Łukasz Pirożek*

Partnerstwo przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych w zapewnieniu cyberbezpieczeństwa

Spis treści

I. Wprowadzenie
II. Cyberprzestrzeń jako nowa płaszczyzna aktywności ludzkiej
III. Cyberbezpieczeństwo jako kategoria interesu publicznego
IV. Status przedsiębiorców dostarczający infrastrukturę i usługi cyfrowe
V. Status podmiotów publicznych odpowiedzialnych za infrastrukturę
VI. Partnerstwo przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych
VII. Zakończenie

Streszczenie

Artykuł dotyczy analizy prawnej partnerstwa przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych w zakresie cyberbezpieczeństwa na gruncie prawa polskiego. Rozważana jest kwestia współdziałania przedsiębiorców z sektora prywatnego dostarczających infrastrukturę oraz usługi cyfrowe, jak również podmiotów publicznych odpowiedzialnych za cyberbezpieczeństwo na podstawie ustawy o krajowym systemie cyberbezpieczeństwa wdrażającej do polskiego systemu prawa dyrektywę NIS.

Słowa kluczowe: publiczno-prywatne partnerstwo; cyberprzestrzeń; cyberbezpieczeństwo; infrastruktura cyfrowa; usługi cyfrowe; CSIRT, incydent.

JEL: K23, K24

I. Wprowadzenie

Partnerstwo przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych w zapewnieniu cyberbezpieczeństwa jest strategicznym modelem współpracy w zakresie gwarantowania cyberbezpieczeństwa (Carr, 2016, s. 4). Podmioty z sektora prywatnego prowadzące działalność gospodarczą w zakresie dostarczania infrastruktury oraz usług cyfrowych

* Radca prawny w EXATEL S.A., doktorant w INP PAN.

mają szczególne miejsce w cyberprzestrzeni, w tym w obszarze zapewniania jej bezpieczeństwa. Genezą takiego stanu rzeczy jest utrata przez państwo, na skutek procesów globalizacyjnych oraz prywatyzacyjnych (Carr, 2016, s. 46), monopolu na budowę i zarządzanie sieciami telekomunikacyjnymi, świadczenie usług telekomunikacyjnych i teleinformatycznych oraz inicjatywy w zakresie rozwoju nowych technologii (Wojdyło, 2014). Z tego powodu przedsiębiorcy z sektora prywatnego są dominującymi zróżnicowanymi podmiotami tworzącymi cyberprzestrzeń, które realizują w przeważającej mierze cele biznesowe w oparciu o rozwiązania telekomunikacyjne oraz teleinformatyczne. Wyróżnia się wśród nich przedsiębiorców dostarczających podstawową infrastrukturę zapewniającą funkcjonowanie Internetu lub prywatnych sieci, np. OT (*Operation Technology*), które to sieci są często uznawane za infrastrukturę krytyczną dla funkcjonowania państwa, oraz przedsiębiorców świadczących usługi cyfrowe, np. dostawców platform handlowych, portali społecznościowych, hostingu, wyszukiwarek internetowych, podmiotów świadczących usługi OTT (*Over-The-Top*). Z uwagi na powyższą rolę tych przedsiębiorców w cyberprzestrzeni, w tym poprzez decydowanie o standardach technicznych oraz procedurach bezpieczeństwa, zajmują oni kluczową pozycję dla zapewnienia bezpieczeństwa infrastruktury i usług cyfrowych (Asghari, 2016, s. 2–3, 25–26).

Przedsiębiorcy z sektora prywatnego w swojej działalności kierują się racjonalnością ekonomiczną w oparciu o zasady wolnorynkowe, tj. maksymalizacją korzyści i minimalizacją kosztów, szybkością i skutecznością (efektywnością) ekonomicznego działania (Stasikowski, 2019, s. XI–XXIII). Powyższa logika działania przedsiębiorców wpływa na ich zdolność oraz umiejętność w zakresie zapewnienia cyberbezpieczeństwa (Carr, 2016, s. 43–49).

Natomiast, podmioty z sektora publicznego działające w imieniu państwa oraz na podstawie norm prawnych są odpowiedzialne za zapewnianie cyberbezpieczeństwa w interesie publicznym. Bezpieczeństwo jest podstawową wartością i dobrem mającym na celu zaspokojenie pierwotnych potrzeb zbiorowości ludzkiej. Państwo ma szczególną rolę w zapewnieniu bezpieczeństwa w cyberprzestrzeni. Rolę tę realizuje za pośrednictwem działania podmiotów publicznych, w tym organów administracji państwowej, w ramach zadania publicznego określonego jako bezpieczeństwo i porządek publiczny (Stasikowski, 2019, s. 42–45). Podmioty publiczne, w odróżnieniu od podmiotów prywatnych, realizują powyższe zadanie publiczne, kierując się logiką racjonalności dobra wspólnego prowadzoną w interesie publicznym (Stasikowski, 2019, s. VII).

Przedmiotem niniejszego artykułu jest analiza prawna modelu partnerstwa (współdziałania) podmiotów prywatnych, tj.: przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych realizujących zadania publiczne w zakresie cyberbezpieczeństwa, w celu zagwarantowania bezpieczeństwa cybernetycznego. Przedmiotowe rozważania oparte są na ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU 2018, poz. 1560) (dalej: uksc) wdrażającej Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2016.194.1) (dalej: dyrektywa NIS).

II. Cyberprzestrzeń jako nowa płaszczyzna aktywności ludzkiej

Rola przedsiębiorców z sektora prywatnego oraz podmiotów z sektora publicznego w zapewnieniu cyberbezpieczeństwa wynika z rozwoju technologii informacyjnych i komunikacyjnych.

Rozwój ten spowodował wyodrębnienie się nowej płaszczyzny aktywności ludzkiej, w której informacja przetwarzana jest na ogromną skalę za pomocą technologii informatycznych. Informacja jest definiowana jako wiedza dotycząca obiektów, takich jak fakty, zdarzenia, przedmioty, procesy lub idee, która w określonym kontekście ma określone znaczenie (Lisiak-Felicka i Szmit, 2016, s. 26). Informacja stanowi dobro społeczne o podstawowym znaczeniu dla zapewnienia funkcjonowania społeczeństw rozwiniętych. Integracja przetwarzanych informacji w przestrzeni cybernetycznej prowadzi do powstania i rozwoju nowej płaszczyzny aktywności ludzkiej, która jest swoistą instytucją społeczną będącą bazą dla budowania społeczeństwa informacyjnego (Banasiński, 2018, s. 4). Ta nowa płaszczyzna aktywności ludzkiej określana jest mianem cyberprzestrzeni i jest to pojęcie niedookreślone, któremu przypisywane są różne znaczenia. Termin ten po raz pierwszy został użyty przez Wiliama Gibsona w 1984 r. w powieści „Neuromancer" jako „konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach" (Banasiński, 2018a, s. 23; Berdel-Dudzińska, 2012, s. 26). W teorii prawa międzynarodowego przestrzeń cybernetyczna jest określana jako międzynarodowa przestrzeń, obok: Antarktydy, przestrzeni kosmicznej i pełnych mórz (Menthe, 1998, s. 70). Cyberprzestrzeń jest też wymieniana jako piąty wymiar zapewniania bezpieczeństwa (*fifth domain*) po lądzie, morzu, powietrzu i kosmosie (Trąbiński, 2017, s. 70).

