Zeszyty Naukowe Politechniki Częstochowskiej
Zarządzanie Nr 33 (2019) s. 144-153
dostępne na: http://www.wz.pcz.pl/znwz

BEZPIECZEŃSTWO INFORMACYJNE W CYBERPRZESTRZENI A STANY NADZWYCZAJNE RZECZYPOSPOLITEJ POLSKIEJ

Izabela Oleksiewicz[1]

Politechnika Rzeszowska
Wydział Zarządzania

Streszczenie: Celem niniejszego artykułu jest analiza bezpieczeństwa informacyjnego państwa w XXI wieku oraz wyzwań prawnych, jakie przed nami stawia. Uznano również za niezbędne pokazanie postępującej złożoności zakresu przedmiotowego bezpieczeństwa informacyjnego, czyli zjawisk i procesów, ze szczególnym uwzględnieniem tych, które mają miejsce w stanach nadzwyczajnych, na przykładzie Polski. Zdaniem autorki warto więc zwrócić uwagę na tak istotne i ważne kwestie, które ulegają ciągłej przemianie na skutek wielu czynników, takich jak innowacje czy globalizacja. Jest to problematyka zajmująca obecnie istotne miejsce wśród zainteresowań badaczy zjawiska bezpieczeństwa. Stwierdzono także, że w warunkach wzrostu współzależności oraz „wyłaniania się" nowych jakościowo cech środowiska bezpieczeństwa informacyjnego niezbędne jest ukazanie ewolucji i postępującej złożoności form, struktur, mechanizmów dotychczasowych regulacji prawnych dotyczących cyberprzestrzeni, które są z zasady niewystarczające i nieadekwatne.

Słowa kluczowe: bezpieczeństwo informacyjne, cyberprzestrzeń RP, stany nadzwyczajne, polityka antycyberterrorystyczna, zarządzanie

DOI: 10.17512/znpcz.2019.1.12

Wprowadzenie – informacja w cyberprzestrzeni

Początkowo przestrzeń informacyjna obejmowała swoim zasięgiem tylko lokalne społeczności, lecz z upływem czasu, rozwojem struktur społecznych, nabyciem umiejętności wykorzystania narzędzi komunikacyjnych obszar jej powiązania zwiększał się. Rozwój informatyki, telekomunikacji i teleinformatyki spowodował, że obecnie obejmuje ona swoim zasięgiem całą kulę ziemską, skracając czas obiegu informacji do minimum. To cyberprzestrzeń przeobraziła przestrzeń informacyjną, nadając jej globalny charakter.

Obecnie sieć powiązań informacyjnych jest niejednorodna i wielopoziomowa. Ukształtowała się jako zespół instytucji, jednostek organizacyjnych, zasobów i systemów informacyjnych oraz technologii informacyjnych, które warunkują funkcjonowanie określonych stosunków społecznych, politycznych i ekonomicznych. Infrastruktura informacyjna obejmuje instytucje, zasoby i systemy oraz technologie informacyjne, które określają działanie systemów społecznych, politycz-

[1] Izabela Oleksiewicz, dr hab., oleiza@prz.edu.pl, ORCID: 0000-0002-1622-7467

nych i ekonomicznych. Jej zadaniem jest gromadzenie, przechowywanie i udostępnianie informacji dla społeczeństwa, gospodarki oraz działalności politycznej (Oleński 2003, s. 15; Oleksiewicz 2017, s. 99).

Cyberprzestępczość jest zjawiskiem obecnie powszechnie znanym, którego skutki rozprzestrzeniają się w zawrotnym tempie w społeczeństwie informacyjnym. Decydują o tym uwarunkowania tego zjawiska, z którego najistotniejszą rzeczą jest transgraniczność. Brak granic powoduje, że cyberprzestępcy z łatwością przenikają obszary poszczególnych państw. Z reguły prowadzą swoje działania w jednym miejscu, zaś ich skutki są widoczne w miejscu oddalonym o tysiące kilometrów, nierzadko na innym kontynencie. Utrudnia to wyznaczenie systemu prawnego, według którego miałoby następować ściganie takich przestępstw. Z drugiej strony w znacznym stopniu komplikuje również wyznaczenie podmiotów odpowiedzialnych za podejmowanie działań ochronnych i zapobiegawczych. Kolejną kwestią jest anonimowość, która nie sprzyja przyśpieszaniu postępowania karnego i wykrycia sprawców przestępstwa oraz sposobów ich działania. Nie jest to jednak całkowicie niemożliwe, ale wymaga podjęcia żmudnych poszukiwań i wdrożenia dobrze przemyślanych, zaplanowanych działań (Polinceusz, Pomykała 2013, s. 660; Oleksiewicz 2014, s. 114-115).

