

Agnieszka WARCHOŁ 

Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie

agnieszka.warchol@up.krakow.pl

CYBERPRZESTRZEŃ W STANACH NADZWYCZAJNYCH W POLSCE – PERSPEKTYWA PORÓWNAWCZA

ABSTRACT **Cyberspace in States of Emergency in Poland**

The aim of the article is to present cyberspace in the regulations on states of emergency in the legal system in Poland. The Constitution of the Republic of Poland in Chapter IX regulates the issue of “States of emergency”. Each of these situations is also regulated by separate acts. The article presents these acts and answers the question why “cyberspace” was introduced into the Polish law in these acts. The article is divided into several parts – introduction, information about the amendment act, and finally the discussion of individual acts.

Keywords: cyberspace, states of emergency, security

Słowa kluczowe: cyberprzestrzeń, stany nadzwyczajne, bezpieczeństwo

WPROWADZENIE

Jeszcze w latach 80. XX w. termin „cyberprzestrzeń” pojawiał się w powieściach *science fiction* jako nazwa wytworu ludzkiej wyobraźni¹. Następna dekada była przełomowa, m.in. za sprawą pułkownika Johna Wardena, który w modelu nazwanym jego nazwiskiem wskazał, że cyberprzestrzeń jest kolejnym polem starć, miejscem oddziaływania na podmioty stosunków międzynarodowych². Po lądzie, morzu, przestrzeni powietrznej i kosmicznej, cyberprzestrzeń jest następnym środowiskiem prowadzenia walki³. Obecnie pojęcie „cyberprzestrzeń” jest przywoływane w dokumentach państwowych i ponadnarodowych, które nadają mu strategiczne znaczenie z punktu widzenia bezpieczeństwa.

Z perspektywy niniejszych rozważań niezwykle ważne jest wskazanie momentu wprowadzenia do polskiego języka prawnego, i zarazem prawniczego, terminu „cyberprzestrzeń”. Miało to miejsce stosunkowo późno, bo dopiero w 2011 r. Pojęcie nie pojawiło się w związku z tworzeniem nowego planu, strategii czy doktryny bezpieczeństwa, ale za sprawą nowelizacji ustaw o stanach nadzwyczajnych. To właśnie połączenie w jednym akcie prawnym dwóch terminów – „cyberprzestrzeń” i „stany nadzwyczajne” – zapoczątkowało dalsze kroki w budowaniu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Celem artykułu jest zobrazowanie kontekstu społeczno-politycznego, w jakim nastąpiły wyżej wymienione zmiany, oraz przybliżenie czytelnikowi regulacji prawnych dotyczących cyberprzestrzeni w stanach nadzwyczajnych. W związku z tym w artykule zostanie podjęta próba odpowiedzi na szereg pytań związanych ze zmianami dokonanymi w 2011 r., m.in.: co zadecydowało o wyborze formy wprowadzenia pojęcia cyberprzestrzeni do powszechnego obiegu? Kto podjął inicjatywę w tym zakresie? Jak ówczesne siły polityczne w parlamencie oceniały zaproponowany pomysł?

Artykuł jest podzielony na kilka części. Pierwsza z nich ma charakter wprowadzający. Autorka koncentruje uwagę czytelników na krótkim rysie historycznym instytucji stanów nadzwyczajnych, gdyż jest to niezbędne do zrozumienia omawianej problematyki. Ponadto znajdują się tu kwestie natury terminologicznej. W drugim fragmencie tekstu przedstawiono poszczególne etapy procesu legislacyjnego związanego ze zmianami ustaw o stanach nadzwyczajnych wprowadzonymi w 2011 r. Kolejną część artykułu poświęcona jest poszczególnym stanom nadzwyczajnym: wojennemu, wyjątkowemu i klęski żywiołowej. Zostały w niej wskazane i omówione zmiany w ustawach oraz potencjalne scenariusze, w których mogłoby dojść do wprowadzenia owych instytucji z uwagi na szczególne zagrożenie spowodowane działaniami w cyberprzestrzeni.

¹ Zob. W. Gibson, *Neuromancer*, Poznań 1996, s. 53.

² J.A. Warden, *The Enemy as a System*, „Airpower Journal” 1995, vol. 9, nr 1, s. 41-55, [online] http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm, 11 XI 2018.

³ Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe” 2012, nr 22, s. 128.

TERMINOLOGIA I ZARYS PROBLEMU

Stany nadzwyczajne są odpowiedzią na nadzwyczajne zagrożenia⁴, sposobem działania, gdy zwykle siły i środki okazują się niewystarczające. Wprowadza się je na podstawie stosownych ustaw, przez upoważnione do tego organy, w określonym trybie. „Stan nadzwyczajny” to pojęcie prawne, które odnosi się do konstrukcji prawnej, w której gromadzą się cechy konkretnych typów stanów nadzwyczajnych⁵. Krzysztof Eckhardt zwraca uwagę, że *istotą stanu nadzwyczajnego, jako instytucji konstytucyjnej, jest legalne, znajdujące podstawę w konstytucji, ograniczone w czasie odejście od normalnego porządku w państwie w celu ratowania jakiegoś dobra prawnie chronionego*⁶. Ogromne znaczenie ma fakt, że wprowadzenie stanów nadzwyczajnych wiąże się z ograniczeniami praw i wolności człowieka i obywatela. Jak wskazuje Leszek Garlicki, uznanie, że w funkcjonowaniu państwa mogą zachodzić sytuacje, których nie da się rozwiązać w ramach istniejącego porządku prawnego, jest równie stare jak instytucja państwa⁷.

Genezy stanu nadzwyczajnego można się doszukiwać już w dyktaturze rzymskiej, w której władzę ograniczoną czasowo obejmował *dictator*⁸. Miał za zadanie odparcie zagrożenia – zewnętrznego lub wewnętrznego. W tym celu był on wyposażony w szereg kompetencji⁹. W średniowieczu możliwość zastosowania instytucji nadzwyczajnych wyprowadzano z zasady suwerenności monarchy¹⁰. Wraz z kształtowaniem się elementów konstytucjonalizmu zaczęły się pojawiać postulaty ograniczenia swobody działania władcy w tym zakresie, np. w angielskiej *Petycji o prawo* z 1628 r. Pierwsze regulacje konstytucyjne zostały sformułowane we Francji w 1799 r. i nadały ramy prawne instytucji stanu oblężenia¹¹.

Na ziemiach polskich aktem prawnym, w którym dokonano regulacji stanu nadzwyczajnego, był dekret o wprowadzeniu stanu wyjątkowego z 2 stycznia 1919 r.¹² Dokument ten wraz z nowelą z 7 lutego 1919 r., dekretem z 2 stycznia 1919 r. *o używaniu wojska w wypadkach wyjątkowych*, rozporządzeniem Rady Ministrów z 18 kwietnia 1919 r. *o sposobie użycia wojska w wypadkach wyjątkowych* oraz dekretem z 11 stycznia

⁴ K. Dobrzeńcki, *Filozofia prawa a stany nadzwyczajne – zarys problematyki*, [w:] *Stan nadzwyczajny. Analizy z perspektywy nauk politycznych i prawnych*, red. J. Markiewicz-Stanny, P. Łukomski, Zielona Góra 2015, s. 20.

