Pułaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warszawa, 24.02.2016 r.

Autor: Kamil Gapiński

W kierunku systemowego cyberbezpieczeństwa – przegląd dotychczasowych strategii i wnioski dla nowego otwarcia

23 lutego Ministerstwo Cyfryzacji opublikowało Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej, dokument programowy zapowiadający prace legislacyjne resortu cyfryzacji w zakresie bezpieczeństwa cywilnych systemów teleinformatycznej infrastruktury krytycznej. Jest to pierwszy projekt obecnego rządu w obszarze cyberbezpieczeństwa, choć podobne inicjatywy legislacyjne i strategiczne pojawiały się już wcześniej. Należy odnotować jednak fakt, iż dotychczasowe dokumenty opracowane przez administrację nie były prawnie wiążące. Nie nadawały one prawnych kompetencji odpowiednim jednostkom państwowym, przez co niemożliwa była ich pełna implementacja (jedynym terminem wprowadzonym do polskiego ustawodawstwa jest „cyberprzestrzeń", jej definicja znajduje się w Ustawie z dnia 27 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej). Problem nieuregulowania prawnego kwestii systemu cyberbezpieczeństwa przez lata był zarówno jednym z najważniejszych wyzwań, jak i zaniedbań w tym obszarze. Prowadził do rozmycia kompetencyjnego, braku podmiotu koordynującego oraz paraliżów decyzyjnych, jak w przypadku budowania potencjału cybernetycznego w Siłach Zbrojnych RP. Ponadto, zdaniem ekspertów, w ochronę cyberprzestrzeni w Polsce zaangażowanych jest zbyt wielu aktorów, nie do końca uświadomionych o swoich uprawnieniach. Opublikowany dokument Ministerstwa Cyfryzacji

> *Zapowiedziane przez Ministerstwo Cyfryzacji stanowisko podsekretarza stanu ds. cyberbezpieczeństwa musi zostać obsadzone przez osobę rozumiejącą nie tylko zagadnienia bezpieczeństwa teleinformatycznego w sensie technicznym, ale posiadającą szerokie rozeznanie w problemach systemowych i organizacyjno-prawnych.*

również posiada charakter „strategiczny", ale docelowo jest zapowiedzią zmian legislacyjnych porządkujących system ochrony cyberprzestrzeni w Polsce.

Przegląd cyberstrategii

Do czasu pojawienia się Założeń obowiązującym dokumentem programowym była Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej przyjęta na drodze uchwały przez Radę Ministrów w czerwcu 2013 r. Nie jest ona zatem aktem powszechnie obowiązującym, jej rekomendacje dotyczą wyłącznie administracji państwowej. Polityka została opracowana wspólnie przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego w oparciu o doświadczenia Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL działające w ramach ABW) oraz wnioski Komitetu Stałego Rady Ministrów dotyczące propozycji zawartych w Rządowym programie ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia. Polityka jest dokumentem strategicznym, wyznaczającym kierunki rozwiązań prawno-organizacyjnych w zakresie ochrony cyberprzestrzeni przez administrację państwową. Celem strategicznym Polityki jest „osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa". Dokument obejmuje m.in. „systemy administracji rządowej, organy władzy ustawodawczej, władze sądowniczą, samorząd terytorialny, a także systemy strategiczne z punktu widzenia bezpieczeństwa państwa" z wyłączeniem niejawnych systemów teleinformatycznych. Jest równocześnie deklaracją uczestnictwa przedstawicieli rządu w zapewnianiu bezpieczeństwa zasobów informacyjnych państwa i jego obywateli. Koordynację realizacji postanowień Polityki zapewnia minister właściwy ds. informatyzacji.

Dokument został przyjęty sceptycznie. Eksperci zarzucają mu niski poziom merytoryczny, brak rzetelnej analizy zagrożeń i zasobów oraz brak wykorzystania „dobrych praktyk" przyjętych międzynarodowo m.in. przez Europejska Agencję ds. Bezpieczeństwa Sieci i Informacji (ang. European Union Agency for Network and Information Security, ENISA). Polityka nie precyzuje również kwestii finansowania procesu wdrażania zabezpieczeń. Enigmatycznym pozostaje także niedookreślony „akceptowalny poziom bezpieczeństwa", potwierdzający niejako niewystarczające przygotowanie organizacyjne i merytoryczne zespołu zadaniowego, po części wynikające z niedofinansowania przedsięwzięcia. Pomimo obowiązku realizacji postanowień Polityki proces ten faktycznie nie zaistniał, na co wskazują

wyniki kontroli Najwyższej Izby Kontroli z czerwca 2015 roku (Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP).

