Jakub Rzucidło¹

Justyna Węgrzyn²

Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni

Słowa kluczowe: stany nadzwyczajne, stan wojenny, stan wyjątkowy, stan klęski żywiołowej, cyberprzestrzeń, cyberwojna, cyberprzestępstwa, cyberterroryzm

Keywords: extraordinary measures, state of emergency, state of martial law, state of natural disaster, cyberspace, cyberwar, cybercrimes, cyberterrorism

Streszczenie

W niniejszej publikacji Autorzy odnoszą się do instytucji stanów nadzwyczajnych w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni. Analiza tego zagadnienia dokonana jest w oparciu o rozwiązania konstytucyjne i ustawowe (ustawa o stanie wojennym, ustawa o stanie wyjątkowym, ustawa o stanie klęski żywiołowej). Autorzy odnoszą się do pojęcia cyberprzestrzeni oraz dokonują klasyfikacji zagrożeń w tym obszarze. Ponadto dokonują oceny zasadności uchwalonych przez prawodawcę środków.

Summary

Extraordinary measures in the event situations of particular danger in cyberspace

In the article the Authors presented a problem of extraordinary measures in the event situations of particular danger in cyberspace. The analysis of this issue is made on the

¹ Autor jest adiunktem w Zakładzie Zarządzania i Administracji Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości. E-mail: jakub.rzucidlo@gmail.com.

² Autorka jest adiunktem w Katedrze Systemów Ustrojowych i Praw Człowieka Wydziału Prawa i Administracji Uniwersytetu Zielonogórskiego. E-mail: j.wegrzyn@wpa.uz.zgora.pl.

basis of constitutional and legal solutions (Act of martial law, Act of the state of emergency, Act of the state of natural disaster). The Authors referred to the concept of cyberspace and classified the risks in this area. They also assessed the appropriateness of the measures adopted by the legislature.

I.

Współcześnie do zagrożeń globalnego bezpieczeństwa zalicza się terroryzm oraz zorganizowaną przestępczość. Ryzyko wystąpienia tych zjawisk istnieje nie tylko w świecie rzeczywistym, ale także i w wirtualnym. W tej drugiej sferze dostrzec należy nowe, jak i znane dotychczas, lecz ewoluujące patologie, takie jak cyberprzestępczość, cyberterroryzm, a nawet cyberwojna³, które pojawiły się na skutek rozwoju Internetu oraz nowych technik teleinformatycznych. Każde państwo może spotkać się z tego typu niebezpieczeństwami, zakłócającymi jego funkcjonowanie. Wobec tego, w zależności od rodzaju i zakresu zagrożeń państwo będzie mogło, a nawet będzie musiało, przedsięwziąć szczególne działania, wykraczające ponad te podejmowane w ramach zwykłych środków konstytucyjnych⁴. Tak jest w przypadku Rzeczypospolitej Polskiej, która nie pozostała obojętna wobec szczególnych zagrożeń w cyberprzestrzeni.

Przedstawiona w niniejszym artykule problematyka skupia się wokół zagadnień związanych z rozwiązaniami przyjętymi przez polskiego prawodawcę w celu umożliwienia wprowadzenia jednego ze stanów nadzwyczajnych w sytuacji wystąpienia szczególnego zagrożenia w cyberprzestrzeni. Stąd też konieczne jest zidentyfikowanie tego ostatniego pojęcia, w szczególności na gruncie regulacji ustawowej, oraz dokonanie oceny zasadności uchwalonych przez prawodawcę środków.

³ Pojęcia te zostaną wyjaśnione w dalszej części opracowania.

⁴ J. Stelmasiak, *Stany nadzwyczajne*, [w:] *Publicznoprawne podstawy bezpieczeństwa wewnętrznego*, red. M. Zdyb, Warszawa 2014, s. 153.

II.

Konstytucjonalizacja problematyki stanów nadzwyczajnych⁵ w polskim porządku prawnym została dokonana już w Konstytucji marcowej⁶, a mianowicie w jej art. 124. Przepis ten odnosił się do dwóch instytucji, tj. stanu wojennego oraz stanu wyjątkowego. Pierwszy z nich mógł być wprowadzony tylko przez Radę Ministrów (dalej: RM) za zgodą prezydenta Rzeczypospolitej Polskiej (dalej także: prezydent RP) podczas wojny lub w sytuacji wystąpienia groźby wybuchu wojny. Drugi „w razie rozruchów wewnętrznych lub rozległych knozań o charakterze zdrady stanu, zagrażających Konstytucji Państwa albo bezpieczeństwu obywateli”⁷.

Jak wynikało z treści wskazanego wyżej przepisu, zarządzenie wprowadzające stan nadzwyczajny musiało zostać niezwłocznie przedstawione Sejmowi do zatwierdzenia. W razie przerwy w obradach Sejm musiał zebrać się w ciągu 8 dni od ogłoszenia zarządzenia. Ponadto wprowadzenie każdego z dwóch stanów wymienionych w Konstytucji marcowej mogło skutkować czasowym zawieszeniem praw obywatelskich⁸. W zamkniętym katalogu tych praw wymieniono: wolność osobistą, nietykalność mieszkania, wolność prasy, tajemnicę korespondencji, prawo koalicji, zgromadzania się i zawiązywania stowarzyszeń.

Instytucja stanów nadzwyczajnych została także uregulowana w Konstytucji kwietniowej⁹, która przewidywała możliwość wprowadzenia stanu

⁵ Na temat pojęcia stanów nadzwyczajnych zobacz np. S. Gebethner, *Stany szczególnego zagrożenia jako instytucja prawa konstytucyjnego*, „Państwo i Prawo” 1982, z. 8; J. Stembrowicz, *Z problematyki stanu nadzwyczajnego w prawie konstytucyjnym*, „Więź” 1988, nr 11–12. Podajemy za: J. Stelmasiak, op.cit., s. 154.

⁶ Ustawa z dnia 17 marca 1921 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. Nr 44, poz. 267). Zaznaczyć jednak należy, że termin „stan nadzwyczajny” nie został wykorzystany przez ustrojodawcę aż do uchwalenia Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm.) (dalej także: Konstytucja RP lub ustawa zasadnicza).

⁷ Ibidem.

⁸ A. Paszkudzki, *Konstytucja Rzeczypospolitej Polskiej z dnia 17 marca 1921 r. z uwzględnieniem zmian ustalonych ustawą z dnia 2 sierpnia 1926 r. Komentarz*, Lwów–Warszawa 1927, s. 151. Podajemy za: M. Brzeziński, *Stany nadzwyczajne w polskich konstytucjach*, Warszawa 2007, s. 71.

⁹ Ustawa Konstytucyjna z dnia 23 kwietnia 1935 r. (Dz.U. Nr 30, poz. 227).

wojennego¹⁰ oraz stanu wyjątkowego¹¹. W porównaniu z poprzednią ustawą zasadniczą możemy dostrzec, że w obszarze interesującego nas zagadnienia nie wprowadzono zasadniczych zmian merytorycznych.

Pewne modyfikacje w zakresie regulacji stanów nadzwyczajnych widoczne były w Konstytucji Polskiej Rzeczypospolitej Ludowej¹² (dalej: Konstytucja PRL lub Konstytucja z 1952 r.). Wynikały one z tego, że początkowo Konstytucja PRL odnosiła się tylko do instytucji stanu wojennego¹³. Potwierdzeniem tego był art. 28, który stanowił, że postanowienie o stanie wojny mogło być powzięte jedynie w razie dokonania zbrojnego napadu

¹⁰ Art. 79 Ustawy Konstytucyjnej z dnia 23 kwietnia 1935 r. stanowił:

„Ust. 1. W razie konieczności użycia sił zbrojnych do obrony Państwa Prezydent Rzeczypospolitej zarządzi stan wojenny na obszarze całego Państwa lub jego części.

Ust. 2. Podczas trwania stanu wojennego Prezydent Rzeczypospolitej ma prawo bez upoważnienia Izb Ustawodawczych wydawać dekrety w zakresie ustawodawstwa państwowego z wyjątkiem zmiany Konstytucji, przedłużyć kadencję Izb Ustawodawczych do czasu zawarcia pokoju oraz otwierać, odraczać i zamykać sesje Sejmu i Senatu w terminach, dostosowanych do potrzeb obrony państwa, jak również powoływać do rozstrzygania spraw, wchodzących w zakres działania Izb Ustawodawczych, Sejm i Senat w zmniejszonym składzie, wyłonionym przez te Izby.

Ust. 3. W czasie trwania stanu wojennego Rząd korzysta z uprawnień, przewidzianych ustawą o stanie wyjątkowym, a nadto z uprawnień szczególnych, określonych ustawą o stanie wojennym”.