W doktrynie wskazuje się, iż cyberprzestrzeń cechuje się stałym rozwojem, potencjalnym brakiem granic oraz dostępnością dla milionów użytkowników. Ma charakter globalny, zdecentralizowany, ciągle zmienia swoje właściwości i nie jest stabilna. Jest bardziej plastyczna niż rzeczywistość. Nie ma geograficznej lokalizacji i jest dostępna dla każdego, w każdym miejscu na świecie przez dostęp do Internetu. W większości przypadków jest zupełnie nieuregulowana, dlatego też podatna jest na ataki i wrogie działania z zewnątrz (Trąbiński, 2017, s. 70–71).

Definicja legalna cyberprzestrzeni została wprowadzona do polskiego systemu prawnego w 2011 roku[1]. Występuje w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (DzU 2017, poz. 1932 t.j. ze zm.) (dalej: ustawa o stanie wojennym) oraz w ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym (DzU 2017, poz. 1928 t.j. ze zm.) (dalej: ustawa o stanie wyjątkowym). Zdefiniowana jest jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Natomiast, system teleinformatyczny występujący w definicji cyberprzestrzeni oznacza zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[2]. Na podstawie powyższego stwierdza się, iż definicja cyberprzestrzeni jest pojęciowo bardzo szeroka, gdyż jej istotą są elementy materialne, które tworzą systemy teleinformatyczne składające się z urządzeń informatycznych (*hardware*) i oprogramowania (*software*) oraz elementy niematerialne (komponenty społeczne), tj. interakcja ludzi z systemami

[1] Definicja cyberprzestrzeni została wprowadzona ustawą z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (DzU 2011, Nr 1323, poz. 222).

[2] Art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (DzU 2014, poz. 1114; 2016, poz. 352).

teleinformatycznymi i relacje pomiędzy ludźmi za pomocą tych systemów (infrastruktury technicznej) (Banasiński, 2018a, s. 25). Dodatkowo, należy podkreślić, iż kluczowym substratem cyberprzestrzeni są dane (*content*) przesyłane lub gromadzone za pomocą sieci i systemów teleinformatycznych (Szpor, 2017, s. 6).

Z uwagi na powyższe, należy stwierdzić, iż szerokie rozumienie cyberprzestrzeni jest korzystne dla zapewnienia odpowiedniego poziomu jej bezpieczeństwa. Szeroka definicja legalna cyberprzestrzeni umożliwia stosowanie do niej różnych regulacji prawnych dotyczących aspektów bezpieczeństwa, w szczególności uksc. Takie podejście jest dopuszczalne, gdyż ani dyrektywa NIS ani uksc nie zawierają definicji cyberprzestrzeni.

III. Cyberbezpieczeństwa jako kategoria interesu publicznego

Doniosłe znaczenie cyberprzestrzeni w wielu aspektach życia społecznego i gospodarczego skutkuje narastającymi zagrożeniami, które mają wpływ na funkcjonowanie społeczeństw, gospodarek oraz poszczególnych państw. Zagrożenia w cyberprzestrzeni mają zróżnicowany charakter począwszy od działań przestępczych (np. *phishing, ramsomware*), zakłóceń funkcjonowania sieci i usług łączności elektronicznych (Rojszczak, 2018, s. 210), np. ataki typu DDoS (*Distributed Denial of Service Attack*), występowanie bezprawnych treści (np. kwerendy SQL-olwe mające na celu przejęcie roli administratora bazy danych, wirusy, trojany) (Polański, 2019, s. 258), poprzez terroryzm (np. ataki typuAdvanced Persistent Threat/Targeted Persistent Threat, APT/TPT) (Chmielewski i Waćkowski, 2018, s. 103), szpiegostwo, a kończąc na działaniach wojennych. Odpowiedzią na te zagrożenia jest zapewnienie bezpieczeństwa w cyberprzestrzeni określane mianem cyberbezpieczeństwa. Pojęcie „cyberbezpieczeństwa" jest definiowane różnorodnie zarówno w wypowiedziach doktryny, w dokumentach programowych, dokumentach normalizacyjnych np. w międzynarodowych normach ISO, jak i w przepisach prawnych. W doktrynie wskazuje się, iż termin „„ ma różne znaczenie dla różnych odbiorców: dla indywidualnych użytkowników, w tym konsumentów ma znaczenie jako poczucie bezpieczeństwa, ochrony danych osobowych oraz prywatności; dla przedsiębiorców to dostępność i ciągłość funkcji biznesowych oraz ochrona poufnych danych. Z kolei dla państw to ochrona obywateli, przedsiębiorstw, infrastruktury krytycznej oraz państwowych zasobów teleinformatycznych (Ganczar, 2017, s. 84). W piśmiennictwie wyróżnia się cyberbezpieczeństwo w znaczeniu wąskim (*sensu stricto*) jako zapewnienie bezpieczeństwa sieci komputerowych w cyberprzestrzeni oraz cyberbezpieczeństwo w znaczeniu szerokim (*sensu largo*) jako zapewnienie „bezpieczeństwa dzięki sieci", czyli wykorzystanie sieci komputerowych w celu zapobiegnięcia zagrożeniom również poza cyberprzestrzenią (Niezgódka, 2017, s. 232). C. Banasiński definiuje cyberbezpieczeństwo jako „sposób wolnego od zakłóceń gromadzenia, przetwarzania i wymiany informacji utrwalonych i przetwarzanych w sposób cyfrowy", co pozwala odróżnić cyberbezpieczeństwo od bezpieczeństwa informacyjnego" (Banasiński, 2018a, s. 27–33).