Istotnym dokumentem strategicznym obejmującym zbliżone do Polityki cele, jest Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, przyjęta i podpisana przez Prezydenta Rzeczypospolitej w styczniu 2015 roku. Opracowany przez Biuro Bezpieczeństwa Narodowego dokument podobnie jak Polityka mieści się w kategorii opracowań strategicznych i zgodnie z założeniem autorów powinien być traktowany jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony. Doktryna powstała na drodze konsultacji z sektorem prywatnym i pozarządowym, stanowi ponadto dokument wykonawczy do Strategii Bezpieczeństwa Narodowego RP. Efektem prac Biura i konsultacji zewnętrznych jest kilkudziesięciostronicowe opracowanie opisujące w punktach cele strategiczne w dziedzinie cyberbezpieczeństwa, zagrożenia wewnętrzne i zewnętrzne, koncepcję zadań operacyjnych oraz rolę i charakter podmiotów uczestniczących. Doktryna stanowi istotny punkt wyjścia realizacji działań strategicznych, jak i określa wizję współpracy poszczególnych podmiotów w zakresie cyberbezpieczeństwa. Przedstawia ona ponadto katalog najważniejszych zagrożeń i wyzwań. Podstawowym problemem Doktryny jest jego wyłącznie koncepcyjny i strategiczny charakter, choć jego niedoskonałość tkwi także w braku konkretnych rekomendacji instytucjonalnych, wytycznych co do źródeł finansowania systemu cyberbezpieczeństwa, a także w nieprecyzyjnym i niespójnym sformułowaniu kwestii tzw. zdolności ofensywnych i roli Sił Zbrojnych RP w systemie. Ponadto, Doktryna wspominając o partnerstwie publiczno-prywatnym, omija konkretne sposoby realizacji takiego przedsięwzięcia, skupiając się wyłącznie na płaszczyźnie zadaniowej. Pomimo widocznych braków i miejscami nazbyt ogólnych wniosków, dokument jest wartościową pozycją z punktu widzenia koncepcji systemowej. Jest również dowodem na wyraźny progres merytoryczny oraz większą rzetelność w zakresie identyfikacji i rozumienia problemu ochrony cyberprzestrzeni.

Warto przy tym wspomnieć o innym dokumencie Biura Bezpieczeństwa Narodowego, pośrednio stanowiącym uzupełnienie dla „Doktryny Cyberbezpieczeństwa RP", a mianowicie Doktrynie Bezpieczeństwa Informacyjnego RP. Projekt tego dokumentu ukazał się w lipcu 2015 r. i jest odpowiedzią na wyzwania związane z zagrożeniami hybrydowymi i wojną informacyjną. Biorąc pod uwagę zmiany strukturalne w Biurze Bezpieczeństwa

Narodowego, prace nad jego dokończeniem stoją pod znakiem zapytania. Możliwe jednak, że z doświadczeń poprzedników w tym obszarze skorzysta nowopowstały zespół ds. cyberbezpieczeństwa.

Prawo a cyberbezpieczeństwo

Sprawnie działający system cyberbezpieczeństwa jest uzależniony od prawidłowego funkcjonowania infrastruktury krytycznej (IK). Istotna w tym kontekście jest Ustawa z dnia 26 kwietnia 2007 r o zarządzaniu kryzysowym, która jasno definiuje IK i należące do niej systemy (m.in. zaopatrzenia w energię i paliwa, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej). Tym samym, należy stwierdzić, że wszystkie systemy teleinformatyczne zapewniające ciągłość infrastruktury krytycznej stanowią nadrzędny przedmiot ochrony w ramach systemu cyberbezpieczeństwa. Jak dowodzą liczne kampanie ukierunkowane m.in. na sektor energetyczny (np. elektrownie) czy transportowy (np. systemy komputerowe na lotniskach), ochrona systemów IK jest kluczowym wyzwaniem dla bezpieczeństwa państwa. Zaniedbania w tym obszarze mogą prowadzić do katastrofalnych skutków, nie tylko w wymiarze strat finansowych, ale również fizycznych.

Wiele wniosków dla ochrony cyberprzestrzeni płynie z Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dokumenty te definiują „system teleinformatyczny" w odniesieniu do, odpowiednio: usług świadczonych drogą internetową oraz klasyfikacji, ochrony i przetwarzania „informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne".

Ekspertyzy i raporty

Analizując zagadnienie cybebezpieczeństwa w Polsce warto zwrócić uwagę na wartościowe opracowania i ekspertyzy niezależne, będące najczęściej zbiorem „dobrych praktyk", rekomendacji i propozycji zmian. W pierwszej kolejności należy tu wymienić kompleksowy raport Instytutu Kościuszki Bezpieczeństwo infrastruktury krytycznej – wymiar teleinformatyczny i ekspertyzę Naukowej i Akademickiej Sieci Komputerowej System

bezpieczeństwa cyberprzestrzeni RP przygotowaną dla Ministerstwa Administracji i Cyfryzacji. Nie do przecenienia jest ponadto wspomniany raport Najwyższej Izby Kontroli Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, sprawdzający zarządzanie ryzykiem zagrożeń w cyberprzestrzeni przez administrację państwową. Przydatne dla bardziej wnikliwej analizy bieżących wyzwań i trendów z zakresu bezpieczeństwa teleinformatycznego są również coroczne raporty CERT.GOV.PL Raport o stanie bezpieczeństwa cyberprzestrzeni RP. Ważny wkład w dyskusję o międzynarodowej współpracy w zakresie cyberbezpieczeństwa może także stanowić przygotowywana przez Fundację im. Kazimierza Pułaskiego Analiza prawna działań w cyberprzestrzeni.