¹¹ Art. 78 Ustawy Konstytucyjnej z dnia 23 kwietnia 1935 r. stanowił: „Ust. 1. W razie zagrożenia Państwa z zewnątrz, jak również w razie rozruchów wewnętrznych lub rozległych knowań o charakterze zdrady stanu, zagrażających ustrojowi lub bezpieczeństwu Państwa albo bezpieczeństwu obywateli – Rada Ministrów za zezwoleniem Prezydenta Rzeczypospolitej zarządzi stan wyjątkowy na obszarze całego Państwa lub części zagrożonej. Ust. 2. Zarządzenie takie będzie przesłane do Sejmu w ciągu siedmiu dni od ogłoszenia. Ust. 3. Jeżeli Sejm jest rozwiązany, zarządzenie o ogłoszeniu stanu wyjątkowego będzie złożone nowoobranemu Sejmowi na pierwszym posiedzeniu. Ust. 4. Sejm może zażądać uchylecia zarządzenia. Ust. 5. Wniosek taki nie może być głosowany na posiedzeniu, podczas którego został zgłoszony. Ust. 6. Jeżeli Senat wypowie się za uchwałą Sejmu, Rząd niezwłocznie uchyli zarządzenia. Ust. 7. Ogłoszenie stanu wyjątkowego daje Rządowi prawo zawieszenia na czas trwania tego stanu swobód obywatelskich oraz możliwość korzystania z uprawnień szczególnych, przewidzianych ustawą o stanie wyjątkowym”.

¹² Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 r. (Dz.U. Nr 33, poz. 232).

¹³ Zobacz na ten temat L. Mażewski, *Bezpieczeństwo publiczne. Stany nadzwyczajne w Rzeczypospolitej Polskiej oraz Polskiej Rzeczypospolitej Ludowej 1918–2009*, Toruń 2010, s. 130 i n.

na Polską Rzeczpospolitą Ludową (dalej: PRL) albo gdy z umów międzynarodowych wynikała konieczność wspólnej obrony przeciwko agresji. Postanowienie takie musiało być uchwalone przez Sejm, a gdy Sejm nie obradował, dokonywała tego Rada Państwa. Rada Państwa mogła wprowadzić stan wojenny na części lub na całym terytorium PRL, jeżeli wymagał tego wzgląd na obronność lub bezpieczeństwo państwa¹⁴. Z tych samych powodów Rada Państwa mogła ogłosić częściową lub powszechną mobilizację.

W późniejszym czasie, tj. w 1983 r., na skutek zmian, jakich dokonano w Konstytucji z 1952 r., możliwe stało się wprowadzenie oprócz stanu wojennego także stanu wyjątkowego, którego regulacja prawna znalazła swoje odzwierciedlenie także w ustawie o stanie wyjątkowym¹⁵. „Taki stan prawny utrzymał się aż do 1997 r. Nowela kwietniowa z 1989 r., a potem Mała Konstytucja z 1992 r., nie wprowadziły bowiem istotniejszych zmian, choć poddały wprowadzenie stanu wyjątkowego pewnym rygorom, w szczególności ograniczając czas jego trwania do trzech miesięcy, a ewentualne przedłużenie uzależniając od zgody Sejmu”¹⁶.

Jak wynika z powyższych rozwiązań obowiązujących na przestrzeni kilkudziesięciu lat, zagadnienie stanów nadzwyczajnych było w mniejszym lub większym zakresie uregulowane w obowiązującej w określonym czasie ustawie zasadniczej. W obecnie obowiązującej Konstytucji RP, w której stanom nadzwyczajnym poświęcono odrębny rozdział, możemy dostrzec, że ustrojodawca w zdecydowanie szerszym stopniu uregulował tę problematykę.

¹⁴ Zob. w szczególności wyrok Trybunału Konstytucyjnego (dalej także: TK) z dnia 16 marca 2011 r., sygn. akt K 38/05, w którym to TK uznał m.in., że dekret z dnia 12 grudnia 1981 r. o stanie wojennym (Dz.U. Nr 29, poz. 154) jest niezgodny z art. 7 Konstytucji Rzeczypospolitej Polskiej w związku z art. 31 ust. 1 Konstytucji Polskiej Rzeczypospolitej Ludowej uchwalonej przez Sejm Ustawodawczy w dniu 22 lipca 1952 r. (Dz.U. 1976, Nr 7, poz. 36) oraz z art. 15 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, otwartego do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977, Nr 38, poz. 167), oraz że dekret z dnia 12 grudnia 1981 r. o postępowaniach szczególnych w sprawach o przestępstwa i wykroczenia w czasie obowiązywania stanu wojennego (Dz.U. Nr 29, poz. 156), jest niezgodny z art. 7 Konstytucji RP w związku z art. 31 ust. 1 Konstytucji PRL oraz z art. 15 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych. Wyrok dostępny jest w bazie Orzeczenia Trybunału Konstytucyjnego, pod adresem: http://otk.trybunal.gov.pl/orzeczenia/ezd/sprawa_lista_plikow.asp?syg=K%2035/08 (8.02.2015).

¹⁵ L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2009, s. 392.

¹⁶ Ibidem.

W art. 228 ust. 1 postanowił, że wprowadzenie stanu nadzwyczajnego jest możliwe w sytuacji szczególnych zagrożeń, które należy rozpatrywać przez pryzmat art. 229¹⁷, art. 230 ust. 1¹⁸ i art. 232¹⁹, bowiem to w tych przepisach wyrażone zostały przesłanki, jakie muszą zostać spełnione, aby można było wprowadzić tego rodzaju instytucję – i po stwierdzeniu, że zwykle środki konstytucyjne są niewystarczające. Ponadto, zgodnie z wyrażoną w art. 228 ust. 2 Konstytucji RP zasadą legalizmu, stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.

Wprowadzenie stanu nadzwyczajnego wiąże się ze zmianą funkcjonowania organów władzy publicznej, co nie jest równoznaczne ze zmianą ich ustroju²⁰. Modyfikacja sposobu funkcjonowania tych organów przejawia się – w tym przypadku – w zachodzących między nimi relacjach prawnych, polegających na „wyeksponowaniu roli organów administracyjnych poprzez rozbudowę ich kompetencji nadzorczych i kontrolnych”²¹. Ważne przy tym jest, że zakres działania organów władzy publicznej w czasie trwania szczególnych zagrożeń jest uregulowany w drodze ustawy. W ten sam sposób uregulowana jest kwestia dotycząca ograniczenia wolności i praw człowieka i obywatela²². W tym aspekcie szczególnie ważna jest treść art. 233 Konstytucji.

¹⁷ W art. 229 Konstytucji RP ustrojodawca wskazał trzy przesłanki wprowadzenia stanu wojennego. Są to: 1. zewnętrzne zagrożenia państwa; 2. zbrojna napaść na terytorium RP; 3. wynikające z umowy międzynarodowej zobowiązania do wspólnej obrony przeciwko agresji.

¹⁸ W art. 230 ust. 1 Konstytucji RP wskazano, że stan wyjątkowy może zostać wprowadzony w razie zagrożenia: 1. konstytucyjnego ustroju państwa; 2. bezpieczeństwa obywateli lub 3. porządku publicznego.

¹⁹ W art. 232 Konstytucji RP wskazano, że stan klęski żywiołowej wprowadza się na części albo na całym terytorium państwa w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia.

²⁰ K. Prokop, *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Białystok 2005, s. 9.

²¹ K. Działocha, *Komentarz do art. 228, [w:] Konstytucja Rzeczypospolitej Polskiej. Komentarz*, T. V, red. L. Garlicki, Warszawa 2005, s. 8.

²² Mowa tu o ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. 2014, poz. 1815); ustawa z dnia 21 listopada 1967 r. o po-

tucji RP, która statuuje wprost, że w czasie stanu wojennego i wyjątkowego ustawa określająca zakres owych ograniczeń nie może ograniczać wolności i praw określonych w art. 30 (godność człowieka), art. 34 i art. 36 (obywatelstwa), art. 38 (ochrona życia), art. 39, art. 40 i art. 41 ust. 4 (humanitarne traktowanie), art. 42 (ponoszenie odpowiedzialności karnej), art. 45 (dostęp do sądu), art. 47 (dobra osobiste), art. 53 (sumienie i religia), art. 63 (petycje) oraz art. 48 i art. 72 (rodzina i dziecko). Przyjęcie takiego rozwiązania oznacza, że inne wolności i prawa człowieka i obywatela nie wymienione *expressis verbis* w art. 233 ust. 1 Konstytucji RP mogą zostać ograniczone. W procesie tym należy jednak wziąć pod uwagę wyrażony w art. 233 ust. 2 zakaz dyskryminacji. Przejawia się on w niedopuszczalności wprowadzenia jakichkolwiek ograniczeń z powodu rasy, płci, języka, wyznania lub jego braku, pochodzenia społecznego, urodzenia oraz majątku.