Wskazuje się również, iż cyberbezpieczeństwo stanowi klauzulę generalną dotyczącą działań państwa podejmowanych w interesie publicznym. Wyróżnia się również twierdzenie, iż cyberbezpieczeństwo stanowi nową kategorię globalnych dóbr publicznych (*global public goods*), czyli dóbr niepodlegających rywalizacji w zakresie wykorzystania, których użycie nie zmniejsza ilości dostępnej dla innych, a ich zasięg jest globalny (Banasiński, 2018a, s. 25).

Istotne dla praktyki definicje cyberbezpieczeństwa zawarte są dokumentach normalizacyjnych. Międzynarodowa norma ISO/IEC 27032 zawiera definicję cyberbezpieczeństwa opartą na atrybutach bezpieczeństwa informacji, tj. jako zachowanie poufności, dostępności i integralności informacji w cyberprzestrzeni. Pozostałe atrybuty bezpieczeństwa, które można odnieść do cyberbezpieczeństwa wynikające z norm ISO/IEC to autentyczność, rozliczalność oraz niezawodność.

Dyrektywa NIS nie zawiera definicji cyberbezpieczeństwa. Posługuje się terminem „bezpieczeństwo sieci i systemów informatycznych". Legalna definicja cyberbezpieczeństwa zawarta jest w uksc, która to definicja jest zbliżona do terminu „bezpieczeństwo sieci i systemów informatycznych" zawartych w dyrektywie NIS. Art. 2 pkt 4) uksc stanowi, iż cyberbezpieczeństwo oznacza „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzania danych lub związanych z nimi usług oferowanych przez te systemy".

W aspekcie partnerstwa przedsiębiorców z sektora prywatnego oraz podmiotów z sektora publicznego, termin cyberbezpieczeństwo powinien być identyfikowany z kategorią interesu publicznego (dobra wspólnego). Powyższa kwalifikacja cyberbezpieczeństwa jest uzasadniona ewoluującym, tj. zmiennym w czasie, charakterem klauzuli interesu publicznego, która uwzględnia potrzeby społeczeństwa aktualnie funkcjonującego w cyberprzestrzeni (Żurawik, Hausner, Niewiadomski i Wróbel, 2013, s. 415). Cyberbezpieczeństwo jako kategoria interesu publicznego stanowi podstawę dla współpracy podmiotów z sektora prywatnego oraz podmiotów z sektora publicznego, gdyż poziom bezpieczeństwa w cyberprzestrzeni leży w interesie obu stron partnerstwa. Przedsiębiorcy mają interes w przeciwdziałaniu zagrożeniom występujących w cyberprzestrzeni skierowanym wobec nich, takich jak: cyberprzestępstwa, przerwanie ciągłości działania, wyciek danych czy utrata renomy, natomiast podmioty z sektora publicznego, oprócz zapewnienia bezpieczeństwa usług publicznych, muszą zajmować się realizacją podstawowych funkcji państwa, jak zapewnienie bezpieczeństwa i porządku publicznego (Żurawik, Hausner, Niewiadomski i Wróbel, 2013, s. 414).

IV. Status przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe

Przedsiębiorcy dostarczający infrastrukturę oraz usługi cyfrowe stanowią zróżnicowaną grupę podmiotów tworzących cyberprzestrzeń. Składają się na nie podmioty zapewniające funkcjonowanie systemów sieciowych od warstwy fizycznej sieci do warstwy aplikacji[3]. Przedsiębiorcy ci poprzez zapewnianie infrastruktury oraz świadczenie usług cyfrowych umożliwiają działanie Internetu oraz sieci prywatnych, w tym infrastruktury krytycznej niezbędnej do funkcjonowania gospodarki i państwa. Dlatego też podmioty te mają zasadniczy wpływ na poziom bezpieczeństwa w cyberprzestrzeni.

Ustawa o krajowym systemie cyberbezpieczeństwa obejmuje regulacją wybraną grupę przedsiębiorców z sektora prywatnego dostarczających infrastrukturę oraz usługi cyfrowe mających znaczenia dla zapewnienia cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją tej ustawy, obok organów administracyjnych, podmiotów publicznych, akredytowanych jednostek oceniających oraz podmiotów świadczących usługi w zakresie cyberbezpieczeństwa, wchodzą w skład pierwszej

[3] J.M. Chmielewski i K. Waćkowski wyróżniają siedem warstw podziału systemów sieciowych, tj. warstwy fizyczną, łącza danych, sieciową, transportową, sesji, prezentacji oraz aplikacji (zob. Chmielewski i Waćkowski, 2018, s. 83).

w Polsce struktury organizacyjnej systemu cyberbezpieczeństwa, którą ustanawia uksc. Jej zakres podmiotowy wynika z rozstrzygnięcia prawodawcy unijnego zawartego w dyrektywie NIS oraz prawodawcy krajowego określonego w uksc.

Zgodnie z uksc operatorami usługi kluczowej w zakresie infrastruktury cyfrowej są przedsiębiorcy mający jednostkę organizacyjną na terenie Polski, scharakteryzowani w załączniku nr 1 do uksc, wobec których organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Zgodnie z załącznikiem nr 1 do ustawy, są to: przedsiębiorcy, którzy świadczą usługi DNS, przedsiębiorcy zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD) oraz przedsiębiorcy prowadzący punkt wymiany ruchu internetowego (IXP). W doktrynie wskazuje się, że za operatorów usług kluczowych powinny być uznawane podmioty, które świadczą usługi uznane za krytyczne dla państwa oraz których może dotyczyć skutek kinetyczny, czyli sytuacja, gdy zaistnienie incydentu u operatora usługi kluczowej skutkuje zakłóceniem u jego usługobiorców (Balcerzak i Durbajło, 2017, s. 53).

Przedsiębiorcy świadczący usługi DNS (*Domain Name System*) zajmują się rejestrowaniem, nadzorem oraz utrzymaniem systemu nazw domen internetowych. Funkcją systemu nazw domen jest zamiana nazw i adresów reprezentowanych przez domeny internetowe na powiązane z nimi adresy IP, które określają logiczną lokalizację w sieci danego komputera lub innego urządzenia (Chrzanowski i Kruk, 2012, s. 83). Usługi DNS są usługą krytyczną dla działania Internetu, gdyż jeżeli przestaje działać system nazw domenowych, przestają działać wszystkie usługi sieciowe, w tym poczta elektroniczna czy sieć WWW (Chrzanowski i Kruk, 2012, s. 88). DNS jest usługą otwartą, dostępną dla każdego, co skutkuje licznymi działaniami zakłócającymi funkcjonowanie cyberprzestrzeni, np. podszywaniem się pod nazwę domenową, zatruwaniem podręcznego serwera domenowego (*cache poisoning*) czy powodowaniem ataków typu rozproszonej odmowy usługi (*Distributed Denial of Service*, DDoS) (Chrzanowski i Kruk, 2012, s. 89). Zbliżoną do usługi DNS jest usługa zarządzania rejestracją nazw domen internetowych w ramach domeny najwyższego poziomu (Top-Level Domain, TLD). W Polsce usługi rejestracji i utrzymywania domeny najwyższego rzędu (domena krajowa .pl) prowadzi Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.