⁵ E. Kurzępa, *Stany nadzwyczajne w polskim porządku prawnym*, Warszawa 2017, s. 57, *Monografie Prawnicze*.

⁶ K. Eckhardt, *Hierarchizacja praw i wolności jednostki w świetle konstytucyjnej regulacji stanu nadzwyczajnego*, „Przegląd Prawa Konstytucyjnego” 2014, nr 2(18), s. 90.

⁷ L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2010, s. 407, *Seria Akademicka*.

⁸ A. Kociołek-Pęksa, J. Menkes, *Międzynarodowe i krajowe prawne regulacje stanów nadzwyczajnych*, [w:] *Stan nadzwyczajny...*, s. 48.

⁹ *Tamże*.

¹⁰ L. Garlicki, *Polskie prawo konstytucyjne...*, s. 407.

¹¹ *Tamże*.

¹² L. Mażewski, *Stany nadzwyczajne w Polsce w latach 1918-1989*, Toruń 2006, s. 17.

1919 r. w przedmiocie kar za przechowywanie lub użycie broni palnej i materiałów wybuchowych w miejscowości ogłoszonej w stanie wyjątkowym zapoczątkowały w Polsce ujmowanie stanu nadzwyczajnego w normy prawne¹³. Po raz pierwszy przepisy regulujące tę instytucję znalazły zastosowanie już 6 stycznia 1919 r. Bezpośrednią przyczyną proklamowania stanu nadzwyczajnego była próba obalenia rządu przeprowadzona z 4 na 5 stycznia przez działaczy związanych z prawicą¹⁴.

Nie wdając się w historyczne dywagacje, warto wspomnieć jedynie o regulacjach stanów nadzwyczajnych w ustawach zasadniczych po odzyskaniu niepodległości w 1918 r. Pierwszym aktem prawnym rangi ustrojowej, który nakreślił elementy reżimu prawnego stanów nadzwyczajnych, była konstytucja z 21 marca 1921 r. W artykułach 123 i 124 przewidywała ona możliwość wprowadzenia dwóch rodzajów stanów nadzwyczajnych: wojennego i wyjątkowego¹⁵. W ustawie zasadniczej z 23 kwietnia 1935 r. stany nadzwyczajne unormowane były nawet w osobnym rozdziale. Konstytucja z 1952 r. regulowała tylko stan wojenny, jednak w sposób niejako łączący oba zagrożenia: wewnętrzne i zewnętrzne. Nowelą z 1983 r. wprowadzono pojęcie stanu wyjątkowego i nie zmieniła tego kolejna – mała – konstytucja z 1992 r., gdyż także zawierała ona w swej treści kategorie stanów: wojennego i wyjątkowego. Obecnie obowiązująca ustawa zasadnicza z 1997 r. reguluje ponadto trzeci rodzaj stanu nadzwyczajnego – stan klęski żywiołowej¹⁶. Jak podkreśla Michał Brzeziński, w Konstytucji Rzeczypospolitej Polskiej (dalej: Konstytucji RP) w zakresie stanów nadzwyczajnych zostały uwzględnione konsekwencje obowiązywania zasady demokratycznego państwa prawnego, co oznacza, że ustawa zasadnicza powinna obowiązywać nie tylko w warunkach pokojowych¹⁷.

Zgodnie z obecnymi rozwiązaniami konstytucyjnymi stan nadzwyczajny to pojawienie się w państwie szczególnego zagrożenia, którego rozwiązanie wymaga sięgnięcia po środki szczególne, takie jak: koncentracja władzy w rękach egzekutywy, ograniczenie praw i wolności obywateli, zmiany w strukturze i zasadach funkcjonowania organów państwowych, zmiany w systemie stanowienia prawa¹⁸.

Wiesław Skrzydło wskazuje, iż wprowadzenie stanu nadzwyczajnego nie jest dyskrecjonalną decyzją konstytucyjnych organów, ale wynikiem wystąpienia ściśle określonych warunków¹⁹. Będzie o nich jeszcze mowa w niniejszym artykule, zwłaszcza że od 2011 r. do katalogu działań mogących generować nadzwyczajne zagrożenia dopisane zostały przez ustawodawcę zdarzenia w cyberprzestrzeni.

¹³ *Tamże*.

¹⁴ *Tamże*, s. 25.

¹⁵ *Tamże*, s. 85.

¹⁶ T. Bryk, *Przegląd regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego” 2011, nr 1(5), s. 223.

¹⁷ M. Brzeziński, *Wybrane zasady stanów nadzwyczajnych w konstytucji z dnia 2 kwietnia 1997 r. – uwagi de lege lata i de lege ferenda*, „Studia Politologiczne” 2017, vol. 45, s. 277.

¹⁸ L. Garlicki, *Polskie prawo konstytucyjne...*, s. 407.

¹⁹ W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Zakamycze 2000, s. 310.

Po wprowadzeniu opisanych zmian rozpoczęła się ożywiona dyskusja przeciwników i zwolenników tego rozwiązania. Ostatecznie stwierdzono, że działania w cyberprzestrzeni mogą być podstawą ogłoszenia każdego z trzech konstytucyjnych stanów nadzwyczajnych. Jest to istotne i warte omówienia, a dla niektórych wręcz kontrowersyjne, z uwagi na fakt, że na mocy Konstytucji RP oraz ustaw dotyczących poszczególnych stanów nadzwyczajnych wprowadzenie stanu nadzwyczajnego wpływa na zasady działania organów władzy publicznej, a także na – wspomniany wyżej – zakres honorowanych praw i wolności jednostki. Dlatego tak ważne jest, by przepisy regulujące instytucje stanów nadzwyczajnych były precyzyjne.

GENEZA ZMIAN

Inicjatorem zmian w ustawach o stanach nadzwyczajnych był Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski. Cel zmian, przygotowanych przez Biuro Bezpieczeństwa Narodowego, zawartych w projekcie ustawy *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* stanowiło uwzględnienie zagrożeń wynikających z działań i zdarzeń w cyberprzestrzeni, jako okoliczności spełniającej normatywną treść przesłanek wprowadzenia stanów nadzwyczajnych²⁰. Istota zmian miała polegać na rozwinięciu niektórych pojęć – traktowanych w Konstytucji RP jako przesłanki wprowadzenia stanu wojennego, stanu wyjątkowego i stanu klęski żywiołowej²¹. Jednym z nich była „cyberprzestrzeń”.

Dotychczas ten termin pojawiał się w obowiązującym prawie jedynie w *Konwencji Rady Europy o cyberprzestępczości* z dnia 23 listopada 2001 r., implementowanej do polskiego prawa *Ustawą z dnia 18 marca 2004 roku o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń*²² oraz w ratyfikowanej *Umowie między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o współpracy w zwalczaniu terroryzmu, przestępczości zorganizowanej i innej przestępczości*²³ z 2003 r.