Odnosząc się do kwestii związanej ze zmianą sposobu funkcjonowania organów władzy publicznej w czasie stanu wojennego, należy zaznaczyć, że modyfikacje w tym zakresie wiążą się z trybem jego wprowadzenia. W tym czasie sprawowanie władzy należy do prezydenta RP, który sam może podjąć decyzję o wprowadzeniu tego stanu, ale na wniosek Rady Ministrów²³. Rozporządzenie prezydenta RP dotyczące wprowadzenia stanu wojennego, a także i stanu wyjątkowego, podlega następnie kontroli Sejmu. Tego typu akt prawa powszechnie obowiązującego musi zostać przekazany Sejmowi w ciągu 48 godzin od jego podpisania. Uznanie przez Sejm rozporządzenia za bezzasadne może skutkować jego uchyleniem bezwzględną większością głosów w obecności co najmniej połowy ustawowej liczby posłów²⁴. Za wyjątkiem powyższego uprawnienia prezydentowi RP przysługuje także prawo do wydawania rozporządzeń z mocą ustawy, z zachowaniem granic wyznaczonych zasadami legalności, celowości i proporcjonalności²⁵.

wszechnym obowiązku obrony Rzeczypospolitej Polskiej (t.j. Dz.U. 2012, poz. 461 ze zm.); ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. Nr 113, poz. 985 ze zm.).

²³ W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 209.

²⁴ Art. 231 Konstytucji RP.

²⁵ J. Jaskiernia, *Akty normatywne w stanach nadzwyczajnych*, [w:] *Konstytucyjny system źródeł prawa w praktyce*, red. A. Szmyt, Warszawa 2005, s. 140 i n.; B. Dzierżyński, *Rozporządzenia z mocą ustawy jako akty nadzwyczajnego ustawodawstwa delegowanego na tle konstytucji polskich – wybrane problemy*, „Przegląd Prawa i Administracji” 2003, t. LIV, s. 86; K. Prokop,

Działania organów władzy publicznej w drugim ze wskazanych wyżej stanów nadzwyczajnych, a więc stanie wyjątkowym, sprowadzają się do nałożenia na prezesa RM – w przypadku gdy zasięg terytorialny obejmuje obszar większy niż jedno województwo – obowiązku przedsięwzięcia takich czynności, które przywrócą konstytucyjny ustroj państwa, bezpieczeństwo obywateli lub porządek publiczny, a w szczególności koordynację i kontrolę funkcjonowania administracji rządowej i samorządowej²⁶. Ten sam obowiązek, który wynika wprost z przepisów ustawy o stanie wyjątkowym (dalej także: usw), odnosi się do właściwego wojewody, gdy stan nadzwyczajny, o którym mowa, obejmuje obszar lub część obszaru województwa²⁷. Zasady działania organów władzy publicznej określone zostały także w art. 11 usw, określającym kompetencje prezydenta RP, który na wniosek prezesa RM może postanowić o użyciu Sił Zbrojnych RP w celu przywrócenia normalnego funkcjonowania państwa, jeżeli dotychczasowe siły i środki zostały wyczerpane. Ponadto, co wynika z powołanej wyżej usw²⁸, prezes RM na wniosek wojewody może zawiesić organy samorządu terytorialnego i ustanowić w ich miejsce zarząd komisaryczny, który jest sprawowany przez komisarza rządowego.

Trzeci stan nadzwyczajny, tj. stan klęski żywiołowej²⁹, może zostać wprowadzony przez RM na czas oznaczony, nie dłuższy niż 30 dni, na części albo na całym terytorium państwa, przy czym przedłużenie tego terminu może nastąpić za zgodą Sejmu³⁰. W porównaniu do poprzednich stanów nadzwyczajnych widzimy, że organem uprawnionym jest w tym przypadku RM, a nie prezydent RP. Ponadto w przypadku rozporządzenia RM wprowadzającego stan klęski żywiołowej nie wymagana jest jego kontrola przez Sejm.

O dopuszczalności oraz zakresie przedmiotowym rozporządzeń z mocą ustawy w czasie stanu wojennego, „Przegląd Sejmowy” 2002, nr 3, s. 48 i n.

²⁶ Zobacz na ten temat W.J. Wołpiuk, *Państwo wobec szczególnych zagrożeń*, Warszawa 2002, s. 92; M. Kaszuba, *Regulacje stanów nadzwyczajnych*, [w:] *Prawo obronne Rzeczypospolitej Polskiej*, red. P. Bała, Warszawa 2014, s. 109.

²⁷ Art. 9 usw.

²⁸ Art. 12 usw.

²⁹ Zobacz na ten temat J. Stelmasiak, op.cit., s. 164 i n.; M. Bartoszewicz, *Materiałne przesłanki wprowadzenia stanu klęski żywiołowej w Polsce*, „Przegląd Prawa i Administracji” 2002, t. XLIX, s. 251.

³⁰ Art. 232 Konstytucji RP.

Oprócz wskazanych wyżej różnic możemy zauważyć także zmiany w zakresie uprawnień i obowiązków działania organów władzy publicznej w czasie trwania klęski żywiołowej. Zapobieżenie jej skutkom lub ich usunięcie leży w kompetencji wójta (burmistrza, prezydenta miasta), starosty lub wojewody, których właściwość wyznacza obszar objęty stanem klęski żywiołowej. Wśród podmiotów uprawnionych ustawodawca wymienia także ministra właściwego do spraw administracji publicznej lub innego ministra, do zakresu działania którego należy zapobieganie skutkom danej klęski żywiołowej lub ich usuwanie, a w przypadku wątpliwości co do właściwości ministra lub w przypadku gdy właściwych jest kilku ministrów – ministra wyznaczonego przez prezesa RM, jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednego województwa³¹.

Również regulacja odnosząca się do ograniczenia wolności i praw jednostki została skonstruowana – w czasie klęski żywiołowej – w odmienny sposób. Świadczy o tym treść art. 233 ust. 3 Konstytucji RP. W przepisie tym ustrojodawca posłużył się klauzulą pozytywną, tzn. dokonał w nim wyliczenia wolności i praw, które mogą zostać ograniczone w drodze ustawy. Chodzi tu o wolności i prawa człowieka i obywatela określone w art. 22 (wolność działalności gospodarczej), art. 41 ust. 1, 3 i 5 (wolność osobista), art. 50 (nienaruszalność mieszkania), art. 52 ust. 1 (wolność poruszania się i pobytu na terytorium RP), art. 59 ust. 3 (prawo do strajku), art. 64 (prawo własności), art. 65 ust. 1 (wolność pracy) art. 66 ust. 1 (prawo do bezpiecznych i higienicznych warunków pracy) oraz art. 66 ust. 2 (prawo do wypoczynku). Wobec tak przyjętej konstrukcji art. 233 ust. 3 ustawy zasadniczej nie budzi wątpliwości, że inne wolności i prawa (niewymienione w tej jednostce redakcyjnej) nie mogą zostać ograniczone w czasie trwania stanu klęski żywiołowej³².

Oprócz wskazanych wyżej rozwiązań warto zwrócić uwagę także i na te, do których odnosi się art. 228 ust. 6 i 7 Konstytucji RP. Pierwszy z tych przepisów ustanawia zasadę ochrony podstaw systemu prawnego, która wyraża zakaz zmiany w czasie stanu nadzwyczajnego: Konsty-

³¹ Art. 8 ustawy o stanie klęski żywiołowej (t.j. Dz.U. 2014, poz. 333 ze zm.).

³² Zobacz szerzej T. Bąkowski, *Prawne formy ograniczania wolności oraz praw człowieka i obywatela w ustawie o stanie klęski żywiołowej*, „Państwo i Prawo” 2003, z. 8, s. 76 i n.

tucji RP, ordynacji wyborczych do Sejmu, Senatu i organów samorządu terytorialnego, ustawy o wyborze prezydenta RP³³ oraz ustawy o stanach nadzwyczajnych³⁴. Drugi przepis stanowi o zasadzie ochrony organów przedstawicielskich³⁵, co oznacza, że w czasie stanu nadzwyczajnego oraz w ciągu 90 dni po jego zakończeniu nie może być skrócona kadencja Sejmu, przeprowadzane referendum ogólnokrajowe, nie mogą być przeprowadzane wybory do Sejmu, Senatu, organów samorządu terytorialnego oraz wybory prezydenta RP, a kadencje tych organów ulegają odpowiedniemu przedłużeniu. Wybory do organów samorządu terytorialnego są możliwe tylko tam, gdzie nie został wprowadzony stan nadzwyczajny³⁶.