Wobec powyższego, ze względu na wagę dla funkcjonowania Internetu, przedsiębiorcy świadczący usługi DNS i TLD są zasadnie uznani za operatorów usługi krytycznej i objęci regulacją uksc, gdyż poziom bezpieczeństwa gwarantowany przez tych przedsiębiorców ma krytyczne znaczenie dla bezpieczeństwa wszystkich użytkowników Internetu.

Kolejni przedsiębiorcy zakwalifikowani jako operatorzy usług krytycznych to podmioty prowadzące punkt wymiany ruchu internetowego (*Internet Exchange Point*, IXP). Punkt wymiany ruchu umożliwia wymianę ruchu IP (*Internet Protocol*) pomiędzy różnymi podmiotami, co pozwala na działania usług internetowych. Ruch pomiędzy sieciami jest zapewniany przez wykorzystanie protokołów IP w formie *peeringu* i tranzytu. Peering IP to bezpłatna i bezpośrednia wymiana ruchu pomiędzy połączonymi sieciami (Piątek, 2011, s. 113). Natomiast, tranzyt IP polega na płatnym przekazywaniu ruchu do sieci innego podmiotu lub do ogólnoświatowych zasobów Internetu poprzez sieć operatora tranzytującego (Piątek, 2011, s. 114). Niezakłócona wymiana ruchu internetowego stanowi podstawowy mechanizm umożliwiający korzystanie z Internetu przez użytkowników. Przedsiębiorcy prowadzący punkt wymiany ruchu są podatni na ataki typu DDoS

skutkujące obciążeniem wolnych zasobów uniemożliwiającym działanie punktu wymiany ruchu czy atakami typu IP *snoofing*, polegając na przejęciu ruchu sieciowego. Dlatego też, bezpieczeństwo przedsiębiorców prowadzących punkt wymiany ruchu internetowego ma szczególne znaczenie dla prawidłowego działania Internetu.

Ustawa o krajowym systemie cyberbezpieczeństwa obejmuje regulacją również dostawców usług cyfrowych, czyli przedsiębiorców świadczących usługi cyfrowe. Usługa cyfrowa, według art. 2 pkt 15) uksc, to usługa świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (DzU 2017, poz. 1219; 2018, poz. 650). Rodzaje usług cyfrowych zostały określone w załącznik nr 2 do ustawy, w którym wymieniono dostawców świadczących: internetowe platformy handlowe, usługi przetwarzania w chmurze oraz wyszukiwarki internetowe. W pierwotnym projekcie dyrektywy NIS, oprócz powyższych dostawców usług cyfrowych, występowali dostawcy portali społecznościowych. W doktrynie podkreśla się, że wyłączenie spod regulacji portali społecznościowych zmniejsza rolę dyrektywy NIS w zapewnieniu cyberbezpieczeństwa (Szpor, 2017, s. 8). Obecnie na gruncie uksc, w przypadku wystąpienia incydentu u dostawcy portalu społecznościowego jego zgłoszenie do CSIRT NASK może nastąpić wyłącznie na zasadzie dobrowolności.

Należy zauważyć, iż katalog dostawców usług cyfrowych objętych regulacją uksc ma charakter wybiórczy. Nie obejmuje on swoim zakresem podmiotów świadczących usługi społeczeństwa informacyjnego w rozumieniu dyrektywy 2015/1535[4] oraz usługi łączności elektronicznej zdefiniowanych w dyrektywie nr 2018/1972 ustanawiającej Europejski kodeks łączności elektronicznej[5], tj. usługi OTT, usługi łączności maszyna-maszyna (M2M), które są dostarczane za pomocą Internetu (Siwicki, 2019, s. 16).

Dodatkowo, interpretacja opisu usług: internetowych platform handlowych, usług przetwarzania w chmurze oraz wyszukiwarek internetowych, zawartych w załączniku nr 2 do uksc może powodować trudności dotyczące kwalifikacji danego przedsiębiorcy w świetle tej ustawy. Wynika to ze złożonego charakteru poszczególnych usług oraz ze względu na ograniczone wymogi regulacyjne wobec tych dostawców w porównaniu z wymogami wobec operatorów usług kluczowych. Z motywu 49 oraz z art. 16 ust. 10 dyrektywy NIS wynika, iż państwa członkowskie nie mogą nakładać na dostawców usług cyfrowych jakichkolwiek dalszych wymogów dotyczących bezpieczeństwa lub zgłaszania incydentów niż zawarte w dyrektywie NIS (Siwicki, 2019, s. 16). Skutkować to może interpretacją zawężającą krąg dostawców usług cyfrowych dostarczających usługi opisane w załączniku nr 2 do uksc.

Ponadto, należy podkreślić, iż uksc nie obejmuje *expressis verbis* regulacją przedsiębiorców udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej, określonych zgodnie z polską ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (DzU 2019, poz. 2460 t.j. ze zm.) (dalej: pt) jako przedsiębiorcy telekomunikacyjni. Podmioty te podlegają pod regulację branżową dotyczącą bezpieczeństwa sieci i usług określoną w art. 175 i n. pt. Na mocy art. 81 pkt 1) lit. a) uksc, ustawodawca włącza pośrednio te podmioty do krajowego systemu cyberbezpieczeństwa poprzez nałożenie obowiązku na Prezesa UKE

[4] Dyrektywa 2015/1535 Parlamentu Europejskiego i Rady (UE) z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie).

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona), Dz.U.UE.L.2018.321.36.

w zakresie przekazywania właściwemu CSIRT informacji uzyskanych od przedsiębiorców telekomunikacyjnych dotyczących naruszenia bezpieczeństwa lub integralności sieci lub usług, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu uksc.

Ze względu na fakt, iż przedsiębiorcy telekomunikacyjni mają podstawowe znaczenie dla funkcjonowania sieci oraz usług telekomunikacyjnych, nie włączenie ich bezpośrednio do krajowego systemu cyberbezpieczeństwa jest krytykowane w doktrynie (Balcerzak i Durbajło, 2017, s. 49) oraz budzi wątpliwości praktyczne, gdyż wydłuża proces w zakresie zgłaszania incydentów do właściwego CSIRT poprzez Prezesa UKE.

