OPINIA WIIS nr 5/2018

Autor: Karol Cheda

WARSZAWSKI INSTYTUT INICJATYW STRATEGICZNYCH

EUROPEJSKIE CYBERZESPOŁY SZYBKIEGO REAGOWANIA

Od czasu wejścia w życie Traktatu Lizbońskiego Unia Europejska znacząco poszerzyła obszary możliwej integracji. Wymiar gospodarczy już dawno przestał być jedynym czynnikiem integracji i choć wciąż pozostawał on kluczowy, w 2009 roku zdecydowano się mocniej zaakcentować obszar wspólnej polityki zagranicznej i bezpieczeństwa. Pomimo tego, przyszło nam jednak czekać niemal osiem lat na ustanowienie stałej współpracy strukturalnej – PESCO, w której uczestniczą wszystkie państwa Unii wyłączając Danię, Maltę i Wielką Brytanię. Pierwsza faza formowania PESCO zakłada realizację 17 wspólnych projektów obejmujących w swoim zakresie tematycznym szeroki obszar europejskiego bezpieczeństwa.

Jednym z ww. projektów jest utworzenie cyberzespołów szybkiego reagowania (Cyber Rapid Response Teams – CRRTs) i wzajemnego wsparcia w obszarze cyberbezpieczeństwa, które mają funkcjonować w ramach PESCO. W tym celu 25 czerwca 2018 roku sześć państw członkowskich: Chorwacja, Estonia, Litwa (inicjator i, co za tym idzie, państwo przewodzące projektowi), Holandia, Rumunia oraz Hiszpania podpisały deklarację woli ich sformowania. Dokument odwołuje się do Dyrektywy Parlamentu Europejskiego i Rady Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS) i tym samym częściowo wpisuje się w proces jej wdrażania. Sama deklaracja opiera się na identyfikacji potrzeby utworzenia i rozwoju zdolności kooperacji w celu *zapobiegania, odstraszania oraz odpowiedzi na cyberzagrożenia*, a jej głównymi założeniami są:

- Stworzenie obszaru pogłębionej współpracy w cyberprzestrzeni poprzez *wzajemne wsparcie w odpowiedzi na cyberincydenty, w tym wymianę informacji, wspólne ćwiczenia, wsparcie wspólnych operacji, B+R i utworzenie wspólnych zdolności*, odbywające się w ramach stałych struktur europejskich;
- Utworzenie sieci CRRT-ów zapewniających jej funkcjonowanie i będących dostarczycielami kompetencji wspierania CERT-ów narodowych;
- Docelowy rozwój drugiej generacji Cyber Toolkit-u, czyli zestawu narzędzi opracowanego, aby wspierał zdolności wykrywania, identyfikacji i zwalczania cyberzagrożeń. Planowo, projekt ma zostać, całkowicie bądź częściowo, sfinansowany przez Europejski Fundusz Obronny;
- Promocja współpracy cywilno-wojskowej oraz wsparcia europejskiego przemysłu bezpieczeństwa teleinformatycznego.

Dokument ma charakter ogólnikowy, nie znalazło się w nim miejsce na szczegółowy plan utworzenia zapowiadanych struktur, jednak zdaje się to wynikać ze specyfiki inauguracyjnej deklaracji. Stanowi jedynie wstępny fundament i w ten sposób interpretowany, napawa optymizmem. Sam fakt identyfikacji potrzeby rozwoju zdolności prowadzenia działań w cyberprzestrzeni na poziomie europejskim jako wymagającej intensywnej rozbudowy wydaje się być największą zaletą omawianego dokumentu. Rozbudzenie świadomości jej istnienia jest pierwszym krokiem do utworzenia wydajnego europejskiego systemu cyberbezpieczeństwa i choć do jego powstania jeszcze daleka droga, deklaracja wyznacza ramy czasowe realizacji zawartych w niej postanowień – do końca 2018 ma zostać podpisany

protokół ustaleń, zaś wstępna gotowość operacyjna CRRT-ów jest przewidziana na 2019 rok, kiedy to zostanie doprecyzowany ich kształt oraz zakres kompetencyjny. Cieszy również zawarta w dokumencie deklaracja utworzenia drugiej generacji Cyber Toolkit-u. Zdolność ciągłego rozwoju i adaptacji do nowych uwarunkowań zajmuje kluczowe miejsce w wachlarzu kompetencji niezbędnych do efektywnego prowadzenia działań w cyberprzestrzenii. Na ocenę skuteczności CRRT-ów przyjdzie czas, jednak w tym momencie wątpliwości może budzić ich nieprecyzyjne umiejscowienie w unijnym systemie cyberbepieczeństwa. Pomimo deklaracji, że istniejące struktury nie zostaną zduplikowane, stworzenie CRRT-ów może doprowadzić do rozproszenia kompetencji w tym obszarze, dlatego niezbędne będzie ich czytelne rozgraniczenie. Podczas gdy Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), wraz z podlegającym jej CERT-EU, pełni funkcje pomocnicze, CRRT-y, wraz z europejską siecią CSIRT-ów (Computer Security Incident Response Team) dysponują potencjałem stania się „frontową" strukturą cyberobrony.

OPINIA WIIS nr 5/2018

Autor: Karol Cheda

WARSZAWSKI INSTYTUT INICJATYW STRATEGICZNYCH

POLSKI PUNKT WIDZENIA:

Polska jest wymieniana obok Finlandii i Francji, jako jeden z trzech krajów, które w najbliższym czasie planują dołączyć do omawianego projektu PESCO. Będzie to już 9 inicjatywa w ramach stałej współpracy strukturalnej z polskim udziałem. Po początkowej fazie niskiej aktywności, Polska znacząco zwiększyła zaangażowanie we wspólną europejską politykę obronną.

Zaangażowanie w projekt utworzenia cyberzespołów szybkiego reagowania oraz ukonstytuowania platformy współpracy wewnątrzeuropejskiej w tym obszarze jest kluczowe z polskiego punktu widzenia. Znacząco wpłynie na jakość cyberobrony i pozwoli na wymianę doświadczeń, co jest szczególnie istotne w okresie reorganizacji systemu cyberbezpieczeństwa wobec konieczności adaptacji do wymogów dyrektywy NIS. Zacieśnienie współpracy wpłynie również na multiplikację możliwości przeciwdziałania atakom oraz skuteczności odpowiedzi na nie. Wspólnotowy charakter inicjatywy przewiduje wzajemne zaangażowanie w wypadku zagrożenia, a także prowadzenie połączonych operacji pod egidą Unii Europejskiej.

Rzeczona inicjatywa jest również ważna ze względu na kontekst geopolityczny. Status Polski jako regionalnego lidera, także pod względem militarnym, wymaga aktywnego zaangażowania w międzynarodowe projekty. Może ona zostać wykorzystana również w celu budowy relacji bilateralnych - znaczna część zaangażowanych w nią państw znajduje się w bezpośredniej strefie zainteresowania polskiej dyplomacji począwszy od inicjatora i lidera projektu, Litwy. Inicjatywa kładzie również nacisk na zaangażowanie podmiotów przemysłowych sektora cybernetycznego krajów członkowskich, co jest doskonałą szansą na promocję polskiego biznesu.

Na podstawie:

- Declaration of Intent on Cooperation in the field of Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity;
- https://eeas.europa.eu/headquarters/headquarters-Homepage_en, European Union External Action;
- http://mon.gov.pl/, Ministerstwo Obrony Narodowej.