Prezydencki projekt ustawy zakładał propozycje zmian w następujących aktach prawnych:

- w ustawie *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*,
- w ustawie o stanie wyjątkowym,
- w ustawie o stanie klęski żywiołowej.

²⁰ *Prezydencki projekt ustawy 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*, Sejm RP, VI kadencja, Prezydent RP, Druk nr 4355, Warszawa, 10 VI 2011, [online] [http://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/\\$file/4355.pdf](http://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/$file/4355.pdf), 11 XI 2018.

²¹ *Tamże*.

²² Dz.U. 2004, nr 69, poz. 626.

²³ Dz.U. 2005, nr 12, poz. 94.

W pierwszym z wymienionych dokumentów oprócz definicji cyberprzestrzeni miała się znaleźć również proponowana charakterystyka „zewnętrznych zagrożeń państwa”. Jest to istotne z uwagi na fakt, że wśród warunków, jakie miałyby zostać spełnione, aby właściwe organy mogły uznać określone czyny za zewnętrzne zagrożenie państwa, wskazywano szkodliwe postępowanie podmiotu zewnętrznego, niezależnie od miejsca podejmowania przez niego działań. Znalazłoby to zastosowanie m.in. w odniesieniu do podmiotów transnarodowych, których przedsięwzięcia skutkowałyby niepożądanymi zdarzeniami na terytorium Rzeczypospolitej Polskiej. Aby zobrazować tego typu potencjalny scenariusz, jako przykład można wskazać cyberatak na infrastrukturę krytyczną państwa, wygenerowany w innym kraju lub w Polsce, ale przez podmiot należący do asymetrycznej struktury sieciowej – zewnętrzny względem naszego państwa. W przypadku tego typu działań lokalizacja podmiotu nie ma znaczenia. Liczy się efekt w postaci zakłócenia prawidłowego funkcjonowania organów władzy państwowej. Do wymiarów, w których dotychczas pojawiały się nadzwyczajne zagrożenia, została dołączona cyberprzestrzeń.

Ponadto na mocy proponowanej ustawy ulec zmianie miała ustawa o stanie klęski żywiołowej. Projekt z dnia 10 czerwca 2011 r. zakładał, że katastrofa naturalna lub awaria techniczna mogą zostać wywołane także przez zdarzenia w cyberprzestrzeni. Zaistniała zatem potrzeba zdefiniowania pojęcia „cyberprzestrzeń”, co zostało wyszczególnione przez inicjatora projektu.

Proponowano także zmiany treści ustawy o stanie wyjątkowym. Miały one polegać na dodaniu działań w cyberprzestrzeni jako kolejnej możliwej przyczyny wprowadzenia stanu nadzwyczajnego z art. 230 Konstytucji RP. Zgodnie z założeniami projektu działania w cyberprzestrzeni mogą stwarzać zagrożenie dla konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego. Wskazano także na konieczność sformułowania definicji terminu „cyberprzestrzeń” – analogicznie do dwóch wyżej wymienionych ustaw²⁴.

30 maja 2011 r. na posiedzeniu Rady Bezpieczeństwa Narodowego została omówiona inicjatywa ustawodawcza Prezydenta RP. Argumenty za wprowadzeniem proponowanych zmian dotyczyły konieczności stworzenia prawnych podstaw do uwzględnienia cyberprzestrzeni w przygotowaniu państwa na ewentualność działania w sytuacjach szczególnych. Podkreślano, że sugerowane rozwiązania będą uzupełnieniem przygotowywanego przez Radę Ministrów Rządowego Programu Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016. Tydzień później z inicjatywy Prezydenta RP Bronisława Komorowskiego odbyło się spotkanie, w którym oprócz głowy państwa udział wzięli szef Biura Bezpieczeństwa Narodowego (dalej: BBN) i przewodniczący sejmowych komisji: Obrony Narodowej, Administracji i Spraw Wewnętrznych oraz Komisji do Spraw Służb Specjalnych. Tematem spotkania był wyżej wymieniony projekt ustawy, potocznie nazywany wtedy „ws. bezpieczeństwa w cyberprzestrzeni”.

Sprawy nabrały tempa z momentem przesłania przez Prezydenta RP projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił

²⁴ *Prezydencki projekt ustawy o zmianie ustawy o stanie wojennym...*

*Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw do Marszałka Sejmu Rzeczypospolitej Polskiej*²⁵. 13 lipca 2011 r. na wspólnym posiedzeniu komisji sejmowych: Obrony Narodowej, Spraw Zagranicznych oraz Administracji i Spraw Wewnętrznych Stanisław Koziej, ówczesny szef BBN, w swoim wystąpieniu poprzedzającym ustanowienie zmiany w ustawach o stanach nadzwyczajnych mówił, że w cyberprzestrzeni należy uformować system bezpieczeństwa tak samo, jak jest on zorganizowany w geoprzestrzeni²⁶. Ponadto odpowiedział na pytanie: dlaczego cyberprzestrzeń zostaje wprowadzona do porządku prawnego akurat w ustawach o stanach nadzwyczajnych? Jako główne motywy takiego działania wskazał:

- brak środków finansowych – wprowadzenie cyberprzestrzeni do obrotu prawnego w ustawach o stanach nadzwyczajnych nie wygeneruje nadprogramowych kosztów wynikających z potrzeby podjęcia konkretnych działań „tu i teraz”, dlatego pojawienie się nowej kategorii bezpieczeństwa nie spowoduje w tym zakresie dodatkowych barier;
- inicjatywę Prezydenta RP, w którego kompetencjach, zgodnie z ustawą zasadniczą, leży decyzja o ogłoszeniu stanów: wojennego i wyjątkowego – stąd wynika jego odpowiedzialność za doprecyzowanie katalogu przesłanek do wprowadzenia tych instytucji;
- potrzebę jak najszybszych zmian wynikającą z nowych wyzwań dla bezpieczeństwa państwa²⁷.

Kolejnym etapem prac było wspólne posiedzenie Komisji Obrony Narodowej, Komisji Spraw Zagranicznych oraz Komisji Administracji i Spraw Wewnętrznych, które odbyło się w Sejmie 17 sierpnia 2011 r. Przedmiotem obrad było rozpatrzenie sprawozdania podkomisji nadzwyczajnej z 26 lipca dotyczące przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy. Członkowie komisji dyskutowali o celowości prezydenckiej inicjatywy i zasadności definiowania cyberprzestrzeni w polskim porządku prawnym, uwzględniając analizę systemów prawnych innych państw i prawa Unii Europejskiej²⁸. Ostatecznie sprawozdanie podkomisji zostało przyjęte – z poprawką konkretyzującą definicję zewnętrznego zagrożenia państwa. Jednocześnie zakończył się kolejny etap prac parlamentarnych w tym zakresie²⁹.

