisji Europejskiej w sprawie skoordynowanego reagowania na incydenty i kryzysy na dużą skalę. Uznano ją za jeden z unijnych podmiotów zaangażowanych w reagowanie na kryzysy w cyberprzestrzeni. Jej zadaniem jest „szybkie analizowanie odnośnych incydentów i informowanie odpowiednich struktur koordynujących." Regularne raportowanie i ostrzeganie przez tę komórkę powinno wzmocnić zdolności i gotowość do adekwatnej reakcji na niebezpieczne zdarzenia i szkodliwe incydenty cybernetyczne. W zaleceniach Komisja włączyła HFC w skoordynowane działania wywiadowcze w formacie SIAC, zobowiązując ją do przygotowania operacyjnego raportu sytuacyjnego na temat stanu bezpieczeństwa cybernetycznego w UE.

Dokument Komisji Europejskiej korespondował z nieco wcześniejszym dokumentem tematycznym dotyczącym wspólnej unijnej akcji dyplomatycznej w odpowiedzi na rosnącą intensywność operacji w cyberprzestrzeni i postulującym wyposażenie państw członkowskich w tzw. cyberdyplomatyczną skrzynkę narzędziową. Odnosząc się do niepokojących procesów w stosunkach międzynarodowych przy wykorzystaniu globalnych sieci teleinformatycznych, w szczególności internetu (cyberataki, incydenty hakerskie, ingerencja w procesy wyborcze, dezinformacja i przekłamania), Rada UE podkreśliła, że z punktu widzenia skuteczności działań prewencyjnych i obronnych, zwłaszcza w świetle prawa międzynarodowego, istotną kwestią jest ustalenie, który podmiot państwowy lub niepaństwowy ponosi odpowiedzialność za szkodliwe działania w cyberprzestrzeni. Dlatego istotne jest uruchomienie zdolności rozpoznawczo-analitycznych w ramach UE, na podstawie podzielanej przez państwa członkowskie świadomości sytuacyjnej adekwatnej do zaistniałych sytuacji. Jednakże – jak podkreśliła Rada – działania takie zależą od suwerennej decyzji politycznej państw członkowskich opartej na danych wywiadowczych pochodzących z wszelkich dostępnych źródeł.

Wnioski Rady UE oznaczały więc danie państwom członkowskim wolnej ręki w uruchamianiu mechanizmów koordynacji odpowiedzi na zagrożenia cybernetyczne, a tym bardziej w sięganiu po zasoby informacji i analiz wywiadowczych będących w posiadaniu rządów państw członkowskich. Dlatego ani zalecenia Komisji, ani wniosku Rady nie skutkowały rozwojem współpracy cyberwywiadowczym ani na poziomie strategicznym, ani – tym bardziej – operacyjnym. Wobec takiego stanu rzeczy Europejska Służba Działań Zewnętrznych postanowiła uruchomić własne zdolności analityczne i organizacyjne. W niedawno opublikowanym dokumencie roboczym ESDZ zaproponowała wzmocnienie roli i aktywności INTCENu, a także funkcjonującej w jego ramach Komórki UE ds. syntezy informacji, w zakresie działań wykrywczych w odniesieniu do cyberataków, jak również przygotowania środków zapobiegania i przeciwdziałania cyberzagrożeniom.

W dokumencie ramowym zaznaczono, że INTCEN powinien wykorzystać najnowsze zdolności wywiadowcze, odzwierciedlając jednocześnie niuanse i potencjalne różnice stanowisk poszczególnych państw członkowskich. W związku z tym oceny zagrożeń na poziomie UE będą miały charakter wprowadzający, doradczy i uzupełniający, a zatem nie mogą zastąpić krajowych analiz wywiadowczych i być uznawane za wspólne stanowisko wobec zidentyfikowanych zagrożeń.

Unia Europejska stworzyła wspólne ramy umożliwiające podejmowanie skoordynowanych działań w celu wzmocnienia cyberbezpieczeństwa, w tym rozwój zdolności wywiadu cybernetycznego. Jednak w dalszym ciągu obowiązuje zasada pełnej odpowiedzialności państw członkowskich za środki, metody i efekty podjętych działań. Cyberbezpieczeństwo jest ujmowane jako element bezpieczeństwa narodowego, wobec czego – zgodnie z art. 4 ust. 2 traktatu o Unii Europejskiej – nakłada na państwa członkowskie wyłączną odpowiedzialność w tej domenie. Niemniej należy zauważyć, na co zresztą niejednokrotnie zwracała uwagę Komisja Europejska, że cyberprzestrzeń nie jest „przypisana" terytorialnie do państw członkowskich i powinna być traktowana jako ponadnarodowa struktura informacyjno-komunikacyjna sterująca transnarodowymi sieciami zarządzania w sektorach gospodarki i finansów, wspólnego bezpieczeństwa i obrony oraz dyplomacji, a także jest podstawą „cyfrowego" wspólnego rynku oraz infrastruktury krytycznej w UE.

Zaznaczenie potrzeby rozwoju zdolności cyberwywiadowczych jest pozytywnym sygnałem, niemniej ciągle postrzeganym w kontekście deklaracji woli (lub jej braku) ze strony poszczególnych państw członkowskich. Rozproszenie organów cyberwywiadowczych na poziomie UE z pewnością nie pomaga w skutecznej koordynacji wysiłków. Zespolenie tych działań w wyraźnie określonych ramach instytucjonalno-organizacyjnych oraz precyzyjne wyznaczenie obszaru kompetencji jednostek unijnych powinno być pierwszym, poniekąd przełomowym krokiem w stronę budowy jednolitych zdolności wywiadu cybernetycznego w Unii Europejskiej.

Autor: Prof. dr hab. Artur Gruszczak - Ekspert Fundacji Instytutu Bezpieczeństwa i Strategii

Pełna wersja tekstu została opublikowana na stronie Fundacji IBIS: Zdolności cyberwywiadowcze UE – wyzwania i ograniczenia