Cyberprzestępczością nazywa się zakazane formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową, Internetem, gdzie naczelnym celem jest naruszenie jakiegokolwiek dobra chronionego prawem (Białoskórski 2011, s. 63). Cyberprzestępstwo jako czyn zabroniony odróżnia się przede wszystkim miejscem działania w środowisku internetowym, gdzie technologia komputerowa i wykorzystanie sieci komputerowych warunkuje popełnienie tego popełniania przestępstwa (Siwicki 2013, s. 20). Jego globalny charakter dzięki Internetowi wpłynął na niezwykle szybką komunikację i przeniesienie większości form aktywności człowieka do sieci, także i tych negatywnie odbieranych. Zmienił się kontekst pojęcia „cyberterroryzm", które jest również obecnie używane w aspekcie politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych dążeń w szerokim rozumieniu tego słowa (Liedel, Piasecka 2011, s. 18).

W cyberprzestrzeni pojawiają się zatem te same problemy co w świecie rzeczywistym, dotyczące społeczności informacyjnej. Należy więc stwierdzić, że cyberprzestępczość jest nowoczesną odmianą przestępstwa, idącą za postępem i możliwościami techniki cyfrowej oraz Internetu.

Stany nadzwyczajne według Konstytucji RP

Konstytucja RP rozróżnia trzy stany nadzwyczajne: stan wojenny, stan wyjątkowy i stan klęski żywiołowej (Dz.U. 1997 nr 78 poz. 483). Wprowadzenie stanu nadzwyczajnego nie jest wynikiem zaistnienia ściśle określonych warunków (Sarnecki 2015, s. 78). Stan nadzwyczajny może być wprowadzony poprzez rozpo-

rządzenie zgodnie z obowiązującą ustawą. Ustawa określa zasady i tryb wyrównywania strat majątkowych wynikających z wprowadzonych ograniczeń (por.: Garlicki 2016, s. 187).

Jednym z podstawowych skutków wprowadzenia stanu nadzwyczajnego jest ograniczenie sfery wolności i praw jednostki. Ten istotny problem został uregulowany w art. 233 ust. 1 Konstytucji RP, która wskazuje wyraźnie, jakie z konstytucyjnych wolności i praw mogą być ograniczone i w jakim zakresie, a które w żadnym przypadku ograniczeniom nie podlegają. Jednocześnie nie pozostawia organom władz publicznych swobody w określaniu, jakie wolności i prawa mogą podlegać ograniczeniom (Konstytucja RP, poz. 483).

T. Bryk stwierdza, że „zasada wyjątkowości polega na tym, że stan wyjątkowy wprowadzić można wyłącznie w przypadku szczególnego zagrożenia, gdy inne środki są niewystarczające" (Bryk 2011, s. 225). W ocenie tego autora zasada legalności wymusza wprowadzenie stanu tylko w formie rozporządzenia i zgodnie z ustawą. Zasada proporcjonalności obliguje natomiast do zastosowania takich instrumentów i środków, które odpowiadają istniejącym zagrożeniom podczas stanu nadzwyczajnego. Z kolei zasada celowości zakłada, że działania podjęte w czasie jego trwania powinny zmierzać do jak najszybszego przywrócenia normalnego działania państwa. Nie można zapomnieć o zasadzie ochrony podstaw systemu prawnego, z której wynika zakaz modyfikacji prawa podczas stanu nadzwyczajnego, m.in. Konstytucji czy samej ustawy o stanach nadzwyczajnych.

Trzecia przesłanka, którą jest zagrożenie konstytucyjnego ustroju państwa, ma bardzo „indywidualny" czy „prywatnoprawny" charakter. Zagrożeniem dla konstytucyjnego ustroju państwa mogą być takie zjawiska jak: zamach stanu, daleko posunięte działania prowadzące do usamodzielnienia określonych części obszaru państwowego, wstrzymanie powszechnych procesów wyborczych czy eliminacja z życia publicznego niezbędnego segmentu stronnictw politycznych (por.: Szmulik 2015).