²⁵ Przesłanie projektu w ramach przysługującej Prezydentowi RP inicjatywy ustawodawczej miało miejsce 10 czerwca 2011 r. Zob. *Opracowany w BBN projekt ustawy o cyberbezpieczeństwie przesłany do Sejmu*, Biuro Bezpieczeństwa Narodowego, 13 VI 2011, [online] <https://www.bbn.gov.pl/wydarzenia/3087,OpracowanywBBNprojektustawyocyberbezpieczenstwieprzeslanydoSejmu.html>, 12 XI 2018.

²⁶ *Cyberprzestrzeń w ustawach o stanach nadzwyczajnych*, Biuro Bezpieczeństwa Narodowego, [online] <https://www.bbn.gov.pl/pl/wolnytekst/3237,Cyberprzestrzen-w-ustawach-o-stanach-nadzwyczajnych.html>, 11 XII 2018.

²⁷ *Tamże*.

²⁸ *Kolejne posiedzenie Komisji Sejmowych na temat cyberbezpieczeństwa*, Biuro Bezpieczeństwa Narodowego, 17 VIII 2011, [online] <https://www.bbn.gov.pl/pl/wydarzenia/3306,KolejneposiedzenieKomisjiSejmowychnatematcyberbezpieczenstwa.html>, 15 XII 2018.

²⁹ *Tamże*.

30 sierpnia 2011 r. ustawa została przyjęta przez Sejm. Z 405 obecnych posłów poparło ją 274, przeciw było 131, nikt nie wstrzymał się od głosu. Poniższa tabela przedstawia wyniki głosowania – z podziałem na kluby/koła – nad przyjęciem w całości projektu ustawy *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*, w brzmieniu proponowanym przez Komisję Administracji i Spraw Wewnętrznych, Komisję Obrony Narodowej oraz Komisję Spraw Zagranicznych.

Tabela 1. Głosowanie nr 4 – posiedzenie 99. dn. 30.08.2011, godz. 09.10

Klub/ Koło	Liczebność	Głosowało	Za	Przeciw	Wstrzymało się	Nie głosowało
PO	208	192	192	-	-	16
PiS	147	130	1	129	-	17
SLD	43	40	40	-	-	3
PSL	31	25	25	-	-	6
niez.	14	8	7	1	-	6
PJN	14	8	7	1	-	6
SDPL	3	2	2	-	-	1

Źródło: *Głosowania*, [online] <http://orka.sejm.gov.pl/SQL.nsf/glosowania?OpenAgent&6&99&4>, 21 XI 2018.

Z tabeli wynika, że prezydencki projekt ustawy poparły wszystkie kluby z wyjątkiem Prawa i Sprawiedliwości (PiS). W sejmowej debacie, w dniu poprzedzającym głosowanie, Jarosław Zieliński z PiS wskazywał, że wprowadzenie definicji cyberprzestrzeni nie przyczyni się do poprawy bezpieczeństwa, zwłaszcza że w projekcie nie zawarto mechanizmów zwalczania cyberzagrożeń. Dodatkowo, zdaniem posła Zielińskiego, jakość tego projektu obniżała rangę urzędu Prezydenta Rzeczypospolitej Polskiej³⁰. W innym tonie wypowiadał się szef BBN, co jest oczywiste z uwagi na jego udział w tworzeniu projektu zmian. Stanisław Koziej przekonywał, że celem tego przedsięwzięcia jest zwrócenie uwagi na problematykę cyberbezpieczeństwa. Podkreślał, że dzięki proponowanej ustawie rozpoczną się konkretne prace związane z przygotowaniem państwa polskiego do działań w cyberprzestrzeni (do walki z nowymi zagrożeniami): budowa i organizacja struktur na wszystkich poziomach funkcjonowania państwa³¹.

13 września 2011 r. Senat przyjął ustawę bez poprawek. Warto jednak zwrócić uwagę na sformułowanie, które znalazło się w opinii do tego dokumentu:

³⁰ *Sprawozdanie stenograficzne z 99 posiedzenia Sejmu Rzeczypospolitej Polskiej w dniu 29 sierpnia 2011 r.*, Sejm RP, VI kadencja, Warszawa 2011, [online] [http://orka2.sejm.gov.pl/StenoInter6.nsf/0/F46671890CD730FAC12578FC0004679D/\\$file/99_a_ksiazka.pdf](http://orka2.sejm.gov.pl/StenoInter6.nsf/0/F46671890CD730FAC12578FC0004679D/$file/99_a_ksiazka.pdf), 12 XI 2018.

³¹ *Tamże*.

przedmiotowa regulacja wprowadza w ustawach dotyczących tzw. stanów nadzwyczajnych definicję cyberprzestrzeni. Jest to pojęcie, które dotychczas nie zostało zdefiniowane w systemie prawnym. W związku z powyższym powstaje wątpliwość, co do zasadności wprowadzenia definicji cyberprzestrzeni jako potencjalnego terminu ściśle technicznego w poszczególnych ustawach regulujących możliwość wprowadzenia określonego stanu nadzwyczajnego³².

27 września 2011 r. Prezydent Rzeczypospolitej Polskiej podpisał ustawę 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. Weszła ona w życie 2 listopada 2011 r. Dokument uzupełnia wszystkie trzy ustawy o stanach nadzwyczajnych o kwestie związane z działaniami w cyberprzestrzeni, m.in. poprzez wprowadzenie jednolitej definicji słowa „cyberprzestrzeń”.

Tabela 2. Kalendarium prac nad ustawą 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

Data	Etapy procesu legislacyjnego
30 V 2011 r.	Posiedzenie Rady Bezpieczeństwa Narodowego dotyczące m.in. cyberbezpieczeństwa
08 VI 2011 r.	Spotkanie Prezydenta Rzeczypospolitej Polskiej z szefami sejmowych komisji: Komisji Obrony Narodowej, Komisji Administracji i Spraw Wewnętrznych oraz Komisji do Spraw Służb Specjalnych
10 VI 2011 r.	Przesłanie projektu ustawy do Sejmu
13 VII 2011 r.	Wspólne posiedzenie komisji sejmowych: Komisji Obrony Narodowej, Komisji Spraw Zagranicznych, Komisji Administracji i Spraw Wewnętrznych. Pierwsze czytanie projektu
26 VII 2011 r.	Posiedzenie podkomisji nadzwyczajnej
17 VIII 2011 r.	Kolejne wspólne posiedzenie Komisji Obrony Narodowej, Komisji Spraw Zagranicznych oraz Komisji Administracji i Spraw Wewnętrznych. Rozpatrzenie sprawozdania komisji nadzwyczajnej
30 VIII 2011 r.	Przyjęcie ustawy przez Sejm
13 IX 2011 r.	Przyjęcie ustawy przez Senat
27 IX 2011 r.	Podpisanie ustawy przez Prezydenta Rzeczypospolitej Polskiej Bronisława Komorowskiego

Źródło: *Prezydent podpisał ustawę o cyberbezpieczeństwie*, [online] <https://www.bbn.gov.pl/pl/wydarzenia/3407,Prezydent-podpisał-ustawe-o-cyberbezpieczenstwie.html>, 11 XI 2018.