Wprowadzenie jednego ze stanów nadzwyczajnych wiąże się ze zmianą sposobu funkcjonowania organów władzy publicznej za wyjątkiem władzy sądowniczej, której zasady działania pozostają bez zmian. Oczywiście modyfikacje, do których odnieśliśmy się wyżej, nie pozostają bez wpływu dla dalszych rozważań poświęconych tematowi niniejszej publikacji, zwłaszcza że ustawodawca w każdej z trzech ustaw, tj. ustawie o stanie wojennym (dalej: uswoj), ustawie o stanie wyjątkowym oraz ustawie o stanie klęski żywiołowej (dalej: uskż), odniósł się do zagrożeń w cyberprzestrzeni jako jednej ze sfer aktywności państwa, w której mogą zaistnieć konstytucyjne przesłanki wprowadzenia stanu nadzwyczajnego. Rozwiązania przyjęte w wymienionych wyżej ustawach stanowią więc „podłoże” do działań, za przyczyną których możliwe jest planowanie, przygotowywanie, a następnie wdrożenie konkretnych przedsięwzięć w celu eliminowania zagrożeń w cyberprzestrzeni³⁷.

³³ Obecnie oznacza to zakaz zmiany ustawy z dnia 5 stycznia 2011 r. – Kodeks wyborczy (Dz.U. Nr 21, poz. 112 ze zm.).

³⁴ L. Garlicki, op.cit., s. 393.

³⁵ Ibidem.

³⁶ K. Orzeszyna, *Extraordinary Measures in the Constitution of the Republic of Poland*, [w:] K. Dunaj, M. Stepnowska (ed.), *Legal Security*, Warsaw 2013, s. 169–170. Podajemy za: M. Czuryk, *Podstawy normatywne wprowadzenia, obowiązywania oraz zniesienia stanu wojennego*, [w:] *Prawo obronne Rzeczypospolitej Polskiej w zarysie*, red. M. Czuryk, W. Kitler, Warszawa 2014, s. 270.

³⁷ Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, s. 64.

III.

Pojęcie cyberprzestrzeni powstało przede wszystkim w języku potocznym i to dla tego języka jest charakterystyczne. Jego włączanie do porządków prawnych uznać należy (jak do tej pory) za postępowanie wyjątkowe i nie zawsze uzasadnione³⁸. Jak wskazał Janusz Wasilewski, po raz pierwszy terminu tego użył pisarz William Gibson już w 1982 r., a to w noweli zatytułowanej *Burning Chrome*³⁹.

Omawiane tutaj pojęcie stanowi połączenie dwóch słów: „cyber” (nie występującego w polszczyźnie samodzielnie) oraz „przestrzeń”. Przedrostek „cyber” jest przede wszystkim pierwszym członem wyrazów złożonych. Wykazuje związek z informatyką. „Przestrzeń” zaś to „część obszaru objęta jakimiś granicami”⁴⁰. W kontekście istnienia państwa „przestrzeń” oznacza – najprościej ujmując – jego terytorium⁴¹. Według Marty Berdel-Dudzińskiej wskazany termin można rozpatrywać w czterech aspektach: technologicznym, psychologicznym, społecznym oraz ekonomicznym. Jednocześnie

³⁸ M. Mróz, *Informacja nt. pojęcia cyberprzestrzeni oraz bezpieczeństwa i zagrożenia cyberprzestrzeni w prawie międzynarodowym i w ustawodawstwie wybranych państw demokratycznych* (druk sejmowy Sejmu VI kadencji nr 4355), s. 4–5.

³⁹ Janusz Wasilewski przytoczył nadto definicję tego pojęcia zaproponowaną przez wskazanego autora powieści science-fiction, którą posłużył się on w 1984 r. w powieści *Neuromancer*. William Gibson opisał ją jako: „Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci uczące się pojęć matematycznych (...). Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność... Światne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych”. Za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Publicznego” 2013, nr 9, s. 226, podobnie P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka” 2009, T. 13, z. 2, s. 584–585.

⁴⁰ Słownik języka polskiego PWN online, hasło: Przestrzeń, <http://sjp.pwn.pl/szukaj/przestrze%C5%84.html> (3.01.2015).

⁴¹ M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego” 2012, nr 2. Dla porządku można dodać, że według słownika języka polskiego cyberprzestrzeń oznacza: „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową”. Słownik języka polskiego PWN online, hasło: Cyberprzestrzeń, <http://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915> (3.01.2015).

Wyjaśnienie to jednak jest dalece nieprecyzyjne, chociażby dlatego, że nie uwzględnia innych niż internetowych sieci, w szczególności sieci Intranet.

podniosła ona, że niekiedy aspekty te trudno od siebie konsekwentnie odseparować⁴². Według Ryszarda Tadeusiewicza cyberprzestrzeń to „ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia, przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do pozyskiwania wiedzy oraz do komunikacji z innymi ludźmi. Najważniejszym, chociaż nie jedynym, składnikiem cyberprzestrzeni jest obecnie Internet”⁴³. Definicja ta jest zatem dwuaspektowa. Cyberprzestrzeń ujęta jest bowiem nie tylko jako pewna infrastruktura techniczna, ale także obejmuje ona swym zakresem relacje ludzi z tą infrastrukturą, jak i interakcje między ludźmi z jej wykorzystaniem. Definicja ta wydaje się wystarczająca do opisanego terminu.

Pojęcie „cyberprzestrzeń” nie zostało także zignorowane przez krajowe organy odpowiedzialne za realizację polityki państwa⁴⁴. Przede wszystkim należy wskazać, że pojawiło się ono w dokumentach: Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia⁴⁵ oraz Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016⁴⁶. W tym pierwszym ustalono, że jest to: „przestrzeń komunikacyjna, tworzona przez system powiązań internetowych. Jako «cyberprzestrzeń państwa» przyjmuje się przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa. Cyberprzestrzeń państwa w przypadku Polski określana jest również mianem «cyberprzestrzeni RP». «Cyberprzestrzeń RP» obejmuje między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także

⁴² Szerzej: M. Berdel-Dudzińska, op.cit.

⁴³ R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka” 2010, nr 4, s. 32.

⁴⁴ Pojęcie to wyjaśniano także w wielu dokumentach pochodzących od różnorodnych organizacji międzynarodowych. Zob. np. M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo narodowe” 2012, nr 22, s. 129–130.

⁴⁵ Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011, Warszawa 2009, s. 4, <https://www.ms.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCR> (3.01.2015).

⁴⁶ Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Warszawa 2010, s. 6, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Poland_Cyber_Security_Strategy.pdf (3.01.2015).

systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne”, w drugim zaś nieco bardziej czytelnie, iż to: „cyfrowa przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniem pomiędzy nimi oraz relacjami z użytkownikami. Cyberprzestrzeń RP [dalej: CRP] – cyberprzestrzeń w obrębie terytorium państwa polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)”. W najnowszej Polityce ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, definiując wskazywany termin, odwołano się już wprost do postanowień ustawowych, o których poniżej. Warto jednak zaznaczyć, że pojęcie „cyberprzestrzeni Rzeczypospolitej Polskiej” określono tak samo jak w polityce na lata 2011–2016⁴⁷.

Każda z wymienionych uprzednio ustaw, regulujących funkcjonowanie organów państwa w stanach nadzwyczajnych, definiuje „cyberprzestrzeń” jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 ust. 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne⁴⁸, wraz z powiązanymi pomiędzy nimi oraz relacjami z użytkownikami. Z kolei system teleinformatyczny to – zgodnie z powołaną wyżej ustawą – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjnego urządzenia końcowego⁴⁹. Ustawodawca szeroko zatem ujął cyberprzestrzeń, nie wyłączając z jej zakresu czynnika ludzkiego.

⁴⁷ Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013, s. 5.
https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf (3.01.2015).

⁴⁸ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, Nr 64, poz. 565).

⁴⁹ Zgodnie z art. 2 pkt 43 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 ze zm.) telekomunikacyjne urządzenie końcowe to urządzenie telekomunikacyjne przeznaczone do połączenia bezpośrednio lub pośrednio do zakończenia sieci.

Janusz Wasilewski wskazał, że zdefiniowanie cyberprzestrzeni jest o tyle ważne, iż rozumienie tego terminu wywiera istotny wpływ na sposób określania zakresu przedmiotowego obszaru bezpieczeństwa⁵⁰. W zakres tego pojęcia wchodzi z pewnością co najmniej określonego rodzaju infrastruktura i procesy, które w niej zachodzą, albo też włącza się do tej definicji także ludzie i relacje, jakie występują między nimi za pośrednictwem tej infrastruktury, jak i między nimi a tą infrastrukturą (tak jak ujął to polski ustawodawca). Trzeba jednak mieć na uwadze, że infrastruktura ta istnieje fizycznie. Tak samo jak możliwe do zidentyfikowania są miejsce i czas, w jakich zachodzą wyżej opisane interakcje ludzi i urządzeń. Stąd też zasadność wyróżnienia nowej przestrzeni bezpieczeństwa publicznego⁵¹ może budzić uzasadnione wątpliwości. Do zagrożenia czy naruszenia dochodzi bowiem w rzeczywistości w wyniku działań podjętych w jednej ze znanych dotychczas przestrzeni. W takim ujęciu skutek też w istocie powstanie w infrastrukturze istniejącej fizycznie na ziemi, wodzie czy nawet w powietrzu.

