CYBERBEZPIECZEŃSTWO – CYWILNE CZY WOJSKOWE? [ANALIZA]

Kto w rządzie odpowiada za cyberbezpieczeństwo? Ministerstwo Cyfryzacji czy Ministerstwo Obrony Narodowej? Każde z nich ma inne zdanie na ten temat. Tymczasem departament ds. cyberprzestrzeni powstanie także w Kancelarii Prezesa Rady Ministrów. Swoje ambicje zgłaszają również MSWiA, które nadzoruje działania policji w obszarze cyberbezpieczeństwa, oraz Ministerstwo Rozwoju wraz z pomysłem Cyberparku Enigma. Odpowiedzialność instytucjonalna za cyberbezpieczeństwo to również kwestia tego, czy powinno ono mieć charakter cywilny czy wojskowy.

MON: pieniądze i spółki

Szef MON Antoni Macierewicz nie pozostawia wątpliwości, że to jego resort odpowiada za cyberbezpieczeństwo. – *Ministerstwo Obrony Narodowej ponosi odpowiedzialność za zabezpieczenie bezpieczeństwa cyberprzestrzeni na poziomie państwowym i nikt nie zwolni nas z tego obowiązku. Jeżeli Polska ma być bezpieczna od zagrożeń cybernetycznych MON musi pozostać środkiem ciężkości całego systemu cyberbezpieczeństwa* – zaznaczył Macierewicz na początku października podczas III Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC 2017.

Czytaj więcej: Macierewicz: Polska będzie mieć 1000 cyberżołnierzy [Cyberdefence24.pl TV]

MON podjęło decyzję o utworzeniu – jak to nazwał minister – wojsk cybernetycznych. Na to zadanie resort ma przeznaczyć ok. 2 mld zł. Zostały zwiększone zadania Narodowego Centrum Kryptologii i powołano pełnomocnika MON ds. bezpieczeństwa i cyberprzestrzeni, którym jest wiceminister Bartłomiej Grabski.

Fot. ppor. Robert Suchy/DKS MON

Według zapowiedzi Macierewicza wojska cybernetyczne mają liczyć przynajmniej tysiąc żołnierzy zdolnych do walki w cyberprzestrzeni.

Czytaj więcej: Utworzono biuro ds. organizacji polskich oddziałów cybernetycznych

Na CYBERSEC 2017 szef MON podkreślił, że wszystkie te działania "są koordynowane" z kancelarią premiera i ministrem Pawłem Szefernakerem, który ma kierować departamentem ds. cyberprzestrzeni w KPRM – *Jesteśmy też w ścisłym kontakcie z Biurem Bezpieczeństwa Narodowego* – dodał Macierewicz. Ministerstwa Cyfryzacji kierowanego przez Annę Streżyńską nie wymienił.

Szef MON podkreśla konieczność suwerennej kontroli państwa nad sieciami telekomunikacyjnymi, "rdzeniem nerwowym" cyberprzestrzeni. W ten właśnie sposób resort uzasadnia przejęcie kontroli nad spółką Exatel, posiadającą 2,6 tys. węzłów telekomunikacyjnych i 20 tys. kilometrów sieci światłowodowej. – *Stanowi ona kręgosłup naszego cyberbezpieczeństwa* – powiedział na początku października minister.

W marcu MON w imieniu Skarbu Państwa wykupiło od – kontrolowanej przez państwo – Polskiej Grupy Energetycznej 100 proc. akcji Exatela. PGE podało w komunikacie, że cena sprzedaży wynosiła 368,5 mln zł.

We wrześniu podczas Międzynarodowego Salonu Przemysłu Obronnego w Kielcach Exatel wspólnie z Polską Grupą Zbrojeniową – również kontrolowaną przez MON – powołało spółkę QBiTT. Jej zadaniem jest dostarczanie rozwiązań z obszaru cyberbezpieczeństwa sektorowi zbrojeniowemu. – *Spółka QBITT, która integruje, koordynuje działania wszystkich spółek wchodzących w skład PGZ, których produkcja wiąże się z działalnością w cyberprzestrzeni. To będzie integrator tego wysiłku walki i obrony w cyberprzestrzeni* – mówił wówczas Macierewicz. Jego zdaniem, aby Polska była zdolna do skutecznej obrony w cyberprzestrzeni trzeba zintegrować wysiłek przemysłu. Taka właśnie ma być rola spółki QBiTT.