Mając na uwadze powyższe, należy stwierdzić, iż nie wszyscy istotni dla zapewnienia cyberbezpieczeństwa przedsiębiorcy z sektora prywatnego zostali objęci regulacją uksc. Brak zakwalifikowania do krajowego systemu cyberbezpieczeństwa przedsiębiorców dostarczających usługi OTT, usługi łączności M2M czy portali społecznościowych pozbawia państwo wpływu na cyberbezpieczeństwo, a w rezultacie obniża poziom bezpieczeństwa w cyberprzestrzeni. Niewłączenie w sposób bezpośredni przedsiębiorców telekomunikacyjnych do krajowego systemu cyberbezpieczeństwa może również skutkować obniżeniem poziomu bezpieczeństwa w cyberprzestrzeni.

V. Status podmiotów publicznych odpowiedzialnych za infrastrukturę

Za podmioty publiczne należy uznać podmioty posiadające na podstawie prawa publicznego określone prawa i obowiązki, które są powołane do realizacji interesu publicznego. Podmioty te posiadają zdolność administracyjnoprawną, czyli możność wykonywania określonych praw i obowiązków (Stasikowski, 2019, s. 93–94). Podmioty publiczne, w tym organy administracji, odpowiedzialne za cyberbezpieczeństwo są wyróżniane w oparciu o kryterium zadań i kompetencji powierzonych im do wykonania przez władzę publiczną na podstawie prawa publicznego (Kiczka, Hausner, Niewiadomski i Wróbel, 2013, s. 539).

W polskim systemie prawnym, przed wejściem w życie uksc, w oparciu o kryterium zadań i kompetencji można było wskazać zróżnicowane podmioty publiczne zajmujące się cyberbezpieczeństwem, np. Ministerstwo Cyfryzacji, Policję, Agencję Bezpieczeństwa Wewnętrznego, Biuro Bezpieczeństwa Narodowego, Urząd Komunikacji Elektronicznej czy Rządowe Centrum Bezpieczeństwa (Trąbiński, 2017, s. 75). Wejście w życie uksc doprowadziło do powstania precyzyjnej listy podmiotów publicznych odpowiedzialnych za bezpieczeństwo cybernetyczne Polski i wchodzących w skład krajowego systemu cyberbezpieczeństwa. Zgodnie z art. 4 uksc podmiotami publicznymi odpowiedzialnymi za cyberbezpieczeństwo są: CSIRT MON, CSIRT NASK, CSIRT GOV, organy właściwe do spraw cyberbezpieczeństwa (tj. ministerstwa odpowiedzialne za dany sektor oraz Komisja Nadzoru Finansowego), Pojedynczy Punkt Kontaktowy do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa.

Pierwszorzędne miejsce w krajowym systemie cyberbezpieczeństwa, w tym w zakresie współpracy z przedsiębiorcami z sektora prywatnego, pełnią tzw. CSIRT (Computer Security Incident Response Team) tzw. Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego. W prawie europejskim używane jest pojęcie CSIRT, w odróżnieniu od oznaczenia CERT (Computer Emergency Response Team), które jest zarejestrowane w Stanach Zjednoczonych. Zespoły te określane są również jako IRT (Incidet Response Team) oraz CIRT (Computer Incident Response Team) (Banasiński, 2018, s. 150). CSIRT są definiowane jako punkty kontaktowe dla

kwestii technicznych związanych z cyberbezpieczeństwem (Morgus, Skierka, Hohmann i Maurer, 2015, s. 9). Status CSIRT jest bardzo zróżnicowany. Cechą wspólną CSIRT jest eksperckie podejście do kwestii cyberbezpieczeństwa. Wyróżnia się CSIRT narodowe, komercyjne oraz sektorowe (Balcerzak i Durbajło, 2017, s. 63). CSIRT sektorowe mogą mieć charakter komercyjny, tj. powołane przez podmioty z sektora prywatnego lub charakter mieszany, czyli powołane przez podmioty z sektora publicznego oraz podmioty z sektora prywatnego. Wskazuje się, że CSIRT narodowe mogą mieć status organizacji pozarządowej, status niezależnego organu administracji lub jednostki organizacyjnej usytuowanej w ramach podmiotu publicznego (Morgus, Skierka, Hohmann i Maurer, 2015, s. 9).

Ustawa o krajowym systemie cyberbezpieczeństwa po raz pierwszy reguluje na poziomie ustawowym status oraz prawa i obowiązki CSIRT. Ustawa ta sankcjonuje strukturę zdecentralizowanych oraz równorzędnych trzech CSIRT narodowych, które są usytuowane w strukturach podmiotów publicznych. Zostały wyróżnione: CSIRT MON znajdujący się w ramach w Ministerstwa Obrony Narodowej, który jest właściwy dla spraw obronności, CSIRT GOV umiejscowiony w ramach Agencji Bezpieczeństwa Wewnętrznego, który jest odpowiedzialny za incydenty występujące w obszarze administracji rządowej oraz infrastruktury krytycznej oraz CSIRT NASK wchodzący w skład NASK – Państwowego Instytutu Badawczego, odpowiadający za incydenty w sektorze cywilnym.

Zgodnie z uksc do kluczowych zadań CSIRT należy monitorowanie, wykrywanie i reagowanie na incydenty, neutralizacja wykrytych incydentów oraz minimalizacja ryzyka wystąpienia nowych incydentów. CSIRT nie zajmują się wszystkimi incydentami, gdyż reagowanie na incydenty powinno należeć w pierwszym rzędzie do podmiotów zainteresowanych, których dotyczy incydent (Balcerzak i Durbajło, 2017, s. 62). Wynika to z regulacji uksc nakładającej obowiązki dotyczące zapewnienia bezpieczeństwa na podmioty krajowego systemu cyberbezpieczeństwa, co uzasadnia się ograniczonym zasobem CSIRT. CSIRT odgrywają rolę tzw. ostatniej instancji (last resort) przez obsłudze incydentów, tj. CSIRT zajmuje się obsługą incydentów w przypadku braku podmiotu właściwego do jego obsłużenia (Prusak-Górniak i Silicki, 2019, s. 235). Podstawową rolą CSIRT dla efektywnego działania krajowego systemu cyberbezpieczeństwa jest wymiana informacji dotyczących cyberbezpieczeństwa zarówno z pozostałymi podmiotami publicznymi odpowiadającymi za cyberbezpieczeństwo, jak i z przedsiębiorcami z sektora prywatnego. Wymiana informacji zwłaszcza z przedsiębiorcami z sektora prywatnego ma doniosłe znaczenie dla minimalizowania skutków incydentów, co stanowi jeden z głównych założeń wynikających z uksc.