Powyższe rozumowanie nie bierze jednak pod uwagę, iż owa infrastruktura, czy też infrastruktura i ludzie wchodzący z nią i za jej pośrednictwem między sobą w różnorodne relacje (także stosunki prawne), tworzy jednak pewnego rodzaju szczególną przestrzeń powstawania, wymiany czy niszczenia informacji. Stąd też można stwierdzić, że zasadne jest jej wyszczególnienie, także jurydyczne. Sama jej nazwa ma tutaj charakter wtórny, pozostaje bez znaczenia dla istoty zagadnienia, choć bardziej właściwe byłoby, gdyby pojęcie to, podniesione obecnie do wysokiej rangi, wykazywało ściślejszy związek z dotychczas stosowaną przez ustawodawcę terminologią.

⁵⁰ J. Wasilewski, *op.cit.*, s. 232.

⁵¹ Pod pojęciem tym można rozumieć: „taki stan, w którym ogółowi obywateli, nieznanemu indywidualnie, jak również innym podmiotom, w tym państwu i instytucjom publicznym, nie zagraża żadne niebezpieczeństwo (zagrożenie określonych dóbr) oraz nie zagraża zakłócenie normalnego toku życia społecznego, funkcjonowania instytucji i urządzeń publicznych”. Definicję autorstwa Jacka Jagielskiego podajemy za: L. Mażewski, *op.cit.*, s. 22. Warto wskazać, że zdaniem Lecha Mażewskiego pojęcie bezpieczeństwa publicznego jest szersze niż bezpieczeństwa państwa, uwzględnia bowiem także bezpieczeństwo obywateli. Szerzej: L. Mażewski, *op.cit.*, s. 20–22.

IV.

Zagrożenia związane z aktywnością w cyberprzestrzeni⁵² można sklasyfikować w trzech kategoriach: cyberwojna, cyberprzestępstwa oraz cyberterroryzm⁵³. Najwięcej problemów pojawia się ze zdefiniowaniem „cyberwojny”. W literaturze nie wyklucza się możliwości wywołania i prowadzenia konfliktu zbrojnego w cyberprzestrzeni⁵⁴. W każdym przypadku takiego konfliktu dopuszczalne – a nawet konieczne – będzie wprowadzenia któregoś ze stanów nadzwyczajnych, najpewniej wojennego (choć nie można także wykluczyć wyjątkowego, przynajmniej w początkowym etapie działań „cyberwojennych”⁵⁵). W literaturze wskazuje się, że można także spotkać się z takim rodzajem konfliktu zbrojnego, który będzie zainicjowany i niejako sterowany wyłącznie działaniami w cyberprzestrzeni (podejmowanymi co najmniej przez jedną stronę)⁵⁶.

⁵² Dariusz Jagiełło stwierdził, że węższą kategorią od powyższych jest cyberatak. Występuje on wówczas, gdy „same informacje, programy, systemy komputerowe lub bazy danych stają się obiektem ataku. Jest on także skrupulatnie przygotowany i potrafi w krótkim czasie wywołać mnóstwo szkód materialnych oraz strat finansowych, prowadzących do destabilizacji zaatakowanego państwa”. Powyższe rozumowanie nakazuje przyjąć, że cyberterroryzm może być kwalifikowanym cyberatakiem. Do takiego wniosku prowadzi dalszy wywód wskazanego autora, który podniósł, że cyberterroryzm powinien odnosić się do ataków lub ich groźby. Zob. D. Jagiełło, *Cyberterroryzm*, „Edukacja Prawnicza” 2013, nr 5, s. 12.

⁵³ Ibidem. wymienia także cyberinwigilację, przez którą rozumie „wykorzystanie cyberprzestrzeni w celach kontroli społecznej (np. identyfikacja lokalizacji, częstości korzystania z technologii informatycznych, treści przekazów, itp.). Na gruncie polskiego kodeksu karnego takie czyny uznać jednak należałoby za cyberprzestępstwa, stąd nie wydaje się celowe ich wyróżnianie.

⁵⁴ Za Michaelem Schmittem można także przytoczyć inną kategoryzację konfliktów, które mogą zostać wywołane w cyberprzestrzeni i będą miały charakter zbrojny. Podział ten stworzony został w oparciu o kategorie „tradycyjnych” konfliktów. Wyróżnić tutaj można: międzynarodowy konflikt zbrojny pomiędzy państwami; międzynarodowy konflikt zbrojny pomiędzy narodowymi ruchami wyzwolenческими; konflikt zbrojny niemający charakteru międzynarodowego pomiędzy państwem a organizacją zbrojną albo pomiędzy takimi organizacjami; konflikt zbrojny niemający charakteru międzynarodowego. Zob. M. Schmitt, *Classification of Cyber Conflict*, „Jurnal of Conflict & Security Law” 2012, nr 2, s. 247 i n.

⁵⁵ Odrębnym zagadnieniem będzie dopuszczalność (obowiązek) ustanowienia stanu wojny (art. 116 Konstytucji RP).

⁵⁶ Szerzej: M. Schmitt, op.cit., s. 255 i n.

Napaść w opisywanym wypadku może nie być tak oczywista jak w przypadku wojny w świecie rzeczywistym. Co więcej, jej przeprowadzenie jest prawdopodobne przy wykorzystaniu nawet mało zaawansowanych, łatwo dostępnych komputerów. Prowadzi to do twierdzenia, że w cyberprzestrzeni państwa tracą monopol na wywoływanie i prowadzenie wojny. Może być ona równie dobrze prowadzona w tym zakresie przez jednostki, a w skrajnych przypadkach nawet przez jedną osobę. Z drugiej zaś strony zachowania, które dotychczas cechowały w zasadzie tylko jednostki, będzie równie dobrze można przypisać państwom (popelnianie cyberprzestępstw czy aktów cyberterroryzmu), o ile tylko ich dokonanie będzie leżało w interesie konkretnego państwa⁵⁷. Co ważne, mogą one zostać dokonane zarówno na szkodę jego własnych obywateli, jak i na szkodę obywateli innych państw, niebędących nawet pod jurysdykcją państwa atakującego.

Cyberprzestępstwa można określić mianem „zwyczajnych czynów kryminalnych”, które mogą także przybierać znamiona działań terrorystycznych. Ogólnie grupę tę można by nazwać przestępstwami komputerowymi⁵⁸. Wśród nich znamienne miejsce przypisać należy przestępstwu stypizowanemu w art. 269 k.k.⁵⁹, nazywanemu sabotażem komputerowym. Może ono polegać na przesyłaniu wirusów, robaków komputerowych, bomb logicznych, atakach DoS (*Denial of Service*)⁶⁰.

Nie wdając się nadto w zawiłości terminologiczne, na potrzeby niniejszego opracowania przyjmujemy za Dariuszem Jagiełłą, że „definicja cyberterroryzmu winna przewidywać występowanie dwóch płaszczyzn: odnosić się do ataków lub ich groźby na systemy i sieci teleinformatyczne, a przy tym nie pomijać ataków zmierzających do wykorzystania działalności organizacji (w tym także terrorystycznych)”⁶¹. Stąd też przez cyberterroryzm należy rozumieć:

⁵⁷ Ibidem, s. 150.

⁵⁸ J. Znamierowski, *Prawnokarna ochrona funkcjonowania państwa przed sabotażem komputerowym*, „Edukacja Prawnicza” 2014, nr 4, s. 23. Autor wskazuje także na inną spotykaną w doktrynie prawa karnego nazwę, a mianowicie „przestępstwa informatyczne”.

⁵⁹ Które może być uznane za przestępstwo o charakterze terrorystycznym.

⁶⁰ A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010, s. 226. Por. D. Jagiełło, op. cit., s. 10.

⁶¹ D. Jagiełło, op. cit., s. 12.

- „politycznie lub militarnie motywowany atak albo groźbę ataku na systemy i sieci teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa oraz zastraszenie i wymuszenie na rządzie lub społeczności daleko idących polityczno-militarnych działań, a także
- świadome wykorzystanie sieci teleinformatycznych oraz globalnej sieci Internet m.in. przez organizacje terrorystyczne, ruchy narodo-wo-wyzwoleńcze oraz ruchy powstańcze do propagandy, rekrutacji on-line, komunikowania się, mobilizacji, zbierania informacji o potencjalnych celach ataku, planowania i koordynacji akcji oraz szeroko pojętej dezinformacji i walki psychologicznej”⁶².

W obrębie wyżej wskazanego zjawiska, a zatem najistotniejszej dla niniejszego opracowania kategorii cyberzagrożenia, można dokonać dalszej klasyfikacji, a to ze względu na źródło w stosunku do atakowanego państwa. W tym obrębie wyszczególnić można trzy kategorie cyberterroryzmu: 1) o charakterze zewnętrznym; 2) o charakterze wewnętrznym; oraz 3) o charakterze mieszanym⁶³.