Konsekwencją stanu nadzwyczajnego jest na przykład zakaz wprowadzenia skrócenia kadencji Sejmu. Mało tego, kadencja Parlamentu nie może w tym okresie ulec zakończeniu, a jednocześnie następuje jej obligatoryjne przedłużenie. Jest to konsekwencją tego, że w okresie 90 dni od zakończenia stanu nadzwyczajnego nie może być zarządzone referendum ogólnokrajowe czy wybory parlamentarne, prezydenckie i samorządowe.

Działania organów upoważnionych do wprowadzenia stanów nadzwyczajnych (Rady Ministrów, która występuje z wnioskiem, Prezydenta, który zarządza, wydając rozporządzenia) znajdują się pod kontrolą Sejmu i to od początku ich obowiązywania. Konstytucja zobowiązuje Prezydenta do przedłożenia Sejmowi w ciągu 48 godzin od podpisania aktu prawnego rozporządzenia o wprowadzeniu stanu wojennego lub wyjątkowego. Rozporządzenie to Sejm jest zobowiązany rozpatrzyć niezwłocznie, a mając zastrzeżenia co do jego zasadności, może je uchylić bezwzględną większością głosów.

Skutkiem uchylenia takiego rozporządzenia jest zniesienie ograniczeń dotyczących wolności i praw człowieka i obywatela oraz powrót do normalnych zasad funkcjonowania władz publicznych.

W związku z tym, że stan nadzwyczajny jest wprowadzany w drodze rozporządzenia, ten akt prawny powinien uściślać (ewentualnie zawężać, gdyż niedopuszczalne jest rozszerzenie), które z uprawnień jednostki podlegających na mocy ustawy ograniczeniu mogą być w konkretnym przypadku ograniczone.

Konstytucja nie dopuszcza (Konstytucja RP, art. 228 ust. 6 i 7), by w okresie stanu nadzwyczajnego mogły być zmieniane regulacje prawne odnoszące się do sytuacji jednostki. Stąd wynika też zakaz zmiany Konstytucji oraz ustaw o stanach nadzwyczajnych w tym okresie.

Zakaz wprowadzania ograniczeń w warunkach obowiązywania stanu wojennego i wyjątkowego obejmuje 14 artykułów Konstytucji dotyczących wolności i praw jednostki, a ponadto istnieje dodatkowy zakaz dyskryminacji jednostki z powodu rasy, płci, języka, wyznania, pochodzenia społecznego, urodzenia i majątku. Przewidziana została także zasada wyrównywania strat majątkowych wynikających z ograniczeń wolności i praw jednostki w czasie obowiązywania stanu nadzwyczajnego (Konstytucja RP, art. 228 ust. 4).

Zupełnie innej natury są przesłanki do wprowadzenia stanu wyjątkowego, są one wyraźnie wskazane w Konstytucji. Pierwszą przesłanką jest zagrożenie konstytucyjnego ustroju państwa, i to nie ze strony czynników zewnętrznych, lecz czynników natury wewnętrznej, np. groźba zamachu stanu i usunięcia siłą konstytucyjnych władz państwa. Drugą stanowi zagrożenie bezpieczeństwa obywateli wskutek wydarzeń w rodzaju zamieszek i zjawisk destabilizujących państwo. Trzecią jest zagrożenie porządku publicznego i normalnego funkcjonowania życia w państwie.

Do wprowadzenia stanu wyjątkowego uprawniony jest również Prezydent działający także na wniosek Rady Ministrów zgodnie z art. 230 Konstytucji. Artykuł 230 ust. 2 utrzymuje prawo Sejmu do przedłużenia stanu wyjątkowego, ale tylko na czas nie dłuższy niż 60 dni. W sumie stan wyjątkowy nie może trwać dłużej niż 150 dni (czyli 5 miesięcy). Problem ten szerzej reguluje ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Garlicki 2016, s. 234).

Zgodnie z art. 232 Konstytucji w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia Rada Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, stan klęski żywiołowej na części albo na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu.

