UZASADNIENIE

Obecnie obserwuje się niezwykle dynamiczny proces przenoszenia aktywności ludzkiej w przestrzeń wirtualną, będącą składową obszaru cyberprzestrzeni. Dotyczy to nie tylko działalności osób fizycznych, ale również administracji publicznej, przedsiębiorców, organizacji społecznych i innych podmiotów. Działalność w cyberprzestrzeni staje się nieodzownym elementem funkcjonowania państwa i społeczeństwa. Należy jednak zauważyć, że postępujący proces informatyzacji, obok niewątpliwych korzyści, rodzi również określone zagrożenia. W szczególności dotyczy to możliwości wykorzystania cyberprzestrzeni w celach sprzecznych z interesami państwa i jego obywateli. Przykładem tego rodzaju zagrożeń są liczne ataki hakerów na różnego rodzaju instytucje o istotnym znaczeniu dla funkcjonowania państwa i społeczeństwa. Ataki takie mogą być niezwykle groźne, bowiem w ich efekcie może dojść do poważnych zakłóceń w funkcjonowaniu państwa, w tym jego struktur i gospodarki. Biorąc powyższe pod uwagę państwo powinno być przygotowane zarówno na odparcie takich ataków jak i zwalczanie jego skutków.

Zasadniczym celem zmian ujętych w projektowanej ustawie jest uwzględnienie zagrożeń wynikających z działań i zdarzeń w cyberprzestrzeni jako okoliczności spełniającej normatywną treść przesłanek wprowadzenia jednego ze stanów nadzwyczajnych, o których mowa w art. 229, 230 i 232 Konstytucji Rzeczypospolitej Polskiej.

Obowiązujące przepisy ustaw regulujących stany nadzwyczajne wskazują przyczyny wprowadzenia tych stanów, niemniej zostały one określone w sposób bardzo ogólnikowy. W związku z tym może to rodzić wątpliwości, co do ich charakteru i źródła.

Jest sprawą oczywistą, że niezbędną przesłanką wprowadzenia stanu nadzwyczajnego (o charakterze ogólnym) powinno stanowić zagrożenie dla określonego przez Konstytucję RP dobra (zewnętrzne zagrożenie państwa, zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego). Biorąc jednak pod uwagę ogromne zagrożenia związane z informatyzacją administracji publicznej i gospodarki narodowej, istnieje potrzeba jednoznacznego wskazania, że jedną z przyczyn wprowadzenia stanu nadzwyczajnego (o charakterze szczególnym) mogą być działania i zdarzenia w cyberprzestrzeni.

Istota zmian ujętych w projektowanej ustawie polega na rozwinięciu niektórych pojęć, traktowanych przez Konstytucję jako przesłanki wprowadzenia stanu wojennego, stanu wyjątkowego i stanu klęski żywiołowej, w dostosowaniu do pojawiających się zagrożeń w obszarze cyberprzestrzeni, mogących mieć bezpośrednie odniesienie do sfery

bezpieczeństwa narodowego. Z oczywistych względów proponowane rozwiązania nie mają na celu katalogizowania zdarzeń, które w sposób automatyczny wypełniałyby przesłanki określone w art. 229, 230 i 232 Konstytucji Rzeczypospolitej Polskiej.

Uwzględniając powyższe, w projekcie przewiduje się zdefiniowanie w ustawie o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (art. 2) pojęcia „zewnętrzne zagrożenie państwa". Proponuje się, aby dla potrzeb zmienianej ustawy pojęcie to oznaczało celowe działania, w tym o charakterze terrorystycznym, godzące w niepodległość, niepodzielność terytorium lub w ważny interes gospodarczy Rzeczypospolitej Polskiej, a także zmierzające do uniemożliwienia wykonywania lub zakłócenia przez organy państwowe ich funkcji, podejmowane przez zewnętrzne w stosunku do niej podmioty, na lądzie, wodzie, w przestrzeni powietrznej, przestrzeni kosmicznej lub cyberprzestrzeni. Taki sposób zdefiniowania wspomnianego terminu ma na celu precyzyjne określenie warunków, jakie muszą zostać spełnione, aby właściwe organy (Prezydent RP i Rada Ministrów) mogły uznać określone działania za zewnętrzne zagrożenie państwa. Należy podkreślić, że jednym z takich warunków jest szkodliwe z punktu widzenia żywotnych interesów i celów strategicznych Polski działanie podmiotu zewnętrznego, niezależnie od miejsca podejmowania przez niego tych działań (zarówno w Polsce, jak i poza jej terytorium). Jednocześnie w projekcie uwzględnia się, że działania te mogą skutkować nie tylko w tradycyjnych dotychczas wymiarach (ląd, woda, przestrzeń powietrzna, przestrzeń kosmiczna), ale również w przestrzeni wirtualnej – cyberprzestrzeni. W konsekwencji zaistniała konieczność zdefiniowania pojęcia „cyberprzestrzeń", która – zgodnie z projektem – oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Proponowana definicja znalazła akceptację podmiotów biorących udział w konsultacjach, a jej treść uwzględnia uwagę zgłoszoną dodatkowo przez Ministra Spraw Wewnętrznych i Administracji.