Powyższy podział ma dla niniejszego opracowania o tyle istotne znaczenie, że uwidacznia jedną istotną cechę cyberataków mających wpływ na możliwość wprowadzenia każdego ze stanów nadzwyczajnych. Każdy z cyberataków może pochodzić spoza terytorium państwa i może wywołać każdy ze stanów nadzwyczajnych. Tymczasem ustawa zasadnicza nie daje żadnych wątpliwości, że stan wojenny może zostać spowodowany tyl-

⁶² Ibidem. Szerzej na temat definicji cyberterroryzmu zob. D. Jagiełło, op.cit., s. 10 i n. W tym miejscu przytoczyć jeszcze można, za Maciejem Siwickim, że omawiane pojęcie „ogólnie służy do określenia grupy czynów polegających na posługiwaniu się elektronicznymi systemami przetwarzania informacji w działalności terrorystycznej”. Na gruncie prawodawstwa polskiego należy mieć także na uwadze ograniczenie formalne, jakim jest wymóg karalności karą co najmniej 5 lat pozbawienia wolności (art. 115 § 20 k.k.). Dlatego też jedynie przestępstwa z art. 165 § 1 pkt 4 i art. 269 § 1 k.k. będą mogły być zakwalifikowane do przestępstw o charakterze terrorystycznym. Pozostałe przestępstwa, choćby były skierowane przeciwko informacjom, danym i systemom je przetwarzającym, nawet jeśli będą spełniały warunki przedstawione przez D. Jagiełłę, nie będą mogły być uznane i ścigane jako terrorystyczne. Por. M. Siwicki, *Cyberprzestępczość*, Warszawa 2014 i cytowana tam w przypisie 13 literatura.

⁶³ S.W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, „Minnesota journal of law, science & technology” 2003, nr 14, s. 148.

ko przez zewnętrzne zagrożenie państwa, które – o czym była już mowa – może być spowodowane działaniami w cyberprzestrzeni. Może zatem dojść do jeszcze jednej konfiguracji zdarzeń, a mianowicie działanie w cyberprzestrzeni będzie dokonywane wprawdzie na terytorium Rzeczypospolitej Polskiej, lecz wywoła ono skutek poza tym terytorium i w efekcie spowoduje zagrożenie, o którym mowa w art. 229 Konstytucji RP. Zaznaczyć jednak trzeba, że legalna definicja „zewnętrznego zagrożenia państwa” w takim wypadku rodzi pewne trudności⁶⁴. Jej interpretacja może doprowadzić do wniosku, że nawet w wyżej opisanej sytuacji do czynienia będziemy mieli z zagrożeniem zewnętrznym, choć pochodzącym z wewnątrz państwa. Kluczowe w tym wypadku staje się zdefiniowanie „podmiotów zewnętrznych w stosunku do Rzeczypospolitej”. Jak można wnioskować z treści uzasadnienia do 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 ustaw⁶⁵, chodzić tutaj może o wszelkie podmioty, których nie łączy z Rzeczypospolitą więź prawna obywatelstwa – w przypadku osób fizycznych, czy posiadania siedziby na terytorium RP – w przypadku osób prawnych i innych podmiotów prawa⁶⁶. Rzecz jasna, rodzi to problem z obywatelami nieprzebywającymi na terytorium państwa. Opierając się o nader skromne wyjaśnie-

⁶⁴ Andrzej Smyt w opinii prawnej do pierwotnie projektowanego art. 2 ust. 1 przedstawionego przez prezydenta Rzeczypospolitej Polskiej 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 (druk sejmowy Sejmu VI kadencji nr 4355) (dalej: opinia) z dnia 11 lipca 2011 r. krytycznie odniósł się do definiowania przez ustawodawcę tego pojęcia. Wyszczególnienie przypadków, które zostały uznane przez prawodawcę za zewnętrzne zagrożenie państwa, może spowodować powstanie negatywnych skutków, a to z powodu możliwości zaistnienia różnych zdarzeń, których taka „zamknięta” definicja nie przewiduje. Zob. A. Smyt, op.cit., s. 3.

⁶⁵ Ustawa 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 (Dz.U. Nr 222, poz. 1323).

⁶⁶ Por. Uzasadnienie do przedstawionego przez prezydenta Rzeczypospolitej Polskiej projektu ustawy..., s. 2. Z drugiej strony taka interpretacja może być zbyt restrykcyjna. Każda osoba fizyczna, jak i inny podmiot prawa prowadzący na terenie RP określonego rodzaju działalność podlega przecież, co do zasady, prawu polskiemu. Stąd kłopotliwe byłoby przypisywanie mu cechy „zewnętrzności”.

nia projektu ustawy, można by wnioskować, że takim podmiotom nie sposób przypisywać cechy „zewnątrżności”.

Powyższe rodzi problemy także na gruncie zorganizowania odpowiednich mechanizmów mających zapobiegać atakom. Niemal tradycyjnie na te, które noszą znamiona wojny, odpowiada armia, zaś na pozostałe – służby cywilne. Takie rozróżnienie w przypadku cyberzagrożeń może nie spełniać swej roli, a to właśnie z racji ich charakteru i trudności z identyfikacją. W przypadku RP możemy dostrzec, że gdy cyberprzestrzeń wykorzystywana jest do walki zbrojnej, to wówczas Siły Zbrojne RP muszą podejmować działania zarówno o charakterze ochronnym, jak i obronnym, aby zapewnić prawidłowe funkcjonowanie państwa i społeczeństwa. Działania w sferze obronnej prowadzą także służby specjalne, do których można zaliczyć np.:

- Służbę Kontrwywiadu Wojskowego⁶⁷, do której zadań w obszarze interesującego nas zagadnienia należy m.in. uzyskanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych RP, lub innych jednostek organizacyjnych MON, oraz podejmowanie działań w celu eliminowania ustalonych zagrożeń; prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy⁶⁸;
- Służbę Wywiadu Wojskowego⁶⁹, do której zadań należy m.in. uzyskanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa potencjału obronnego RP, bezpieczeństwa

⁶⁷ Służba Kontrwywiadu Wojskowego jest służbą specjalną właściwą w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez ministra obrony narodowej – art. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz.U. z 2014 r, poz. 253), dalej: uskwsww.

⁶⁸ Art. 5 uskwsww.

⁶⁹ Służba Wywiadu Wojskowego jest służbą specjalną właściwą w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez ministra obrony narodowej – art. 2 uskwsww.

i zdolności bojowej Sił Zbrojnych RP, warunków realizacji przez Siły Zbrojne RP zadań poza granicami państwa; prowadzenie wywiadu elektronicznego na rzecz Sił Zbrojnych RP oraz przedsięwzięć z zakresu kryptoanalizy i kryptografii⁷⁰;

- Agencję Bezpieczeństwa Wewnętrznego⁷¹, do której zadań w omawianym zakresie należy m.in. rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenności i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa; rozpoznawanie, zapobieganie i wykrywanie przestępstw: szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa; realizowanie w granicach swojej właściwości zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych; uzyskanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego⁷²;
- Agencję Wywiadu⁷³, do której zadań w interesującym nas obszarze należy m.in. uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP oraz jej potencjału ekonomicznego i obronnego; rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronności, niepodległość i nienaruszalność terytorium RP; zapewnienie ochrony kryptograficznej łączności z polskimi placówkami

⁷⁰ Art. 6 uskwsww.

⁷¹ Agencja Bezpieczeństwa Wewnętrznego jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego i jego porządku konstytucyjnego – art. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. 2010, Nr 29, poz. 154 ze zm.), dalej: uabwaw.

⁷² Art. 5 uabwaw.

⁷³ Agencja Wywiadu jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego państwa – art. 2 uabwaw.

dypłomatycznymi i konsularnymi oraz poczty kurierskiej; prowadzenie wywiadu elektronicznego⁷⁴;

które, co wynika z przypisanych im zadań, koncentrują się wokół szeroko rozumianego bezpieczeństwa informacyjnego.

Ustawodawca, ustanawiając w ogólny sposób możliwość wprowadzenia stanu nadzwyczajnego z uwagi na określonego rodzaju działania w cyberprzestrzeni, pozostawił jednak w niezmienionym kształcie katalog środków, które mogą zostać wykorzystane w trakcie trwania tychże szczególnych sytuacji. Założyć jednak wstępnie wypada, że zdaniem ustawodawcy dotychczasowy katalog środków był wystarczający, aby chronić konstytucyjny porządek w czasie trwania stanu nadzwyczajnego, także w przypadku gdy stosowne działania były podejmowane co najmniej w cyberprzestrzeni. Skoro tak, to ponownie powraca pytanie o zasadność poczynionego wyróżnienia, ale także należałoby dokonać co najmniej przeglądu obecnie oferowanych przez ustawodawcę instrumentów w zakresie ograniczeń wolności i praw jednostek, służących władzy publicznej do odpowiedniego zarządzania państwem.