Polityka antycyberterrorystyczna RP w zakresie walki z cyberprzestępczością

Na tle innych państw członkowskich UE Polska jest dopiero na początku budowy zintegrowanego systemu bezpieczeństwa cyberprzestrzeni. Jedną z pierwszych podstaw była przyjęta przez Komitet Stały Rady Ministrów 25 czerwca 2013 r. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*. Zawiera ona koncepcję systemu zarządzania cyberprzestrzenią oraz definiuje zależności między poszczególnymi organami i instytucjami państwowymi, a także ich wyspecjalizowa-

nymi komórkami odpowiedzialnymi za zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego w cyberprzestrzeni. Jest to dokument o charakterze rządowym (por.: Adamczuk, Liedel 2015, s. 286; Szajt 2014, s. 46).

Polityka Ochrony Cyberprzestrzeni RP jako cel strategiczny wskazuje osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. W celu jego realizacji należy stworzyć ramy organizacyjno-prawne oraz system skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami cyberprzestrzeni Rzeczypospolitej Polskiej. Do szczegółowych zadań zalicza się np. zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa oraz zdolności do przeciwdziałania zagrożeniom w cyberprzestrzeni, a także ograniczanie skutków ataków godzących w bezpieczeństwo teleinformatyczne. Ponadto należy doprecyzować i jednoznacznie określić funkcje i zadania podmiotów odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni. Duże znaczenie będzie mieć umiejętne stworzenie spójnego systemu zarządzania bezpieczeństwem w cyberprzestrzeni mającego na celu trwałą wymianę informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni. Zgodnie z *Polityką Ochrony Cyberprzestrzeni* nie powinno się zapominać o stałej edukacji użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni (Dziędziela, Szajt, 2015, s. 67-68).

We wspomnianym dokumencie wskazano m.in., że w obliczu wielu coraz częściej występujących zagrożeń niezbędne jest skoordynowanie działań, które umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom teleinformatycznym i oferowanym przez nie usługom. Systemy teleinformatyczne eksploatowane przez administrację zarówno rządową, jak i samorządową, organy władzy ustawodawczej, władzę sądowniczą, a także systemy strategiczne z punktu widzenia bezpieczeństwa państwa oraz przedsiębiorców i osób fizyczych zostały objęte *Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (http://cyberpolicy.nask.pl).

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej zaprezentowana 22 stycznia 2015 r. określa warunki do zespolenia i strategicznego ukierunkowania wysiłków na rzecz budowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Przede wszystkim określa cel strategiczny, który ma zostać osiągnięty przez implementację zadań o charakterze operacyjnym i przygotowawczym w dziedzinie cyberbezpieczeństwa. Ponadto zawiera ocenę zagrożeń, ryzyk i szans w dynamicznie rozwijającym się środowisku cyberbezpieczeństwa, a także wskazuje najważniejsze – jakie czynności operacyjne mają być podjęte w sektorze publicznym, prywatnym i obywatelskim oraz wskazuje czynności przygotowawcze mające na celu doskonalenie, rozwój i transformację systemu cyberbezpieczeństwa, z uwzględnieniem podsystemu kierowania oraz publicznych i prywatnych ogniw wykonawczych (Adamczuk, Liedel 2015, s. 287).

Zgodnie z przyjętą doktryną zapewnienie bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej powinno być realizowane w kilku płaszczyznach: przez sektor publiczny (w wymiarze państwowym i międzynarodowym), sektor komercyjny, obywatelski oraz w wymiarze transsektorowym. Zadania te można podzielić następująco:

- zadania sektora publicznego w wymiarze państwowym – rozpoznawanie zagrożeń, wymiana informacji, analiza ryzyka, zabezpieczenie kryptologiczne najważniejszych informacji, monitoring i szybkie reagowanie na incydenty w sieci oraz przeciwdziałanie cyberprzestępczości; ważną rzeczą jest stały audyt środków i mechanizmów cyberbezpieczeństwa, opracowanie procedur reagowania na cyberataki oraz implementacja celów dyrektywy NIS;
- zadania sektora publicznego na poziomie międzynarodowym – wymiana informacji, doświadczeń i dobrych praktyk na poziomie międzynarodowym, oddziaływanie za pomocą organizacji międzynarodowych na sektor prywatny oraz udział w reagowaniu na zagrożenia cybernetyczne, a w szczególności w strukturach Unii Europejskiej i NATO;
- zadania sektora komercyjnego – współpraca z sektorem publicznym obejmująca wymianę informacji o potencjalnych zagrożeniach dla cyberbezpieczeństwa, przeciwdziałanie zagrożeniom, opracowywanie propozycji zmian prawnych oraz wymianę informacji o zagrożeniach i incydentach;
- zadania sektora obywatelskiego – społeczne inicjatywy wspierające cyberbezpieczeństwo, edukowanie i samokształcenie w zakresie bezpieczeństwa w sieci;
- zadania transsektorowe – koordynacja współpracy sektora publicznego i prywatnego, tworzenie mechanizmów wymiany informacji oraz standardów i dobrych praktyk w zakresie cyberbezpieczeństwa (Babiński 2015, s. 197-200).