³² *Opinia do ustawy 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*, Kancelaria Senatu RP, Druk nr 1350, Warszawa, 1 IX 2011, [online] <https://www.senat.gov.pl/prace/senat/posiedzenia/tematy,265,1.html>, 13 XII 2018.

STAN WOJENNY

Zgodnie z Konstytucją RP stan wojenny może być wprowadzony w sytuacji zaistnienia jednej z trzech przesłanek: zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji³³. Zgodnie z przepisami *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* pierwsza z wymienionych przesłanek, czyli zagrożenie zewnętrzne, może być spowodowana działaniami w cyberprzestrzeni.

Nowelizacja z 2011 r. wprowadziła do ustawy definicje zagrożenia zewnętrznego i cyberprzestrzeni. Zgodnie z jej art. 2 ust. 1a zagrożenie zewnętrzne to *celowe działania, godzące w niepodległość, niepodzielność terytorium, ważny interes gospodarczy Rzeczypospolitej Polskiej lub zmierzające do uniemożliwienia albo poważnego zakłócenia normalnego funkcjonowania państwa, podejmowane przez zewnętrzne w stosunku do niej podmioty*³⁴. Przez cyberprzestrzeń rozumie się *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3³⁵ ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570) wraz z powiązaniem pomiędzy nimi oraz relacjami z użytkownikami*³⁶. Definicja ta budzi wątpliwości części ekspertów, którzy wskazują, że jest ona niewystarczająco precyzyjna, co z kolei może implikować nadużycia ze strony władz, a konkretnie wykorzystanie instytucji stanu nadzwyczajnego w przypadku niegroźnego incydentu w cyberprzestrzeni. Nie sposób się jednak zgodzić z tym stanowiskiem, gdyż wszystkie trzy przesłanki wprowadzenia stanu wojennego muszą być analizowane w kontekście art. 228 ust. 1 Konstytucji RP, co oznacza, że może on zostać ogłoszony wyłącznie w sytuacjach szczególnych zagrożeń, jeżeli zwykle środki konstytucyjne są niewystarczające. Ten przepis w Konstytucji wyklucza niebezpieczeństwo nadużyć. Ponadto ustawodawca w definicji cyberprzestrzeni wyszczególnia jej komponenty w postaci systemów teleinformatycznych. W dzisiejszych czasach od współpracujących ze sobą odpowiednich urządzeń informatycznych i oprogramowania w dużej mierze zależy poprawne funkcjonowanie organów bezpośrednio odpowiedzialnych za

³³ Art. 229 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483.

³⁴ Art. 2 ust. 1a *Ustawy z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, Dz.U. 2002, nr 156, poz. 1301.

³⁵ System teleinformatyczny – 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 w rozumieniu przepisów *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*, Dz. U. 2016, poz.: 1489, 1579, 1823, 1948, 1954 i 2003.

³⁶ *Tamże*, art. 2 ust. 1b.

bezpieczeństwo państwa³⁷. Systemy sieci teleinformatycznych są jednym ze składników infrastruktury krytycznej państwa, wymienionych w *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*³⁸. Wydaje się, że stan wojenny mógłby zostać wprowadzony właśnie w celu przywrócenia normalnego funkcjonowania państwa po zakłóceniu lub uszkodzeniu jego infrastruktury krytycznej – do czego doszłoby w wyniku działań zewnętrznych podmiotów w cyberprzestrzeni – kiedy zwykle siły i środki byłyby niewystarczające. Należy pamiętać, że aby zakwalifikować takie poczynania jako zewnętrzne zagrożenie, pozwalające na zastosowanie owej instytucji, muszą one mieć następujące cechy:

- celowość,
- uderzenie w niepodległość, niepodzielność terytorium, ważny interes gospodarczy Polski lub uniemożliwienie albo poważne zakłócenie normalnego funkcjonowania państwa,
- inicjatywa podmiotów zewnętrznych względem Rzeczypospolitej Polskiej.

Wbrew pozorom przy obecnej informatyzacji życia społecznego oraz rozwoju nowoczesnych technologii przedstawiony scenariusz nie wydaje się wykluczony. Wystarczy wziąć pod uwagę nową formę konfliktu, jaką jest cyberwojna. Według części badaczy był nią zmasowany cyberatak na Estonię w 2007 r., w wyniku którego zablokowane zostały strony internetowe sektora publicznego oraz prywatnego i usługi, w tym działu bankowości i ratownictwa medycznego. Zdaniem innych, aby wydarzenie uznać za cyberwojnę, muszą wystąpić: śmiertelność, instrumentalność i polityczna motywacja³⁹. Bez względu na spory definicyjne cyberatak na Estonię był celowy i zgodnie z tym, co udało się ustalić, zainicjowała go Federacja Rosyjska. Tallin poradził sobie z odparciem napaści i zastosowanie szczególnych środków nie było konieczne, ale warto w zarysowanym kontekście rozważyć potencjalny scenariusz cyberataku, np. przy wykorzystaniu metody *swarming attack*. Polega ona na spiętrzeniu i nałożeniu na siebie działań wymierzonych w infrastrukturę krytyczną państwa (prowadzonych w cyberprzestrzeni oraz fizycznie), przeciwko jej materialnym nośnikom⁴⁰. Przykładowo, w wyniku zmasowanego ataku mogłoby dojść do przerwania ciągłości działania administracji publicznej, co z kolei – gdyby było przeprowadzone przez podmioty zewnętrzne, np. inny kraj – należałoby uznać za zablokowanie normalnego funkcjonowania państwa, a więc za zagrożenie zewnętrzne. Gdyby konstytucyjne siły i środki okazały się niewystarczające do przywrócenia poprawnego działania państwa, to prawdopodobne, że w takiej sytuacji konieczne byłoby wprowadzenie stanu wojennego.

Pozostałe przesłanki ogłoszenia stanu wojennego z art. 229 Konstytucji nie są przedmiotem niniejszego artykułu, jednak warto wspomnieć, iż drugą sytuacją, której

³⁷ A. Bujak, M. Witkowski, *Systemy teleinformatyczne wykorzystywane na potrzeby kierowania bezpieczeństwem państwa*, „Logistyka” 2014, vol. 6, [online] <https://www.czasopismologistyka.pl/artykuly-naukowe/send/319-artykuly-na-plycie-cd-6/5494-artykul>, 12 XII 2018.

³⁸ Dz.U. 2007, nr 89, poz. 590.

³⁹ T. Rid, *Cyber War Will Not Take Place*, „The Journal of Strategic Studies” 2012, vol. 35, nr 1, s. 6.