Gdy idzie o stan wojenny, to wskazać należy, że w przypadku tego stanu spowodowanego działaniami w cyberprzestrzeni najistotniejsze znaczenie będą miały:

- możliwość przeszukania osób, których działalność zagraża bezpieczeństwu lub obronności państwa, jak i ich mieszkania oraz innych należących do nich pomieszczeń, pojazdów, statków powietrznych oraz jednostek pływających, a także zajęcia przedmiotów wykorzystywanych do prowadzenia wskazanej działalności (art. 20 ust. 1 i ust. 2 uswoj);
- możliwość wprowadzenia kontroli treści korespondencji telekomunikacyjnej i rozmów telefonicznych lub sygnałów przesyłanych w sieciach telekomunikacyjnych (art. 20 ust. 1 pkt 3 uswoj)⁷⁵;
- możliwość zawieszenia prawa do organizowania zgromadzeń, imprez masowych i prowadzonych w ramach działalności kulturalnej

⁷⁴ Art. 6 uabwaw.

⁷⁵ W zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni. Mają one wyeliminować trwające ataki lub zapobiegać potencjalnym atakom np. na serwery rządowe, wojskowe, które przyczyniają się m.in. do kradzieży różnego rodzaju informacji np. o charakterze strategicznym czy ekonomicznym.

impresz artystycznych i rozrywkowych niebędących imprezami masowymi (art. 22 ust. 1 pkt 1 i pkt 2 uswoj)⁷⁶;

- możliwość ograniczenia wolności działalności gospodarczej (art. 24 ust. 1 pkt 2 uswoj)⁷⁷;
- możliwość ograniczenia funkcjonowania systemów łączności oraz działalności telekomunikacyjnej poprzez nakazanie wyłączenia urządzeń łączności lub zawieszenia świadczenia usług na czas określony, a także poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub ustalenie innego sposobu ich zabezpieczenia przed wykorzystaniem w sposób zagrażający bezpieczeństwu lub obronności państwa (art. 24 ust. 1 pkt 5 uswoj)⁷⁸;
- możliwość ograniczenia dostępu do informacji publicznej (art. 24 ust. 1 pkt 7 uswoj).

Podobne narzędzia prawodawca przewidział w czasie trwania stanu wyjątkowego. Można tutaj zatem wyróżnić dopuszczalność:

- ograniczenia prawa do organizowania zgromadzeń, imprez masowych oraz prowadzonych w ramach działalności kulturalnej imprez

⁷⁶ O ile takie organizowanie odbywa się za pośrednictwem środków komunikacji elektronicznej.

⁷⁷ W zakresie, w jakim działalność taka polega na świadczeniu usług dostępu do publicznej sieci telekomunikacyjnej.

⁷⁸ W przypadkach wskazanych w art. 20 ust. 1 pkt 3 uswoj i art. 24 ust. 1 pkt 5 uswoj organy kontroli (np. Szef Agencji Bezpieczeństwa Wewnętrznego, Komendant Główny Policji) są uprawnione do zatrzymania w całości lub części m.in. korespondencji telekomunikacyjnej, a także do przerywania rozmów telefonicznych i transmisji sygnałów przesyłanych w sieciach telekomunikacyjnych. Zatrzymaną korespondencję telekomunikacyjną, której treść pochodzi z przestępstwa, była przeznaczona do popełnienia przestępstwa albo została objęta zakazem posiadania, organ kontroli przekazuje niezwłocznie, najpóźniej bezpośrednio po zniesieniu stanu wojennego lub stanu wyjątkowego, organom właściwym do prowadzenia postępowania karnego lub orzeczenia przepadku rzeczy. W literaturze podnosi się, że powyższe rozwiązania mają wyeliminować trwające ataki lub zapobiegać potencjalnym atakom np. na serwery rządowe, wojskowe, które przyczyniają się m.in. do kradzieży różnego rodzaju informacji np. o charakterze strategicznym czy ekonomicznym. Zob. J.W. Wójcik, *Zagrożenia w cyberprzestrzeni. Wybrane zagadnienia kryminologiczne i kryminalistyczne*, [w:] *Problemy współczesnej kryminalistyki*, t. XII, red. E. Gruza, T. Tomaszewski, M. Goc, Warszawa 2008, s. 367.

artystycznych i rozrywkowych, niebędących imprezami masowymi, a także strajków (art. 16 ust. 1 pkt. 1–5 usw);

- ograniczenia prawa do zrzeszania się (art. 16 ust. 1 pkt 6 usw);
- wprowadzenia kontroli treści korespondencji telekomunikacyjnej i rozmów telefonicznych lub sygnałów przesyłanych w sieciach telekomunikacyjnych (art. 20 ust. 1 pkt 3 usw);
- ograniczenia wolności działalności gospodarczej (art. 21 pkt 2 usw);
- ograniczenia funkcjonowania systemów łączności oraz działalności telekomunikacyjnej poprzez nakazanie wyłączenia urządzeń łączności lub zawieszenia świadczenia usług na czas określony, a także poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub ustalenie innego sposobu ich zabezpieczenia przed wykorzystaniem w sposób zagrażający konstytucyjnemu ustrojowi państwa, bezpieczeństwu obywateli albo porządkowi publicznemu (art. 21 pkt 6 usw);
- ograniczenia dostępu do informacji publicznej (art. 21 pkt 8 usw).

Gdy zaś idzie o stan klęski żywiołowej, to należy w szczególności wskazać na możliwość:

- zawieszenia działalności określonych przedsiębiorców (art. 21 ust. 1 pkt 1 uskż);
- nakazania lub zakazania prowadzenia działalności gospodarczej określonego rodzaju (art. 21 ust. 1 pkt 2 uskż);
- nakazania lub zakazania określonego sposobu przemieszczania się (art. 21 ust. 1 pkt 15 uskż);
- ograniczenia pracy urządzeń radiowych nadawczych lub nadawczo-odbiorczych oraz wykonywania usług telekomunikacyjnych (art. 25 ust. 2 uskż).

Ponadto można dodać, że redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani do niezwłocznego, nieodpłatnego podania do publicznej wiadomości odpowiednich rozporządzeń o wprowadzeniu stanu nadzwyczajnego i innych aktów prawnych dotyczących tego stanu, przekazanych im przez wojewodę właściwego ze względu na siedzibę redakcji lub nadawcy (art. 5 uswoj, art. 6 usw, art. 5 ust. 4 uskż).

Jak zostało to zaznaczone, bezpieczeństwo RP w cyberprzestrzeni stanowi obecnie jedno z fundamentalnych zadań w dziedzinie bezpieczeństwa kraju⁷⁹. Jego urzeczywistnienie powinno obejmować zarówno działania defensywne, tzn. obejmujące „ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni, jak i ofensywne”⁸⁰. Ponadto do osiągnięcia zamierzonego celu bardzo ważna jest „współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej; prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni; wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie; rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej w cyberprzestrzeni; współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych”⁸¹. Można zatem założyć, że ustawodawca stanął na stanowisku, że dotychczas stosowane instrumenty będą wystarczające do przywrócenia prawidłowego funkcjonowania państwa oraz porządku i bezpieczeństwa publicznego. Takie postępowanie wydaje się prawidłowe tylko jeżeli skutki działania w cyberprzestrzeni wystąpią w innych niż wskazana przestrzeń państwa. W przypadku gdy efekt takiej działalności wywrze skutek w przestrzeni wirtualnej państwa, to nawet drobiazgowa kontrola sygnałów przesyłanych w sieciach telekomunikacyjnych czy ograniczenia funkcjonowania systemów łączności oraz działalności telekomunikacyjnej najprawdopodobniej okażą się niewystarczające, a to gdy źródło niebezpieczeństwa będzie pochodziło spoza terytorium Rzeczypospolitej. Wówczas niezbędne byłoby nie tylko odizolowanie systemów teleinformatycznych państwa od takiego zagrożenia, ale także ścisła koordynacja między państwowa w celu jego zneutralizowania. Nadto wydaje się, że dotychczasowa regulacja nie uwzględnia w wystarczającym stopniu konieczności

⁷⁹ Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014, <http://www.bbn.gov.pl/ftp/SBN%20RP.pdf> (5.04.2015).

⁸⁰ Ibidem.

⁸¹ Ibidem.

zabezpieczenia teleinformatycznego prowadzonych przez państwo systemów informatycznych.