Wobec powyższego, należy stwierdzić, iż zespoły CSIRT stanowią jądro krajowego systemu cyberbezpieczeństwa (Balcerzak i Durbajło, 2017, s. 61). Uregulowanie CSIRT aktem prawnym rangi ustawowej skutkuje, iż uzyskały one zdolność administracyjnoprawną w zakresie praw i obowiązków nadanych im w uksc. Wzmocnienie ich pozycji wśród podmiotów publicznych odpowiedzialnych za cyberbezpieczeństwo ma pozytywny wpływ na poziom bezpieczeństwa w cyberprzestrzeni. Z tej przyczyny, zespoły CSIRT, jako podmioty działające na podstawie przepisów prawa, mają przymiot niezależności w zakresie współpracy z przedsiębiorcami z sektora prywatnego. Dodatkowo, należy podkreślić, iż korzystnym rozstrzygnięciem ustawodawcy krajowego w zakresie współpracy z sektorem prywatnym jest stworzenie trzech zdecentralizowanych CSIRT narodowych oraz umożliwienie tworzenia kolejnych tzw. sektorowych zespołów cyberbezpieczeństwa.

Ustanowienie struktury rozproszonej CSIRT efektywnie wpływa na współpracę z sektorem prywatnym, gdyż w cyberprzestrzeni działają liczni przedsiębiorcy o zróżnicowanej specyfice działania i jeden CSIRT narodowy miałby ograniczone zdolności współpracy wynikające z mechanizmów funkcjonowania sektora publicznego (inaczej: Hydzik, 2019, s. 86).

VI. Partnerstwo przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych

Partnerstwo przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych w zakresie cyberbezpieczeństwa (określane również jako publiczno-prywatne partnerstwo w zakresie cyberbezpieczeństwa[6]) definiuje się jako model współdziałania (kooperacja) partnerów z sektora prywatnego oraz partnerów z sektora publicznego, obejmujący różne formy działania, nakierowany na osiągnięcie wspólnego celu, którym jest ochrona cyberprzestrzeni. Model partnerstwa łączy się z zasadami organizacji wykonywania zadań publicznych i może być opisywany przez takie pojęcia, jak „uspołecznienie" oraz „prywatyzacja materialna (zadaniowa)". W doktrynie przez pojęcie „uspołecznienie" rozumiane jest zjawisko polegające na włączeniu podmiotów z sektora prywatnego do wykonywania zadania publicznego (Stasikowski, 2019, s. 86–87). Podobnie jest opisywane zjawisko prywatyzacji materialnej (zadaniowej) jako przekazanie zadania publicznego do realizacji przez podmiot z sektora prywatnego (Stasikowski, 2019, s. 199). Model publiczno-prywatnego partnerstwa w cyberbezpieczeństwie jest wskazywany w piśmiennictwie, w dokumentach programowych oraz wynika z regulacji prawnych, tj.: dyrektywy NIS oraz uksc.

W doktrynie przyjmuje się, iż publiczno-prywatne partnerstwo stanowi fundament dla cyberbezpieczeństwa. Jest opisywane jak horyzontalna, niehierarchiczna relacja podmiotów prywatnych z podmiotami publicznymi oparta na uzgodnionych decyzjach w celu realizacji wspólnego celu, którym jest bezpieczeństwo cybernetyczne. Podkreśla się, iż głównym komponentem tego partnerstwa jest dzielenie się informacjami z zakresu cyberbezpieczeństwa pomiędzy podmiotami publicznymi oraz prywatnymi (Carr, 2016, s. 43, 54–55). Wskazuje się, iż publiczno-prywatne-partnerstwo wywodzi się z nowego modelu zarządzania administracją publiczną, określaną jako New Public Management, w którym promowana jest deregulacja, liberalizacja oraz prywatyzacja. Partnerstwo, oparte na tym modelu, opisywane jest jako kooperacja w różnych formach, oparta na samoregulacji oraz samoorganizacji bezpieczeństwa sieci oraz systemów teleinformatycznych przez podmioty z sektora prywatnego, rolą państwa jest zaś kształtowanie warunków partnerstwa (Dunn Cavelty i Suter, 2009, s. 2, 7). W polskim piśmiennictwie wskazuje się, iż partnerstwo w zakresie cyberbezpieczeństwa może być realizowane za pomocą instytucji umownego partnerstwa publiczno-prywatnego, a kluczowym przedmiotem tego partnerstwa ma być wymiana na zasadach dowolności informacji o incydentach i ryzykach naruszających bezpieczeństwo w cyberprzestrzeni (Ganczar, 2017, s. 87). Publiczno-prywatne partnerstwo jest elementem strategii oraz programów bezpieczeństwa narodowego w wielu państwach (Carr, 2016, s. 44). W ramach programu

[6] Publiczno-prywatne partnerstwo w zakresie cyberbezpieczeństwa to przyjęty w rozumieniu niniejszego artykułu model współdziałania (współpraca) przedsiębiorców z sektora prywatnego oraz podmiotów z sektora publicznego mający na celu ochronę cyberprzestrzeni. Powyższe pojęcie nie należy odnosić wyłącznie do instytucji partnerstwa publiczno-prywatnego w rozumieniu ustawy z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym (DzU 2019, poz. 1445 t.j. ze zm.), choć instytucja partnerstwa publiczno-prywatnego wchodzi w jego zakres.

ramowego UE w zakresie badań naukowych i innowacji na lata 2014–2020 „Horyzont 2020”[7] wymienione jest kontraktowe partnerstwo publiczno-prywatne w zakresie rozwoju i wdrożenia badań, które może być realizowane w dziedzinie bezpieczeństwa cybernetycznego (Banasiński, 2018a, s. 56). Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 w pkt 7.2.[8] odwołuje się do modelu partnerstwa publiczno-prywatnego, wskazując, iż rząd zamierza wspierać formę współpracy pomiędzy sektorem publicznym i prywatnym w zapewnienie bezpieczeństwa w cyberprzestrzeni.