⁴⁰ D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, przeł. K. Masłowski, Gliwice 2004, s. 300.

zaistnienie umożliwiła odwołanie się do tej instytucji, jest zbrojna napaść na terytorium Rzeczypospolitej Polskiej, co jest bliskie określone w art. 116 Konstytucji stanowi wojny, o którym decyduje Sejm. Różnica dotyczy zakresu regulacji. Stan wojenny odnosi się do wewnętrznego bezpieczeństwa państwa i zabezpieczenia publicznego, natomiast stan wojny ma bezpośredni związek z obronnością państwa i jest instytucją z zakresu międzynarodowego prawa publicznego⁴¹.

Trzecim uzasadnieniem wprowadzenia stanu wojennego jest zobowiązanie Rzeczypospolitej Polskiej, na mocy umowy międzynarodowej, do wspólnej obrony przeciwko agresji. Ta przesłanka również występuje już we wcześniejszych przepisach ustawy zasadniczej – w art. 116 ust. 2 – i stanowi podstawę do podjęcia przez Sejm uchwały o stanie wojny.

Decyzja o ogłoszeniu stanu wojennego należy do Prezydenta RP. Poprzedza ją wniosek Rady Ministrów, w którym określone są przyczyny i obszar, na którym ma zostać wprowadzony, a także odpowiednie rodzaje ograniczeń wolności i praw człowieka i obywatela⁴². Po niezwłocznym rozpatrzeniu wniosku Prezydent RP wydaje rozporządzenie o wprowadzeniu stanu wojennego. Ma prawo także odmówić jego wydania. Decyzja egzekutywy podlega kontroli sejmowej. W ciągu 48 godzin Prezydent przedstawia rozporządzenie Sejmowi, który niezwłocznie je rozpatruje i może uchylić bezwzględłą większością głosów w obecności co najmniej połowy ustawowej liczby posłów⁴³. Podsumowując, stan wojenny jest instytucją, która chroni państwo przed klasycznym zagrożeniem zewnętrznym⁴⁴.

STAN WYJĄTKOWY

Zgodnie z art. 230 Konstytucji RP stan wyjątkowy może być wprowadzony w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego. Przesłanki wskazują, że warunkiem jest tu wystąpienie zagrożenia wewnętrznego, którego nie sposób usunąć poprzez użycie zwykłych środków konstytucyjnych.

W znowelizowanej w 2011 r. *Ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym* wskazano dodatkowo, że działania w cyberprzestrzeni mogą być podstawą do wprowadzenia stanu wyjątkowego. Bez wątplenia przesłanki w tym wypadku są trudno definiowalne. Jak wskazuje Krzysztof Prokop, nie posiadają one oparcia w obowiązującym prawodawstwie (brak definicji legalnych)⁴⁵, co daje organom egzekutywy większą

⁴¹ L. Mażewski, *Stany nadzwyczajne...*, s. 8.

⁴² Art. 2 ust. 2 *Ustawy z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, Dz.U. 2002, nr 156, poz. 1301.

⁴³ Art. 231 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Dz.U. 1997, nr 78, poz. 483.

⁴⁴ M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016, s. 182.

⁴⁵ *Tamże*, 202.

możliwość zastosowania omawianej instytucji⁴⁶. Należy jednak pamiętać, że pomimo iż wprowadzenie stanu wyjątkowego z pewnością należy do decyzji politycznych, które zostaną zweryfikowane – zarówno przez historyków, jak i Trybunał Stanu – następnie, dopiero w przyszłości, w przypadku ogłoszenia każdej z trzech kategorii stanu nadzwyczajnego organy władzy publicznej obowiązują następujące zasady: wyjątkowości, legalności, proporcjonalności, celowości, ochrony podstaw systemu prawnego i organów przedstawicielskich⁴⁷.

Z zagrożeniem konstytucyjnego ustroju państwa mamy do czynienia w sytuacji zamachu na instytucje rangi konstytucyjnej, np. zbrojnego zamachu stanu⁴⁸. Drugą przesłanką, czyli zagrożenie bezpieczeństwa obywateli, ma miejsce w sytuacji zagrożenia życia, zdrowia lub mienia w znacznych rozmiarach. Ostatnią przyczyną, czyli zagrożenie porządku publicznego, budzi największe zastrzeżenia z uwagi na nieostrość definicji. Pojęcie „porządek publiczny” występuje w różnych gałęziach prawa. Zdaniem Krzysztofa Prokopa na ten warunek można się powołać, gdy sytuacja uzasadniająca wprowadzenie stanu wyjątkowego jest na tyle złożona, że nie da się jej uargumentować tylko zagrożeniem konstytucyjnego ustroju lub bezpieczeństwa obywateli⁴⁹.

W ustawie o stanie wyjątkowym definicja cyberprzestrzeni jest taka sama jak w ustawie o stanie wojennym. Działanie w cyberprzestrzeni, które miałyby powodować ogłoszenie opisywanej instytucji, bez wątpienia będzie się mieścić w kategoriach świadomej działalności człowieka. Ponadto zagrożenie wewnętrzne powstałe w jego wyniku nie jest możliwe do usunięcia poprzez użycie zwykłych środków konstytucyjnych⁵⁰. Tak jak w przypadku stanu wojennego, z wnioskiem o wprowadzenie stanu wyjątkowego występuje Rada Ministrów. Prezydent RP podejmuje decyzję i wydaje rozporządzenie, które podlega kontroli Sejmu w trybie określonym w art. 231 Konstytucji RP.

STAN KLĘSKI ŻYWIŁOWEJ

W przeciwieństwie do dwóch pozostałych stanów nadzwyczajnych i przyczyn ich wprowadzenia wystąpienie klęski żywiołowej jest zazwyczaj niezależne od ludzkiej woli⁵¹. Zastosowanie instytucji stanu klęski żywiołowej pozwala na uruchomienie nadzwyczajnych działań władz, nie powodując jednocześnie tak rozległych skutków

⁴⁶ *Tamże*.

⁴⁷ Zob. M. Frańczuk, *Zagrożenia bezpieczeństwa i porządku publicznego działaniami w cyberprzestrzeni jako przesłanką wprowadzenia stanów nadzwyczajnych ze szczególnym uwzględnieniem bezpieczeństwa finansowego*, „Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie” 2014, nr 2(926), s. 80.

⁴⁸ M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa...*, s. 202.

⁴⁹ *Tamże*.

⁵⁰ Art. 2 ust. 1 *Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym*, Dz.U. 2002, nr 117, poz. 985.

⁵¹ K. Prokop, *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Białyłstok 2005, s. 101.

prawnych jak w sytuacjach wprowadzenie stanu wojennego czy stanu wyjątkowego⁵². Zgodnie z art. 232 Konstytucji dopuszcza się ogłoszenie stanu klęski żywiołowej w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia.

Ustawodawca definiuje klęskę żywiołową jako katastrofę naturalną lub awarię techniczną, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, przy czym pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji podlegających jednolitemu kierownictwu⁵³.