Ponadto projekt przewiduje zmianę ustawy o stanie klęski żywiołowej (art. 3 ust. 2), gdzie zakłada się, że katastrofa naturalna lub awaria techniczna mogą zostać dodatkowo wywołane nie tylko przez działania terrorystyczne, ale również przez zdarzenia w cyberprzestrzeni. W związku z tym zaistniała potrzeba zdefiniowania pojęcia „cyberprzestrzeń" również w tej ustawie (art. 3 ust. 1 pkt 4).

Niezależnie od powyższego, w projekcie przewiduje się także zmianę art. 2 w ustawie o stanie wyjątkowym, gdzie proponuje się uwzględnienie działań w cyberprzestrzeni, które stwarzają zagrożenie dla konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, jako możliwej przyczyny wprowadzenia stanu wyjątkowego. Również i w tej ustawie zaistniała konieczność zdefiniowania pojęcia „cyberprzestrzeni", która – analogicznie jak w obydwu wcześniej wymienionych ustawach - oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

W tym kontekście należy podkreślić, że rozporządzenia Prezydenta RP i Rady Ministrów o wprowadzeniu określonego stanu nadzwyczajnego mają charakter fakultatywny, a ich wydanie uzależnione jest zawsze od oceny stopnia zagrożenia w sferze zewnętrznego bądź wewnętrznego bezpieczeństwa państwa. Zatem ustawowe nadanie bezpieczeństwu w cyberprzestrzeni rangi istotnego segmentu bezpieczeństwa narodowego znajduje pełne uzasadnienie. W ten sposób bowiem wskazana ocena dokonywana będzie także przez pryzmat skutków naruszeń bezpieczeństwa w przestrzeni wirtualnej, dając w efekcie Prezydentowi RP i Radzie Ministrów poszerzony obraz skali występujących zagrożeń.

Ustawowe wyeksponowanie cyberprzestrzeni jako obszaru stwarzającego potencjalne zagrożenia, mogące skutkować koniecznością wprowadzenia jednego ze stanów nadzwyczajnych, nie ma charakteru precedensowego. Powiela ono bowiem rozwiązania przyjęte w toku prac parlamentarnych nad ustawami o stanach nadzwyczajnych, uznające – pod wpływem wydarzeń z dnia 11 września 2001 r. na terytorium USA – działania terrorystyczne za przyczynę powstania zagrożeń. Przedstawiony projekt pozostawia wskazaną przyczynę, dostosowując jedynie brzmienie formułujących ją zapisów do definicji przestępstwa o charakterze terrorystycznym, ujętej w art. 115 § 20 Kodeksu karnego.

Dodać należy, iż pojęcie cyberprzestrzeni nie jest obce obowiązującemu prawu. Operuje nim na przykład *Konwencja o cyberprzestępczości* z dnia 23 listopada 2001 r., implementowana do prawa polskiego ustawą z dnia 18 marca 2004 r. *o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń* (Dz. U. Nr 69, poz. 626), a także ratyfikowana *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o współpracy w zwalczaniu terroryzmu, przestępczości zorganizowanej i innej przestępczości, podpisana w Ankarze w dniu 7 kwietnia 2003 r.* (Dz. U. z 2005 r. Nr 12, poz. 94).

Ujęte w projekcie rozwiązania wkomponowują się w przygotowywany przez Radę Ministrów „Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016", stanowiąc jego ważne uzupełnienie.

Ponadto rozwiązania te pozostają w pełnej zgodności z nową Koncepcją Strategiczną NATO, przyjętą na szczycie w Lizbonie, w której wskazano ataki cybernetyczne jako jedno z istotnych zagrożeń bezpieczeństwa dla państw członków Sojuszu Północnoatlantyckiego.

Projekt ustawy został poddany konsultacjom z właściwymi organami administracji rządowej, w szczególności z Ministrami: Obrony Narodowej, Spraw Wewnętrznych i Administracji, Sprawiedliwości, Spraw Zagranicznych i Infrastruktury oraz z Szefami: Kancelarii Prezesa Rady Ministrów, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego. Ponadto projekt był konsultowany z Rektorami Politechniki Warszawskiej i Akademii Obrony Narodowej.

Niezależnie od powyższego, niniejsza inicjatywa została omówiona podczas posiedzenia Rady Bezpieczeństwa Narodowego w dniu 30 maja 2011 r.

Wejście w życie projektowanej ustawy nie pociąga za sobą skutków finansowych dla budżetu państwa. Projekt nie jest objęty zakresem prawa Unii Europejskiej.