Obecnie jest już realizowany kolejny Program Strategii Cyberbezpieczeństwa RP opracowany na lata 2017-2022 (MC 2017). Stanowi on kontynuację działań zapoczątkowanych w *Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2011-2016* (MSWiA 2010). Jego głównym zadaniem była implementacja dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii zwanej dalej Dyrektywą NIS (Dz.Urz. UE 2016 L 194). Główne założenia obecnej Strategii to:

- potrzeba zapobiegania i reagowania w odniesieniu do incydentów oraz minimalizacja skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
- stworzenie zasad dobrej współpracy pomiędzy sektorami publicznym i prywatnym,
- umiejętne podejście do oceny ryzyka wystąpienia ataku w cyberprzestrzeni,
- edukacja, informacja i szkolenia na temat cyberbezpieczeństwa,
- działania odnoszące się do planów badawczo-rozwojowych z zakresu bezpieczeństwa teleinformatycznego,
- współpraca międzynarodowa dotycząca cyberbezpieczeństwa.

Podsumowanie

Istotnym problemem Polski jest ustalenie zasad bezpieczeństwa w cyberprzestrzeni. Z roku na rok zwiększa się liczba incydentów komputerowych, zorganizowanych cyberataków i nowych zagrożeń, w tym związanych z cyberterroryzmem. Przestrzeń wirtualna jest środowiskiem szalenie dynamicznym, co generuje potrzebę

wprowadzania prawno-organizacyjnych i systemowych zmian. Polska jest zupełnie nieprzygotowana na możliwość wystąpienia zmasowanego ataku cybernetycznego, a jego zaistnienie dałoby podstawę do wprowadzenia stanu nadzwyczajnego.

Warto w tym miejscu zaznaczyć, że w Polsce pomimo wprowadzenia dyrektywy NIS nie ma nadal ustawowych przepisów wskazujących zakres kompetencji organów w obszarze cyberbezpieczeństwa, pomimo że takie założenia zostały przyjęte w obecnym *Programie Strategii Cyberbezpieczeństwa RP*. Jednocześnie nie należy zapominać o ciągłym monitorowaniu cyberprzestrzeni, chociaż podjęcie decyzji o wprowadzeniu danego rodzaju stanu nadzwyczajnego będzie zależeć od oceny stopnia zagrożenia bezpieczeństwa państwa. Kwestią bezsporną pozostaje objęcie ochroną cyberprzestrzeni ze względu na jej wpływ na bezpieczeństwo narodowe, a w szczególności finanse publiczne państwa. Z kolei rzeczą problematyczną pozostaje sama ocena zagrożenia cyberprzestrzeni.

Konkludując, warto podkreślić fakt, że chociaż ustawodawca polski przewidział w art. 3 Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. 2002 nr 62 poz. 558) możliwość wprowadzenia takiego stanu nadzwyczajnego m.in. w przypadku tzw. awarii technicznej rozumianej jako nieprzewidziane uszkodzenie urządzenia technicznego lub systemu urządzeń technicznych powodującego przerwę w ich używaniu lub utratę ich właściwości, której skutki zagrażają życiu lub zdrowiu dużej liczby osób lub mieniu w wielkich rozmiarach. Dlatego ważne byłoby wprowadzenie do polskiej legislacji, a przede wszystkim do ustaw regulujących stany nadzwyczajne, pojęcia cyberprzestępczości, co zgodne jest zarówno z samą Strategią RP, jak i dyrektywą NIS (por.: Frańczuk 2014, s. 86-87).