W motywie 35 dyrektywy NIS zawarta jest wytyczna, która potwierdza znaczenie współpracy pomiędzy sektorem publicznym a sektorem prywatnym. Motyw ten wskazuje, iż przedsiębiorcy powinni być zachęcani do tworzenia własnych nieformalnych mechanizmów współpracy, a dzielenie się informacjami oraz najlepszymi praktykami nie może powodować konsekwencji dla zainteresowanych. W uksc zawartych jest szereg przepisów odnoszących się do partnerstwa przedsiębiorców z sektora prywatnego oraz podmiotów z sektora publicznego. Art. 11 ust. 1 pkt 2), 4) i 5) uksc dotyczący operatorów usługi kluczowej oraz art. 18 ust. 1 pkt 2), 4) i 5) uksc odnoszący się do dostawców usług cyfrowych, regulują współdziałanie z zespołami CSIRT w zakresie dwustronnego dzielenia się informacjami o incydentach oraz obsługi incydentów. Na podstawie art. 26 ust. 6 pkt 2) uksc CSIRT NASK jest uprawniony do tworzenia i udostępniania narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach. Natomiast, art. 46 ust. 1 pkt 1) ustawy, wskazuje, iż współpraca podmiotów w ramach partnerstwa może być realizowana za pomocą systemu teleinformatycznego, którego rozwój i utrzymanie zapewnia minister właściwy do spraw informatyzacji. Podkreślenia wymaga, iż dwustronne dzielenie się informacjami o zagrożeniach, podatnościach na incydenty oraz o zaistniałych incydentach stanowi najważniejszy element publiczno-prywatnego partnerstwa w zakresie cyberbezpieczeństwa. Ponieważ przedsiębiorcy dysponują jako pierwsi wiedzą na temat wystąpienia incydentów w ich sieci i systemach teleinformatycznych, informacja o incydencie decyduje o czasie reakcji i ograniczeniu rozpowszechniania się ich na inne sieci i systemy teleinformatyczne. Wymiana informacji dotyczących potencjalnych podatnościach systemów teleinformatycznych, pozwala eliminować zagrożenie przed wystąpieniem incydentu. Również istotna jest współpraca przedsiębiorców i zespołów CSIRT przy obsłudze zaistniałych incydentów, co pozwala na efektywniejsze i szybsze ich neutralizowanie.

Należy zauważyć, iż partnerstwo przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych jest realizowane za pomocą regulacji administracyjnoprawnej opartej na środkach niewładczych w postaci czynności materialno-technicznych, którymi są: wymiana informacji pomiędzy partnerami, działania w postaci ostrzegania o podatnościach czy przedstawianie rekomendacji w zakresie cyberbezpieczeństwa. W zakresie dobrowolnej wymiany informacji o podatnościach i incydentach pomiędzy podmiotami ma zastosowanie forma umowy cywilno-prawnej (Stasikowski, 2009, s. 19–21). Wymaga podkreślenia, iż stosowanie środków niewładczych do publiczno-prywatnego partnerstwa w zakresie cyberbezpieczeńsywa pozwala na równorzędną i opartą na zaufaniu współpracę pomiędzy partnerami, która skutkuje

[7] Rozporządzenie Parlamentu Europejskiego i rady (UE) nr 1291/2013 z dnia 11 grudnia 2013 r. ustanawiające „Horyzont 2020” – program ramowy w zakresie badań naukowych i innowacji (2014–2020) oraz uchylające decyzję nr 1982/2006/WE.

[8] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. z 2019 r., poz. 1037).

zapewnieniem wysokiego poziomu ochrony cyberprzestrzeni, która leży w interesie wszystkich jego użytkowników.

VII. Zakończenie

Biorąc pod uwagę rolę przedsiębiorców z sektora prywatnego oraz podmiotów publicznych w cyberprzestrzeni, można stwierdzić, iż współdziałanie tych podmiotów w efektywnym zapewnieniu bezpieczeństwa w cyberprzestrzeni jest niezbędne. Zarówno interes przedsiębiorców z sektora prywatnego funkcjonujących w cyberprzestrzeni, jak i interes podmiotów publicznych odpowiedzialnych za bezpieczeństwo częściowo się pokrywają. Przedsiębiorcy prowadzący aktywność gospodarczą w cyberprzestrzeni mają interes w przeciwdziałaniu zagrożeniom skierowanym wobec nich, takich jak: cyberprzestępstwa, przerwanie ciągłości ich działania, wyciek danych czy utrata renomy. Podmioty publiczne działające jako przedstawiciele państwa realizują interes bezpieczeństwa publicznego, czyli w wymiarze szerszym niż interes poszczególnych przedsiębiorców. Inna logika (mechanizm działania) podmiotów z sektora prywatnego tj. oparta na racjonalności ekonomicznej i podmiotów z sektora publicznego, tj. oparta na racjonalności dobra wspólnego, z jednej strony umożliwiają wzajemne uzupełnianie się interesów w zakresie zapewniania bezpieczeństwa w cyberprzestrzeni, z drugiej zaś – prowadzi do kolizji interesów tych podmiotów. Przedsiębiorcy ze względu na realizację modelu biznesowego próbują unikać odpowiedzialności za zapewnienie bezpieczeństwa, jeżeli nie przynosi im to wymiernych korzyści biznesowych. Natomiast, podmioty publiczne nie mają wystarczających zdolności oraz wiedzy w zakresie zapewnienia cyberbezpieczeństwa. Odpowiedzią na powyższe zróżnicowane interesy, cele i mechanizmy działania przedsiębiorców i podmiotów publicznych jest model publiczno-prywatnego partnerstwa. Model ten prowadzi do wykonywania zadania publicznego, którym jest ochrona cyberprzestrzeni za pomocą reguł rynku i mechanizmu konkurencji.

Analiza przepisów prawnych wskazuje, iż zarówno dyrektywa NIS, jak i uksc zawierają regulacje prawne dotyczące publiczno-prywatnego partnerstwa w zakresie cyberbezpieczeństwa. Aspekt współpracy pomiędzy sektorem publicznym oraz sektorem prywatnym w zakresie cyberbezpieczeństwa jest zauważany i promowany w dokumentach programowych i strategicznych dotyczących cyberbezpieczeństwa oraz w motywach dyrektywy NIS. Ustawa o krajowym systemie cyberbezpieczeństwa zawiera szczegółowe rozwiązania prawne umożliwiające współdziałanie przedsiębiorców oraz podmiotów publicznych odpowiedzialnych za cyberbezpieczeństwo. Status oraz kompetencje podmiotów objętych krajowym systemem cyberbezpieczeństwa wskazują, iż kluczowe znaczenie dla współpracy przy ochronie cyberprzestrzeni przed zagrożeniami mają przedsiębiorcy dostarczający infrastrukturę oraz usługi cyfrowe, a po stronie podmiotów publicznych wyspecjalizowane zespoły CSIRT. Należy jednak zwrócić uwagę, iż uksc ma ograniczony zakres działania ze względu na nie włączenie do krajowego systemu cyberbezpieczeństwa takich podmiotów, jak: dostawcy OTT, dostawcy portali społecznościowych czy przedsiębiorcy telekomunikacyjni.