Fot. Exatel

Szef MON często podkreśla, że w czerwcu 2016 r. na szczycie w Warszawie NATO uznało cyberprzestrzeń za strefę działań operacyjnych, obok lądu, morza, powietrza i przestrzeni kosmicznej. Minister zwraca też uwagę, że dezinformacja jest bronią chętnie używaną przez naszego potencjalnego przeciwnika, czyli Rosję.

Czytaj więcej: MSPO 2017: QBiTT – nowa spółka PGZ i Exatel

MC: strategia i koncepcje

Pomimo ambicji wyrażonych przez szefa MON w Krakowie to Ministerstwo Cyfryzacji stworzyło polską strategię cyberbezpieczeństwa, która jako Krajowe Ramy Polityki Cyberbezpieczeństwa na lata 2017-2022 została przyjęta w kwietniu przez Radę Ministrów. Strategia ta nie wskazuje wprost na rolę przewodnią Ministerstwa Cyfryzacji, ale wyznacza szereg zadań dla ministra właściwego do spraw informatyzacji.

Czytaj więcej: Bezpieczna Polska w cyfrowej erze. Strategia Cyberbezpieczeństwa na lata 2017-2022 [ANALIZA]

W Krajowych Ramach czytamy m.in.:

Minister właściwy do spraw informatyzacji, we współpracy z innymi resortami, dokona przeglądu regulacji sektorowych i szczególnych, które dotyczą omawianej problematyki oraz regulacji prawnych, które mogą mieć oddziaływanie na inne obszary, na przykład na ochronę danych osobowych, czy infrastrukturę krytyczną w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej.

Ponadto minister właściwy ds. informatyzacji *zapewni działanie systemu analizy i bieżącego*

zarządzania ryzykiem w cyberprzestrzeni RP oraz będzie odpowiedzialny za przygotowanie i wdrożenie programu „Złota Setka”.

Krajowe Ramy wyznaczają również ministrowi właściwemu do spraw informatyzacji koordynowanie wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa. Ponadto minister opracowuje propozycję działań korygujących po dwóch latach od przyjęcia dokumentu.

Powyższe stwierdzenia pozwalają wnioskować, że Minister Cyfryzacji powinno odgrywać rolę głównego koordynatora we wprowadzaniu Krajowych Ram we współpracy z innymi instytucjami, w tym z MON.

Zastanawiające jest jednak finansowanie Krajowych Ram. Minister Streżyńska w wywiadzie dla CyberDefence24.pl podczas forum CYBERSEC 2017 w Krakowie powiedziała, że pieniądze na realizację strategii są w budżecie MON. Streżyńska dodała jednak, że szef MON jest świadomy zadań MC w obszarze cywilnego aspektu cyberbezpieczeństwa i dlatego wie, jakie wydatki będą realizowane. Minister powiedziała, że nie ma żadnych obaw, że część wydatków zostanie zmilitaryzowana. W wypowiedzi dla Cyberdefence24, poinformowała, że przygotowując preliminarz tych wydatków, dokładnie określono, co w nich jest.

Czytaj więcej: Streżyńska dla CyberDefence24.pl TV: Pieniądze na realizację strategii cyberbezpieczeństwa są w budżecie MON (CYBERSEC 2017)

Ministerstwo Cyfryzacji koordynuje również prace nad ustawą o krajowym systemie cyberbezpieczeństwa, która między innymi implementują dyrektywę NIS do polskiego porządku prawnego oraz ustali kompetencje poszczególnych ministerstw w obszarze cyberbezpieczeństwa, pozwalając na uniknięcie sporów kompetencyjnych. Resort Streżyńskiej koordynuje również prace nad planem działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa.

Minister cyfryzacji Anna Streżyńska. www.mc.gov.pl

Warto przypomnieć, że w styczniu 2016 r. minister cyfryzacji jednoznacznie powiedziała w wywiadzie dla "Dziennika Gazety Prawnej", że to jej resort odpowiada za cywilną politykę cyberbezpieczeństwa kraju, i zaznaczyła, że kwestie cyberbezpieczeństwa dotyczące policji, wojska i służb pozostają pod resortami za nie odpowiedzialnymi. Odpowiedzialność ministra cyfryzacji za całe krajowe cyberbezpieczeństwo i jego koordynację została zdefiniowana w ustawie o działaniach administracji.