Poza tym analiza aktualnego stanu prawnego prowadzi do przekonania, że szczególną rolę w modelowaniu i unifikacji prawa cyberprzestrzeni odgrywa *soft law* – tzw. miękkie prawo. Mimo że prawo miękkie nie ma charakteru prawnie wiążącego, nie można go bagatelizować. Model tworzenia *soft law* odpowiada wolnościowej i oddolnej strukturze cyberprzestrzeni. Dopuszczenie do dyskusji podmiotów prywatnych oraz nowych aktorów, którym tradycyjnie nie przypisuje się atrybutu podmiotu prawa międzynarodowego, powoduje zapewnienie równowagi i proporcjonalności pomiędzy dążeniami rządów a zabezpieczeniem interesu użytkowników przestrzeni wirtualnej. Ogromne znaczenie mają rezolucje Zgromadzenia Ogólnego ONZ oraz niewiążące akty unijne. Mogą one szybko reagować na zmieniającą się sytuację technologiczno-społeczną. *Soft law* może też być pewnym drogowskazem dla państw, wskazaniem pożądanego kierunku rozwoju cyberprzestrzeni. Co więcej, akty o charakterze prawa miękkiego mogą być doskonałą podstawą do stworzenia konwencji wielostronnych. Jeśli zaproponowany przez rezolucję, postanowienie czy zalecenie tryb postępowania będzie ogólnie stosowany, może również doprowadzić do wykształcenia się normy zwyczajowej.

Dotychczasowe regulacje prawa międzynarodowego dotyczące cyberprzestrzeni są z zasady niewystarczające i nieadekwatne. Międzynarodowe regulacje są fragmentaryczne i rozproszone, niekompleksowe, nie oferują jednolitej terminologii. Na gruncie prawa karnego konwencja o cyberprzestępczości pełni rolę pewnego wzoru, zbioru minimalnych standardów dotyczących walki z działaniami przestęp-

czymi w sieciach cyfrowych. Podobnych rozwiązań brak jednak w innych dziedzinach prawa. Przestrzeń cyfrowa szczególnie skomplikowała tematykę regulacji w obrębie praw własności intelektualnych oraz obrotu gospodarczego. Cyberprzestrzeń jest obszarem, na który w sposób naturalny wpływa technologia i nowe innowacyjne rozwiązania. Przestrzeń ta szybko inkorporuje nowości techniczne, pozostawiając prawo w tyle. Dlatego też wciąż brak jest międzynarodowych dokumentów regulujących status prawny chmury obliczeniowej, walut wirtualnych, usług cyfrowych oraz innych form działalności człowieka w cyberprzestrzeni. Wydaje się, że w chwili obecnej mamy do czynienia z *law in action*, prawem w działaniu rozumianym jako stopniowe formułowanie się dziedziny prawa cyberprzestrzeni. Państwa i organizacje międzynarodowe mają świadomość niedoskonałości przyjętych rozwiązań i ciągle pracują nad nowymi regulacjami. Można więc przypuszczać, że w kolejnych latach powstanie wiele nowych propozycji legislacyjnych w zakresie prawa cyberprzestrzeni. Powinny one być elastyczne, przejrzyste, efektywne, adekwatne i neutralne technologicznie.

Literatura

1. Adamczuk M., Liedel K. (2015), *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 12.
2. Aleksandrowicz T.R., Liedel K. (2014), *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, [w:] Liedel K., Piasecka P., Aleksandrowicz T.A. (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa.
3. Babiński A. (2015), *Bezpieczeństwo cyberprzestrzeni – wyzwania dla państwa*, [w:] Babiński A., Jurgilewicz M., Malec N. (red.), *Państwo. Prawo. Bezpieczeństwo*, t. 1, Wyższa Szkoła Policji w Szczytnie, Szczytno.
4. BBN (2014), *Doktryna Komorowskiego – założenia*, Biuro Bezpieczeństwa Narodowego, http://bbn.gov.pl (dostęp: 28.06.2017)
5. Białoskórski R. (2011), *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa.
6. Bryk T. (2011), *Przegląd regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego", nr 1.
7. Denning D. (2000), *Cyberterrorism*, „Global Dialogue", Autumn.
8. Denning D. (b.r.), *Is Cyber Terror Next?*, www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc (dostęp: 15.04.2017).
9. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. (Dz.Urz. UE 2016 L194).
10. Dziędziela E., Szajt M. (2015), *Zarządzanie bezpieczeństwem miasta w świetle badań sondażowych wśród jego mieszkańców*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie", nr 17.
11. „e-Terroryzm.pl" 2012, nr 5(5).
12. Franczuk M. (2014), *Zagrożenia bezpieczeństwa i porządku publicznego w cyberprzestrzeni jako przesłanka wprowadzenia stanów nadzwyczajnych ze szczególnym uwzględnieniem bezpieczeństwa finansowego*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", nr 2(926).
13. Garlicki L. (2016), *Konstytucja RP. Komentarz*, Wydawnictwo Sejmowe, Warszawa.
14. Jaskuła S. (2010), *Informacyjna przestrzeń tożsamości*, Ośrodek Rozwoju Edukacji, Warszawa.

