Zeszyty Naukowe Uniwersytet Ekonomiczny w Krakowie

2(926)

ISSN 1898-6447
Zesz. Nauk. UEK, 2014; 2(926): 71–87

Magdalena Frańczuk
Katedra Prawa Publicznego
Uniwersytet Ekonomiczny w Krakowie

Zagrożenie bezpieczeństwa i porządku publicznego działaniami w cyberprzestrzeni jako przesłanka wprowadzenia stanów nadzwyczajnych ze szczególnym uwzględnieniem bezpieczeństwa finansowego

Streszczenie

W niniejszym opracowaniu przedstawiono zarys problematyki związanej z możliwością wprowadzenia jednego z wymienionych w Konstytucji RP stanów nadzwyczajnych w sytuacji zagrożenia bezpieczeństwa obywateli i porządku publicznego działaniami w cyberprzestrzeni. Przytoczono definicje cyberprzestrzeni oraz zwrócono uwagę na zagrożenia panujące w niej we współczesnym świecie. W tym zakresie powołano się zarówno na regulacje krajowe, jak i międzynarodowe. W dalszej części opracowania odwołano się także do pojęcia bezpieczeństwa finansowego państwa i podjęto próbę jego zdefiniowania. Bezpieczeństwo finansowe nie jest bowiem uregulowane wprost ani w Konstytucji RP, ani w aktach prawnych niższych rangą. W omawianym kontekście interesująca jest przede wszystkim płaszczyzna zagrożenia atakami hakerskimi mogącymi powodować bezpośrednie zagrożenie dla systemu finansowego państwa, a w konsekwencji – zagrożenie bezpieczeństwa finansowego obywateli i porządku publicznego.

Słowa kluczowe: cyberatak, bezpieczeństwo, przepisy, porządek publiczny, finanse.

1. Wprowadzenie

Niniejsze opracowanie stanowi refleksję nad stosunkowo niedawno włączoną do prawa polskiego regulacją pozwalającą na wprowadzenie stanu nadzwyczajnego w sytuacji zagrożenia bezpieczeństwa obywateli i porządku publicznego działaniami w cyberprzestrzeni. Możliwość taką daje obecnie Konstytucja RP oraz obowiązujące w tym zakresie ustawy. W artykule przeanalizowano nie tylko akty prawa krajowego – nawiązano także do regulacji międzynarodowych. Jako punkt wyjścia przyjęto rozważania nad definicją cyberprzestrzeni. Podjęto również próbę zrekonstruowania definicji bezpieczeństwa finansowego, nie istnieje bowiem spójna definicja tego pojęcia ani w pracach o charakterze ekonomicznym, ani prawniczym.

Należy podkreślić, że w obecnym stanie prawnym możliwość wprowadzenia stanu wyjątkowego, stanu wojennego bądź stanu klęski żywiołowej istnieje odpowiednio:

1) w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych (w przypadku stanu wyjątkowego)[1],

2) w razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami w cyberprzestrzeni (w przypadku stanu wojennego)[2],

3) w przypadku m.in. awarii technicznej, rozumianej jako gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, 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 (w przypadku stanu klęski żywiołowej)[3].

Jak wskazują M. Grzelak i K. Liedel [2012, s. 132], niebezpieczeństwo w cyberprzestrzeni wychodzi poza ramy czynu o charakterze przestępczym w rozumieniu kodeksu karnego. W skrajnych przypadkach działanie takie może bowiem przybrać postać, która w świetle Konstytucji stanowi podstawę do wprowadzenia jednego ze stanów nadzwyczajnych.

---

[1] Art. 2 Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym [Ustawa z dnia 21 czerwca 2002 r. …], zwanej dalej ustawą o stanie wyjątkowym.

[2] Art. 2 Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i o zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej [Ustawa z dnia 29 sierpnia 2002 r.], zwanej dalej ustawą o stanie wojennym.

[3] Art. 3 Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej [Ustawa z dnia 18 kwietnia 2002 r. …], zwanej dalej ustawą o stanie klęski żywiołowej.