Biorąc pod uwagę rozwiązania przyjęte na gruncie uprzednio wskazanych trzech ustaw regulujących problematykę stanów nadzwyczajnych, należy także zastanowić się, czy dokonane na skutek nowelizacji wyróżnienie nowej przestrzeni zagrożeń było niezbędne. Zdaniem autorów nawet w przypadku braku takiego zabiegu legislacyjnego można byłoby uznać, że cyberprzestrzeń i tak jest chroniona tak samo jak każdy inny aspekt „terytorium” państwa, co znajduje swoje uzasadnienie także w braku szczególnego rodzaju instrumentów czy to w zakresie funkcjonowania samej władzy publicznej w trakcie trwania stanu nadzwyczajnego, czy to w sferze dopuszczalnych ograniczeń wolności i praw jednostek. To, że ustawodawca zdecydował się na możliwość wprowadzenia stanu nadzwyczajnego w sytuacji gdy jedna z konstytucyjnych przesłanek, o których mowa w art. 229, art. 230 i art. 232, ziściłaby się w wyniku działań w wirtualnej przestrzeni państwa, świadczy o wadze, jaką przywiązuje się do tego zagadnienia. Z pewnością jest to jednak doniosłe przedsięwzięcie, które w szczególny sposób podkreśla wagę bezpieczeństwa publicznego w cyberprzestrzeni jako jednego z elementów bezpieczeństwa narodowego.

V.

Zagrożenia w cyberprzestrzeni niosą za sobą zarówno znane, jak i coraz to nowe problemy. Dzięki szerokiemu zastosowaniu technik teleinformatycznych w funkcjonowaniu aparatu państwa niebezpieczeństwa te znacząco zwiększają jednak skalę. Szpiegostwo gospodarcze z wykorzystaniem wskazanych technik aktywnie prowadzą Chiny (najprawdopodobniej władze państwowe) w stosunku do Stanów Zjednoczonych Ameryki. Z ustaleń poczynionych w raporcie Pentagonu z maja 2013 r. wynika, że celem ataków pochodzących z terytorium Chin były zarówno informacje przemysłowe, jak i te dotyczące bieżącego zarządzania państwem. Ataki te w połowie 2014 r. tak przybrały na sile, że zagroziły kryzysem w stosunkach dyplomatycznych pomiędzy tymi dwoma krajami⁸², którego jednak szeroko nie ko-

⁸² Szerzej zob. Ch. P. Skinner, *An International Law Response to Economic Cyber Espionage*, „Connecticut Law Review” 2014, nr 4, s. 1168 i n.

mentowano. Wydaje się, że dobrze uwidacznia to skalę problemu oraz to, jak trudno jest przyznać się danemu państwu, że ma problem z ochroną swojej przestrzeni stworzonej przez urządzenia teleinformatyczne⁸³.

Specyfika wirtualnej rzeczywistości powoduje, że nie łatwo jest umieścić ją pośród znanych dotychczas „tradycyjnych” przestrzeni państwa. Rosnące uzależnienie państwa od nowoczesnych technologii powoduje, że problem ten musi leżeć w sferze zainteresowania prawodawcy. Jednakże ze względu na wskazaną tutaj charakterystykę cyberprzestrzeni wątpliwe jest, by państwo samodzielnie było w stanie ochronić „swoją” cyberprzestrzeń. Nie da się wytyczyć jej granic, tak jak w przypadku innych przestrzeni państwa. Dlatego też ochrona ta powinna zostać ustanowiona przede wszystkim na szczeblu międzynarodowym, zaś jej wzmocnienia czy konkretyzacji należy dokonać na poziomie krajowym.

Ponownie wypada zwrócić uwagę na specyfikę zagrożeń w cyberprzestrzeni. Wyróżnienie tej sfery bezpieczeństwa państwa w ustawach regulujących stany nadzwyczajne może być uważane za co najwyżej pierwszy etap dostosowywania prawodawstwa w tym zakresie do wyzwań, jakie stawia współczesny rozwój techniki. O ile bowiem rozwijane są regulacje w zakresie wdrażania technik informatycznych i teleinformatycznych w działaniu władzy publicznej, o tyle brakuje szczególnych regulacji na wypadek powstania zagrożeń w cyberprzestrzeni, gdy zwykle środki konstytucyjne okażą się niewystarczające.

Literatura

- Bartoszewicz M., *Materialne przesłanki wprowadzenia stanu klęski żywiołowej w Polsce*, „Przegląd Prawa i Administracji” 2002, t. XLIX.
- Bąkowski T., *Prawne formy ograniczania wolności oraz praw człowieka i obywatela w ustawie o stanie klęski żywiołowej*, „Państwo i Prawo” 2013, z. 8.
- Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego” 2012, nr 2.
- Brenner S.W., *Cyber-threats and the Limits of Bureaucratic Control*, „Minnesota journal of law, science & technology” 2003, nr 14.

⁸³ Powszechnie znane są natomiast przykłady ataków na Estonię czy Wielką Brytanię, zob. np.: D. Jagiełło, op.cit.; J. Znamierowski, op.cit.

- Brzeziński M., *Stany nadzwyczajne w polskich konstytucjach*, Warszawa 2007.
- Czuryk M., *Podstawy normatywne wprowadzenia, obowiązywania oraz zniesienia stanu wojennego*, [w:] *Prawo obronne Rzeczypospolitej Polskiej w zarysie*, red. M. Czuryk, W. Kitler, Warszawa 2014.
- Działocha K., *Komentarz do art. 22*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. V, red. L. Garlicki, Warszawa 2005.
- Dzierżyński B., *Rozporządzenia z mocą ustawy jako akty nadzwyczajnego ustawodawstwa delegowanego na tle konstytucji polskich – wybrane problemy*, „Przegląd Prawa i Administracji” 2003, t. LIV.
- Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2009.
- Gebethner S., *Stany szczególnego zagrożenia jako instytucja prawa konstytucyjnego*, „Państwo i Prawo” 1982, z. 8.
- Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo narodowe” 2012, nr 22.
- Jagiello D., *Cyberterroryzm*, „Edukacja Prawnicza” 2013, nr 5.
- Jaskiernia J., *Akty normatywne w stanach nadzwyczajnych*, [w:] *Konstytucyjny system źródeł prawa w praktyce*, red. A. Szmyt, Warszawa 2005.
- Kaszuba M., *Regulacje stanów nadzwyczajnych*, [w:] *Prawo obronne Rzeczypospolitej Polskiej*, red. P. Bała, Warszawa 2014.
- Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011.
- Mażewski L., *Bezpieczeństwo publiczne. Stany nadzwyczajne w Rzeczypospolitej Polskiej oraz Polskiej Rzeczypospolitej Ludowej 1918–2009*, Toruń 2010.
- Mról M., *Informacja nt. pojęcia cyberprzestrzeni oraz bezpieczeństwa i zagrożenia cyberprzestrzeni w prawie międzynarodowym i w ustawodawstwie wybranych państw demokratycznych* (druk sejmowy Sejmu VI kadencji nr 4355).
- Orzeszyna K., *Extraordinary Measures in the Constitution of the Republic of Poland*, [w:] K. Dunaj, M. Stepnowska (ed.), *Legal Security*, Warsaw 2013.
- Paszkudzki A., *Konstytucja Rzeczypospolitej Polskiej z dnia 17 marca 1921 r. z uwzględnieniem zmian ustalonych ustawą z dnia 2 sierpnia 1926 r. Komentarz*, Lwów–Warszawa 1927.
- Prokop K., *O dopuszczalności oraz zakresie przedmiotowym rozporządzeń z mocą ustawy w czasie stanu wojennego*, „Przegląd Sejmowy” 2002, nr 3.
- Prokop K., *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Białystok 2005.
- Schmitt M., *Classification of Cyber Conflict*, „Journal of Conflict & Security Law” 2012, nr 2.
- Sienkiewicz P., *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka” 2009, t. 13, z. 2.

- Siwicki M., *Cyberprzestępczość*, Warszawa 2014.
- Skinner Ch.P., *An International Law Response to Economic Cyber Espionage*, „Connecticut Law Review” 2014, nr 4.
- Stelmasiak J., *Stany nadzwyczajne*, [w:] *Publicznoprawne podstawy bezpieczeństwa wewnętrznego*, red. M. Zdyb, Warszawa 2014.
- Stembrowicz J., *Z problematyki stanu nadzwyczajnego w prawie konstytucyjnym*, „Więź” 1988, nr 11–12.
- Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010.
- Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, „Nauka” 2010, nr 4.
- Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Publicznego” 2013, nr 9.
- Wołpiuk W.J., *Państwo wobec szczególnych zagrożeń*, Warszawa 2002.
- Wójcik J.W., *Zagrożenia w cyberprzestrzeni. Wybrane zagadnienia kryminologiczne i kryminalistyczne*, [w:] *Problemy współczesnej kryminalistyki*, t. XII, red. E. Gruza, T. Tomaszewski, M. Goc, Warszawa 2008.
- Znamierowski J., *Prawnokarna ochrona funkcjonowania państwa przed sabotażem komputerowym*, „Edukacja Prawnicza” 2014, nr 4.