W znowelizowanej treści *Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej* doprecyzowano, iż wśród zdarzeń wywołujących katastrofę naturalną lub awarię techniczną znajdują się także te, które dotyczą cyberprzestrzeni⁵⁴. Należą do nich zdarzenia związane z działaniem sił natury, w szczególności: wyładowania atmosferyczne, wstrząsy sejsmiczne, silne wiatry, intensywne opady atmosferyczne, długotrwałe występowanie ekstremalnych temperatur, osuwiska ziemi, pożary, susze, powodzie, zjawiska lodowe na rzekach i morzu oraz jeziorach i zbiornikach wodnych, masowe występowanie szkodników, chorób roślin lub zwierząt albo chorób zakaźnych ludzi, albo też działanie innego żywności⁵⁵. Awaria techniczna to gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich używaniu lub utratę ich właściwości⁵⁶.

Najprościej jest wyobrazić sobie cyberatak przeprowadzony z dowolnego miejsca, przy użyciu niewielkich nakładów finansowych, który skutkuje awarią techniczną. Biorąc pod uwagę ustawowy *definiens* awarii technicznej, należy stwierdzić, że tego rodzaju napadzi mogą spowodować zarówno uszkodzenia i zniszczenia obiektów budowlanych, jak i urządzeń technicznych czy też całych systemów urządzeń technicznych, np. systemy kontroli lotów, systemów ratownictwa, zaopatrzenia w wodę.

Znane są przypadki eksplozji, do których doszło wskutek działań w cyberprzestrzeni, np. wybuch ropociągu (BTC – Baku–Tbilisi–Ceyhan) łączącego Azerbejdżan z Morzem Śródziemnym, z pominięciem Federacji Rosyjskiej. Wybuchy to jedna z metod, która potencjalnie doprowadza do zniszczeń obiektów budowlanych wskutek działań w cyberprzestrzeni, np. szpitali, szkół i wielu innych miejsc, w których zagrożone jest życie i zdrowie ludzkie. Podobnie rzecz się ma ze zniszczeniem urządzeń technicznych – mogą być dokonane np. przy wykorzystaniu złośliwego oprogramowania. Oczywiście, aby uznać tego typu działania za noszące znamiona klęski żywiołowej, ich

⁵² W. Skrzydło, *Konstytucja...*, s. 315.

⁵³ Art. 3 ust. 1 pkt 1 *Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*, Dz.U. 2002, nr 62, poz. 558.

⁵⁴ *Tamże*, art. 3 ust. 2.

⁵⁵ *Tamże*, art. 3 ust. 1 pkt 2.

⁵⁶ *Tamże*, art. 3 ust. 1 pkt 3.

skutki muszą zagrażać życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, a żeby wprowadzić stan klęski żywiołowej dodatkowo zwykłe siły i środki powinny się okazać niewystarczające do eliminacji zagrożenia i usunięcia skutków zdarzenia.

Ustawodawca wskazuje także na niebezpieczeństwo wystąpienia katastrof naturalnych w wyniku zdarzenia w cyberprzestrzeni. Bez wątpienia jest to mniej prawdopodobne niż przy awariach technicznych, jednak także możliwe. Wydaje się, że gdyby taki scenariusz faktycznie zaistniał, jego skutki byłyby bardzo trudne do opanowania. Przykładowo, za katastrofę naturalną uważa się masowe występowanie chorób zakaźnych. Jak wiadomo, ich przyczyną mogą być np. bakterie czy też wirusy. Gdyby haker włamał się do systemu informatycznego sterującego pracą lokalnego zakładu uzdatniania wody, nietrudno wyobrazić sobie sytuację, w której zmodyfikowałby skład mieszanki chemicznych substancji dodawanych do wody w celu uczynienia jej zdanej do picia. Efektem mogłoby być zatrucie wody i zagrożenie dla życia lub zdrowia ludzi na danym terytorium. Choć wydaje się, że ten przykład mieści się bardziej w kategorii *fiction* niż *science*, to stacja BBC w 2011 r. poinformowała o podobnych zajściach w stanie Illinois, gdzie cyberatak spowodował zniszczenie pompy, która doprowadzała wodę do tysięcy domów. Podobne zdarzenie miało miejsce w południowej części Houston w Teksasie⁵⁷. Tam dopuszczono się cyberataku na stację uzdatniania wody i oczyszczania ścieków, a przestępcy na skutek wielokrotnego włączania i wyłączania pompy doprowadzili do jej uszkodzenia⁵⁸. Choć życie i zdrowie ludzi nie zostało zagrożone, jest to wydarzenie, które obrazuje możliwości wykorzystania cyberprzestrzeni.

Wracając do polskiego ustawodawstwa – i w celu podsumowania niniejszych rozważań – warto dodać, że stan klęski żywiołowej wprowadza Rada Ministrów w drodze rozporządzenia, z własnej inicjatywy lub na wniosek właściwego wojewody, na całym terytorium kraju lub jego części na czas nie dłuższy niż 30 dni, przy czym może on być przedłużony za zgodą Sejmu⁵⁹.

PODSUMOWANIE

Dodanie działań w cyberprzestrzeni do katalogu przesłanek umożliwiających wprowadzenie stanów nadzwyczajnych wydaje się uzasadnione. Tak jak w przypadku terroryzmu, działania w cyberprzestrzeni mogą wywoływać zagrożenia zewnętrzne i wewnętrzne względem podmiotu państwowego, a w konsekwencji prowadzić do utraty zdrowia i życia obywateli. Dopiero ataki terrorystyczne w 2001 r. uruchomiły liczne zmiany w krajowych systemach prawnych, które muszą być dostosowane do nowych

⁵⁷ M. Goodman, *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, przeł. M. Lipa, Gliwice 2015, s. 29.

⁵⁸ *Hackers „hit” US water treatment systems*, „BBC News” 2011, 21 XI, [online] <https://www.bbc.com/news/technology-15817335>, 12 XII 2018.

⁵⁹ Art. 5 ust. 1 *Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*, Dz.U. 2002, nr 62, poz. 558.

typów zagrożeń. Warto próbować takie same działania podjąć w odniesieniu do potencjalnych incydentów w cyberprzestrzeni, ale zanim się wydarzą, a więc prewencyjnie.

Wprowadzenie pojęcia „cyberprzestrzeń” do języka prawnego było konieczne. Przemawiające za tym argumenty Biura Bezpieczeństwa Narodowego, które opierały się na niskich kosztach i braku czasu na inne rozwiązania, wydają się zasadne, przynajmniej w tamtym czasie, w 2011 r. Wybór ustaw o stanach nadzwyczajnych jako wprowadzających cyberprzestrzeń do powszechnego obiegu jest kwestionowany, jednak każda metoda jest dobra, by rozwijać system bezpieczeństwa, a bez wątplenia zauważanie zagrożeń w kolejnej płaszczyźnie wzajemnego oddziaływania na siebie podmiotów można nazwać postępek. Zasygnalizowanie potrzeby zmiany prawa, na którym miała się opierać budowa cyberbezpieczeństwa Rzeczypospolitej Polskiej, należy uznać za rozsądne. Niestety, w porównaniu do systemów prawnych innych krajów, nasze ustawodawstwo w tym zakresie nadal pozostaje ubogie. Zmiany nie nabrały tempa. Powstało kilka dokumentów, ale brak środków finansowych na rozwijanie potencjału ofensywnego i defensywnego w cyberprzestrzeni, a także spory kompetencyjne pomiędzy organami władzy państwowej jedynie pogarszają sytuację, w której znajduje się nasze państwo, a zatem my – obywatele – codziennie narażani na działania cyberprzestępców.