Wnioski i rekomendacje

1. Program cyberbezpieczeństwa na najbliższe lata powinien zakładać powstanie ustawy regulującej system ochrony cyberprzestrzeni w Polsce.

2. Ustawa musi w sposób precyzyjny określać: a) ramy instytucjonalne, b) podział kompetencyjny podmiotów zaangażowanych, c) jednostkę(i) koordynującą(e). Warto w tych działaniach uwzględnić wnioski z ekspertyzy System bezpieczeństwa cyberprzestrzeni RP. Zważywszy na ograniczenia strukturalne administracji, najbardziej odpowiednie wydaje się zastosowanie modelu scentralizowanego. Podobny model jest proponowany w Założeniach, gdzie jednostką koordynującą na poziomie strategicznym i operacyjnym jest Ministerstwo Cyfryzacji.

3. Należy rozwinąć problematykę partnerstwa publiczno-prywatnego. Zadania i możliwości współpracy sektora publicznego z biznesem zostały opracowane w dokumentach strategicznych. Obecnie nadszedł czas utworzenia i usankcjonowania specjalistycznej grupy kontaktowej umożliwiającej rozpoczęcie owej współpracy.

4. Ważnym jest, by działania w sferze cywilnej nie wchodziły w kompetencje zadań Ministra Obrony. Niezbędna jest natomiast wymiana doświadczeń oraz informacji. Racjonalny w tym względzie wydaje się zatem postulat Ministerstwa Cyfryzacji o powołaniu Narodowego Centrum Cyberbezpieczeństwa.

5. Zapowiedziane przez Ministerstwo Cyfryzacji stanowisko podsekretarza stanu ds. cyberbezpieczeństwa musi zostać obsadzone przez osobę rozumiejącą nie tylko zagadnienia bezpieczeństwa teleinformatycznego w sensie technicznym, ale posiadającą

szerokie rozeznanie w problemach systemowych i organizacyjno-prawnych. Idealnym kandydatem na to stanowisko wydaje się niezależny ekspert współpracujący zarówno z administracją, jak i sektorem prywatnym i organizacjami pozarządowymi.

Autor: *Kamil Gapiński, Fundacja Pułaskiego, Koordynator Programu Cyberbezpieczeństwa*

Fundacja im. Kazimierza Pułaskiego jest niezależnym think tankiem specjalizującym się w polityce zagranicznej i bezpieczeństwie międzynarodowym. Głównym obszarem aktywności Fundacji Pułaskiego jest dostarczanie analiz opisujących i wyjaśniających wydarzenia międzynarodowe, identyfikujących trendy w środowisku międzynarodowym oraz zawierających implementowalne rekomendacje i rozwiązania dla decydentów rządowych i sektora prywatnego.

Fundacja w swoich badaniach koncentruje się głównie na dwóch obszarach geograficznych: transatlantyckim oraz Rosji i przestrzeni postsowieckiej. Przedmiotem zainteresowania Fundacji są przede wszystkim bezpieczeństwo, zarówno w rozumieniu tradycyjnym jak i w jego pozamilitarnych wymiarach, a także przemiany polityczne oraz procesy ekonomiczne i społeczne mogące mieć konsekwencje dla Polski i Unii Europejskiej.

Fundacja Pułaskiego skupia ponad 40 ekspertów i jest wydawcą analiz w formatach: „Stanowiska Pułaskiego", „Komentarza Międzynarodowego Pułaskiego" oraz „Raportu Pułaskiego". Fundacja wydaje też „Informator Pułaskiego", będący zestawieniem nadchodzących konferencji i spotkań eksperckich dotyczących polityki międzynarodowej. Eksperci Fundacji regularnie współpracują z mediami.

Fundacja przyznaje nagrodę "Rycerz Wolności" dla wybitnych postaci, które przyczyniają się do promocji wartości przyświecających generałowi Kazimierzowi Pułaskiemu tj. wolności, sprawiedliwości oraz demokracji. Do dziś nagrodą uhonorowani zostali m.in.: profesor Władysław Bartoszewski, profesor Norman Davies, Aleksander Milinkiewicz, prezydent Lech Wałęsa, prezydent Aleksander Kwaśniewski, prezydent Valdas Adamkus, Javier Solana, Bernard Kouchner i Richard Lugar.

Fundacja Pułaskiego posiada status organizacji partnerskiej Rady Europy.

www.pulaski.pl