KPRM: nowy departament

Na początku października premier Beata Szydło zapowiedziała powołanie wspomnianego już departamentu ds. cyberprzestrzeni. – *Chcąc sprostać wyzwaniom współczesności i chcąc mieć nowoczesny urząd premiera, również i ja muszę mieć zaplecze eksperckie u siebie w Kancelarii, który pozwoli mi nie tylko koordynować prace w rządzie, ale też być na bieżąco w tych zmieniających się bardzo szybko informacjach dotyczących cyberprzestrzeni* – mówiła szefowa rządu. Dodała, że nowa komórka ma być zapleczem eksperckim dla premiera i odpowiadać analizowanie i monitorowanie cyberprzestrzeni.

– *Niebezpieczeństwo dla państwa istnieje także poza jego granicami. Dziś nie potrzeba czołgów i rakiet, by zaatakować inny kraj. Wystarczy do tego komputer i odpowiednio przeszkolony człowiek* – powiedziała premier. Podkreśliła, że Polska w tej nowej rzeczywistości powinna być zdolna do obrony oraz posiadać narzędzia i ludzi zdolnych przeciwstawić się atakom z zewnątrz.

Czytaj więcej: Beata Szydło: Cyberbezpieczeństwo jest priorytetem polskiego rządu (CYBERSEC 2017)

MSWiA, Ministerstwo Rozwoju i BBN

MSWiA odpowiada za kwestię walki z cyberprzestępczością, co stanowi cywilny aspekt cyberbezpieczeństwa. W listopadzie 2016 roku utworzono Biuro do Walki z Cyberprzestępczością w Komendzie Głównej Policji, które koordynuje działania wojewódzkich wydziałów do walki z cyberprzestępczością i od tamtego czasu stale ewoluuje, dostosowując się do dynamicznie zmieniających się warunków.

Czytaj więcej: Polska policja łapie przestępców za Torem [WYWIAD]

Ministerstwo Rozwoju w ramach Planu na rzecz Odpowiedzialnego Rozwoju promuje program rozwojowy Cyberpark Enigma. Jego głównym celem jest rozwój kompetencji polskich firm i jednostek naukowo-badawczych w dziedzinie cyberbezpieczeństwa i analizy danych. Ministerstwo Rozwoju zakłada powstanie ośrodka dysponującego potencjałem pozwalającym konkurować na europejskim rynku specjalistycznych usług IT oraz stworzenie Krajowego Centrum Cyberbezpieczeństwa we współpracy z MON i MC.

Czytaj więcej: Plan Morawieckiego w cyberprzestrzeni

Biuro Bezpieczeństwa Narodowego aktywnie angażuje się w pracę nad strategicznymi aspektami cyberbezpieczeństwa, wytyczając kierunki działania wpisujące się w sytuację międzynarodową. Biuro przygotowywało wciąż obowiązującą Doktrynę Cyberbezpieczeństwa Rzeczpospolitej Polskiej oraz projekt Doktryny Bezpieczeństwa Informacyjnego

Podsumowanie

Najważniejsze dokumenty w dziedzinie cyberbezpieczeństwa opracowało lub opracowuje Ministerstwo Cyfryzacji, któremu przypisano rolę głównego koordynatora w tym obszarze. Jednak to MON dysponuje budżetem na wdrożenie dokumentów opracowanych w MC.

Cyberprzestrzeń jest na tyle szeroką domeną, że zarówno MON i MC będą miały wiele zadań do zrealizowania. Niemożliwe jest tworzenie cyberobrony bez udziału wojska. Z drugiej strony trudno sobie wyobrazić, żeby wojsko zajmowało się ściganiem pedofili w sieci, hejtu i przejawów cyberprzemocy. Dlatego konieczna jest współpraca między tymi dwoma instytucjami, które powinny zostać wsparte przez inne resorty, jak chociażby Ministerstwo Spraw Wewnętrznych i Administracji czy Ministerstwo Rozwoju. Dokładne kompetencje poszczególnych instytucji w cyberprzestrzeni zdefiniuje ustawa o krajowym systemie cyberbezpieczeństwa.

W celu zagwarantowania wysokiej ochrony systemów teleinformatycznych potrzebna jest ścisła współpraca pomiędzy różnymi instytucjami. Dotychczas była ona niewystarczająca, co stwierdził raport NIK z 2015 roku. Sytuacja ta musi ulec zmianie.

Rafał Lesiecki i Andrzej Kozłowski