BIBLIOGRAFIA

- Bryk T., *Przegląd regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego” 2011, nr 1(5), <https://doi.org/10.15804/ppk.2011.01.11>.
- Brzeziński M., *Wybrane zasady stanów nadzwyczajnych w konstytucji z dnia 2 kwietnia 1997 r. – uwagi de lege lata i de lege ferenda*, „Studia Politologiczne” 2017, vol. 45.
- Bujak A., Witkowski M., *Systemy teleinformatyczne wykorzystywane na potrzeby kierowania bezpieczeństwem państwa*, „Logistyka” 2014, vol. 6, [online] <https://www.czasopismologistyka.pl/artykuly-naukowe/send/319-artykuly-na-plycie-cd-6/5494-artikul>.
- Cyberprzestrzeń w ustawach o stanach nadzwyczajnych*, Biuro Bezpieczeństwa Narodowego, [online] <https://www.bbn.gov.pl/pl/wolnytekst/3237,Cyberprzestrzen-w-ustawach-o-stanach-nadzwyczajnych.html>.
- Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.
- Dobrzeńcki K., *Filozofia prawa a stany nadzwyczajne – zarys problematyki*, [w:] *Stan nadzwyczajny. Analizy z perspektywy nauk politycznych i prawnych*, red. J. Markiewicz-Stanny, P. Łukomski, Zielona Góra 2015.
- Eckhardt K., *Hierarchizacja praw i wolności jednostki w świetle konstytucyjnej regulacji stanu nadzwyczajnego*, „Przegląd Prawa Konstytucyjnego” 2014, nr 2(18), <https://doi.org/10.15804/ppk.2014.02.06>.
- Frańczuk M., *Zagrożenia bezpieczeństwa i porządku publicznego działaniami w cyberprzestrzeni jako przesłanka wprowadzenia stanów nadzwyczajnych ze szczególnym uwzględnieniem bezpieczeństwa finansowego*, „Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie” 2014, nr 2(926), <https://doi.org/10.15678/ZNUEK.2014.0926.0205>.

- Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2010, *Seria Akademicka*.
- Gibson W., *Neuromancer*, Poznań 1996.
- Głosowania*, [online] <http://orka.sejm.gov.pl/SQL.nsf/glosowania?OpenAgent&6&99&4>.
- Goodman M., *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, przeł. M. Lipa, Gliwice 2015.
- Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe” 2012, nr 22.
- Hackers „hit” US water treatment systems, „BBC News” 2011, 21 XI, [online] <https://www.bbc.com/news/technology-15817335>.
- Kociołek-Pęksa A., Menkes J., *Międzynarodowe i krajowe prawne regulacje stanów nadzwyczajnych*, [w:] *Stan nadzwyczajny. Analizy z perspektywy nauk politycznych i prawnych*, red. J. Markiewicz-Stanny, P. Łukomski, Zielona Góra 2015.
- Kolejne posiedzenie Komisji Sejmowych na temat cyberbezpieczeństwa*, Biuro Bezpieczeństwa Narodowego, 17 VIII 2011, [online] <https://www.bbn.gov.pl/pl/wydarzenia/3306,KolejneposiedzenieKomisjiSejmowychnatematcyberbezpieczenia.html>.
- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Dz.U. 1997, nr 78, poz. 483.
- Kurzępa E., *Stany nadzwyczajne w polskim porządku prawnym*, Warszawa 2017, *Monografie Prawnicze*.
- Mażewski L., *Stany nadzwyczajne w Polsce w latach 1918-1989*, Toruń 2006.
- Opinia do ustawy 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*, Kancelaria Senatu RP, Druk nr 1350, Warszawa, 1 IX 2011, [online] <https://www.senat.gov.pl/prace/senat/posiedzenia/tematy,265,1.html>.
- Opracowany w BBN projekt ustawy o cyberbezpieczeństwie przesłany do Sejmu*, Biuro Bezpieczeństwa Narodowego, 13 VI 2011, [online] <https://www.bbn.gov.pl/pl/wydarzenia/3087,OpracowanywBBNprojektustawyocyberbezpieczenstwieprzeslanydoSejmu.html>
- Prezydencki projekt ustawy 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*, Sejm RP, VI kadencja, Prezydent RP, Druk nr 4355, Warszawa, 10 VI 2011, [online] [http://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/\\$file/4355.pdf](http://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/$file/4355.pdf).
- Prokop K., *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Białystok 2005.
- Rid T., *Cyber War Will Not Take Place*, „The Journal of Strategic Studies” 2012, vol. 35, nr 1, <https://doi.org/10.1080/01402390.2011.608939>.
- Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Zakamycze 2000.
- Sprawozdanie stenograficzne z 99 posiedzenia Sejmu Rzeczypospolitej Polskiej w dniu 29 sierpnia 2011 r.*, Sejm RP, VI kadencja, Warszawa 2011, [online] [http://orka2.sejm.gov.pl/StenoInter6.nsf/0/F46671890CD730FAC12578FC0004679D/\\$file/99_a_ksiazka.pdf](http://orka2.sejm.gov.pl/StenoInter6.nsf/0/F46671890CD730FAC12578FC0004679D/$file/99_a_ksiazka.pdf).
- Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*, Dz.U. 2016, poz.: 1489, 1579, 1823, 1948, 1954 i 2003.
- Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*, Dz.U. 2002, nr 62, poz. 558.
- Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym*, Dz.U. 2002, nr 117, poz. 985.

Ustawa z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002, nr 156, poz. 1301.

Verton D., *Black Ice. Niewidzialna groźba cyberterroryzmu*, przeł. K. Masłowski, Gliwice 2004.

Warden J.A., *The Enemy as a System*, „Airpower Journal” 1995, vol. 9, nr 1, [online] http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

Dr Agnieszka WARCHOŁ – doktor nauk społecznych w dyscyplinie nauk o polityce ze specjalnością polityka bezpieczeństwa. Adiunkt w Katedrze Bezpieczeństwa Wewnętrznego w Instytucie Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Zainteresowania naukowe: cyberbezpieczeństwo, współczesne koncepcje bezpieczeństwa, bezpieczeństwo informacyjne, sztuczna inteligencja. Autorka monografii naukowej *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku* oraz współautorka i redaktorka monografii, a także artykułów naukowych w zakresie współczesnych problemów bezpieczeństwa międzynarodowego i narodowego.