15. Konstytucja RP, Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 nr 78 poz. 483).
16. Kwećka R. (2014), *Strategia bezpieczeństwa informacyjnego państwa*, Warszawa.
17. Liedel K., Piasecka P. (2011), *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe", nr 1.
18. MC (2017), *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Ministerstwo Cyfryzacji, Warszawa, https://mc.gov.pl/aktualnosci/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 (dostęp: 10.04.2017).
19. MSWiA (2010), *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf (dostęp: 25.10.2015).
20. NIK (2015), https://www.nik.gov.pl/aktualnosci/sprawozdanie-z-dzialalnosci-nik-2015.html (dostęp: 27.04.2018).
21. Obwieszczenie Prezesa Rady Ministrów o sprostowaniu błędów w Konstytucji (Dz.U. 2001 nr 28 poz. 319).
22. Oleksiewicz I. (2014), *Ochrona praw jednostki a problem cyberterroryzmu*, „HSS", Vol. 19, No. 21(1).
23. Oleksiewicz I. (2017), *Bezpieczeństwo informacyjne jako wyzwanie w XXI wieku*, „Zeszyty Naukowe WSAiZ", t. 15, z. 4(41).
24. Oleksiewicz I., Krztoń W. (2017), *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Rambler, Warszawa.
25. Oleński J. (2003), *Ekonomika informacji. Metody*, PWE, Warszawa.
26. Polinceusz M., Pomykałą M. (2013), Och*rona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, [w:] Bogdalski P., Nowakowski Z., Płusa T., Rajchel J., Rajchel K. (red.), *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, WSPol, WSIZiA, WSOSP, WIM, Warszawa.
27. Sarnecki P. (red.) (2015), *Prawo konstytucyjne RP*, C.H. Beck, Warszawa.
28. Steinmüller W. (1977), *Zautomatyzowane systemy informacyjne w administracji prywatnej i publicznej*, „Organizacja – Metoda – Technika", nr 9.
29. Suchorzewska A. (2010), *Ochrona prawna systemów informatycznych*, Wolters Kluwer, Warszawa.
30. Szajt M. (2014), *Zmiany w strukturze działowo-gałęziowej w Polsce na tle innych państw europejskich*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie", nr 14.
31. Szmulik B. (2015), *Konstytucyjny system organów państwowych*, Wolters Kluwer, Warszawa.
32. Ustawy o stanie klęski żywiołowej z dnia 18 kwietnia 2002 r. (Dz.U. 2002 nr 62 poz. 558).
33. Ustawa o zmianie Konstytucji Rzeczypospolitej Polskiej z dnia 7 maja 2009 r. (Dz.U. 2009 nr 114 poz. 946).
34. Ustawa o zmianie Konstytucji z dnia 8 września 2006 r. (Dz.U. 2006 nr 200 poz. 1471).

INFORMATION SECURITY IN CYBERSPACE AND EMERGENCY STATES IN THE REPUBLIC OF POLAND

Abstract: The aim of this article is to analyze the country's information security in the 21st century and the legal challenges it poses. It was also considered necessary to show the progressive complexity of the scope of the subject of information security, that is the phenomena and processes, with particular emphasis on those taking place in emergency states, on the example of Poland. According to the author, it is worth paying attention to such essential and important issues that are constantly changing due to many factors such

as innovation or globalization. This is an issue currently occupying an interest among the researchers of the phenomenon of security. It was also found that in conditions of increased interdependence and the emergence of qualitatively new features of the information security environment, it is necessary to show the evolution and progressive complexity of the forms, structures and mechanisms of the current legal regulations regarding cyberspace, which are in principle insufficient and inadequate.

Keywords: information security, cyberspace of the Republic of Poland, emergency states, anti-cyberterrorist policy, management