Z analizy uksc wynika, iż przedmiotowe partnerstwo jest uregulowane za pomocą instrumentów administracyjnoprawnych o charakterze niewładczym. Z tego powodu, współpraca partnerów może odbywać się na zasadzie dobrowolności, co skutkuje, iż zakres oraz intensywność współpracy zależy od samych zainteresowanych. Dlatego też, doniosłe znaczenie dla rozszerzania

oraz pogłębiania współpracy podmiotów z sektora prywatnego oraz sektora publicznego ma świadomość partnerów dotycząca współpracy oraz właściwe kształtowanie otoczenia regulacyjnego przez organy administracji państwowej. Szczególne znaczenie w tym zakresie może mieć funkcja regulacyjna administracji publicznej o charakterze *ex ante*, której celem byłoby kształtowanie warunków partnerstwa w dziedzinie cyberbezpieczeństwa. Silne partnerstwo podmiotów z sektora prywatnego i publicznego w zakresie cyberbezpieczeństwa jest najskuteczniejszym remedium na zagrożenia płynące z funkcjonowania cyberprzestrzeni.

Bibliografia

Asghari, H. (2016). *Cybersecurity via Intermediaries: Analyzing Security Measurements to Understand Intermediary Incentives and Inform Public Policy*. Doctoral thesis. TU Delft. Pozyskano z: https://repository.tudelft.nl/islandora/object/uuid:3694edf5-d6e0-4484-b847-750da2b9d1b9?collection=research.

Balcerzak, P.M. i Durbajło, P. (2017). Organizacyjno-prawne aspekty implementacji dyrektywy Parlamentu Europejskiego i Rady z 6.7.2016 r. W: A. Gryszczyńska, G. Szpor (red.), *Internet. Strategie bezpieczeństwa*. Warszawa: Wydawnictwo C.H. Beck.

Banasiński, C. (2018). *Prawo administracyjne wobec współczesnych wyzwań. Księga Jubileuszowa Dedykowana Profesorowi Markowi Wierzbowskiemu*. Warszawa: Wydawnictwo C.H. Beck.

Banasiński, C. (red.). (2018a). *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolter Kluwer.

Berdel-Dudzińska, M. (2012). Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym. *Przegląd Prawa Publicznego*, (2).

Carr, M. (2016). Public-private partnership in national cyber-security strategies. *International Affairs*, *92*(1).

Chmielewski, J.M. i Waćkowski, K. (2018). W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolter Kluwer.

Chrzanowski, M. i Kruk, T.J. (2012). Bezpieczeństwo systemu nazw domenowych. W: G. Szpor, W. Wiewiórowski (red.), Internet. *Prawno-informatyczne problemy sieci, portali i e-usług*. Warszawa: Wydawnictwo C.H. Beck.

Dunn Cavelty, M. i Suter, M. (2009). Public-private partnerships are no silver bullet: An expended governance model for Critical Infrustructure Protection. *International Journal od Critical Infrastructure Protection*, 2(4). https://doi.org/10.1016/j.ijcip.2009.08.006.

Ganczar, M. (2017). Umowne partnerstwo publiczno-prywatne w kontekście bezpieczeństwa sieci i systemów informacji administracji publicznej. W: A. Gryszczyńska, G. Szpor (red.), *Internet. Strategie bezpieczeństwa*. Warszawa: Wydawnictwo C.H. Beck.

Hydzik, W. (2019). Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych. *Business Law Journal*, (3).

Kiczka, K., Hausner, R., Niewiadomski, Z. i Wróbel A. (red.). (2013). *System Prawa Administracyjnego. Publiczne prawo gospodarcze. Tom 8A*. Warszawa: Wydawnictwo C.H. Beck.

Lisiak-Felicka, D. i Szmit, M. (2016). *Cyberbezpieczeństwo w administracji publicznej w Polsce, Wybrane zagadnienia*. Kraków: European Association for Security.

Menthe, D.C. (1998). Jurisdiction in Cyberspace: A Theory of International Space. *Michigan Telecommunications and Technology Law Rewiew,* (69).

Morgus, R., Skierka, I., Hohmann, M. i Maurer, T. (2015). *National CSIRTs and Their Role in Computer Security Incident Response*, listopad. Washington: New America.

Niezgódka, E. (2017). Profilowanie a cyberbezpieczeństwo. W: A. Gryszczyńska, G. Szpor (red.), *Internet. Strategie bezpieczeństwa*. Warszawa: Wydawnictwo C.H. Beck.

Piątek, S. (2011). *Sieci szerokopasmowe w polityce telekomunikacyjnej*. Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

Polański, P. (2019). Zwalczanie bezprawnych treści w Internecie a cyberbezpieczeństwo. W: G. Spor, K. Czaplicki (red.), *Internet. Analityka danych*. Warszawa: Wydawnictwo C.H. Beck.

Prusak-Górniak, K. i Silicki, K. (2019). W: G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), *Ustawa o krajowym Systemie Cyberbezpieczeństwa. Komentarz*. Warszawa: Wolters Kluwer.

Rojszczak, M. (2018). W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolter Kluwer.

Siwicki, M. (2019). Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego. *Europejski Przegląd Sądowy*, wrzesień.

Stasikowski, R. (2009). O funkcji policyjnej administracji publicznej. *Przegląd Prawa Publicznego*, (4).

Stasikowski, R. (2019). *Pluralizm administracji publicznej*. Warszawa: Wydawnictwo C.H. Beck.

Szpor, G. (2017). Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa. W: A. Gryszczyńska, G. Szpor (red.), *Internet. Strategie bezpieczeństwa*. Warszawa: Wydawnictwo C.H. Beck.

Trąbiński, P. (2017). Podział kompetencji w zapewnieniu cyberbezpieczeństwa. W: A. Gryszczyńska, G. Szpor (red.), *Internet. Strategie bezpieczeństwa*. Warszawa: Wydawnictwo C.H. Beck.

Wojdyło, K. (2014). Europejskie podejście do cyberbezpieczeństwa. W: P. Rutkowski, K. Wojdyło (red.), *Cyberbezpieczeństwo*, listopad. Warszawa: Wardyński + Wspólnicy. Pozyskano z: https://www.wardynski.com.pl/w_publication/raport-cyberbezpieczenstwo.

Żurawik, A., Hausner, R., Niewiadomski, Z. i Wróbel, A. (red.). (2013). *System Prawa Administracyjnego. Publiczne prawo gospodarcze. Tom 8A*. Warszawa: Wydawnictwo C.H. Beck.