2. Cyberprzestrzeń – definicja, zagrożenia

2.1. Definicja cyberprzestrzeni

Cyberprzestrzeń była początkowo pojęciem używanym na określenie rzeczywistości wirtualnej, czyli sztucznej rzeczywistości, będącej połączeniem elementów świata realnego z fikcyjnym, tworzonej przy wykorzystaniu technologii informatycznych. Definiowano ją jako „sposób użycia technologii komputerowej w tworzeniu efektu interaktywnego trójwymiarowego świata, w którym obiekty dają wrażenie przestrzennej obecności" ([Burdea i Coiffet 2003, s. 20] za: [Stepaniuk 2011, s. 75]). Z czasem znaczenie tego pojęcia uległo zmianie. Obecnie cyberprzestrzeń jest rozumiana przede wszystkim jako przestrzeń wirtualna, w której funkcjonują połączone siecią (najczęściej przez Internet) i komunikujące się ze sobą komputery oraz inne media cyfrowe. Jest to zatem przestrzeń w głównej mierze informatyczna, ale – co należy podkreślić – także nowy i bardzo popularny rodzaj przestrzeni społecznej. Według A. Wadhwa i S.B. Kotha z Uniwersytetu w Waszyngtonie cyberprzestrzeń jest specjalnym rodzajem społecznego miejsca otwartego, gdzie ludzie mogą łączyć się za pomocą komputerów (za: [Szpunar 2004, s. 107]). Sieci komputerowe pozwalają na komunikację „jeden do jednego" lub „wielu do wielu", co sprzyja powstaniu nowych form społecznych – społeczności wirtualnych.

Taka społeczna cyberprzestrzeń stanowi doskonałe pole do pożądanych i legalnych działań, ale jest także miejscem działań niezgodnych z prawem i zagrażających interesom państwa, podmiotów zbiorowych, jak i całej rzeszy jednostek składających się na wirtualną (w sensie zgromadzoną w cyberprzestrzeni) społeczność. Wobec wzrostu popularności Internetu i skali zagrożeń z nim związanych obecnie jednym z priorytetów państwa powinna być ochrona obywateli nawiązujących interakcje w cyberprzestrzeni oraz organizujących się tam w różne formy społeczne. Pamiętać należy, że społeczność wirtualna stanowi zbiór realnie istniejących obywateli, którzy działają zarówno poprzez Internet, jak i w świecie rzeczywistym.

Jako pojęcie prawne cyberprzestrzeń została zdefiniowana w ustawie o stanie wyjątkowym, w ustawie o stanie wojennym oraz w ustawie o stanie klęski żywiołowej. W tym miejscu warto wspomnieć, że w ramach wszystkich tych ustaw przepisy dotyczące cyberprzestrzeni wprowadzono w życie stosunkowo niedawno, mianowicie dnia 2 listopada 2011 r.[4] W uzasadnieniu prezydenckiego projektu

[4] Zob. 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 [Ustawa z dnia 30 sierpnia 2011 r. …].

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 wskazano, że „obecnie obserwuje się niezwykle dynamiczny proces przenoszenia aktywności ludzkiej w przestrzeń wirtualną, będącą składową obszaru cyberprzestrzeni. Dotyczy to nie tylko działalności osób fizycznych, ale również administracji publicznej, przedsiębiorców, organizacji społecznych i innych podmiotów. Działalność w cyberprzestrzeni staje się nieodzownym elementem funkcjonowania państwa i społeczeństwa. Należy jednak zauważyć, że postępujący proces informatyzacji, obok niewątpliwych korzyści, rodzi również określone zagrożenia. W szczególności dotyczy to możliwości wykorzystania cyberprzestrzeni w celach sprzecznych z interesami państwa i jego obywateli. Przykładem tego rodzaju zagrożeń są liczne ataki hakerów na różnego rodzaju instytucje o istotnym znaczeniu dla funkcjonowania państwa i społeczeństwa. Ataki takie mogą być niezwykle groźne, bowiem w ich efekcie może dojść do poważnych zakłóceń w funkcjonowaniu państwa, w tym jego struktur i gospodarki. Biorąc powyższe pod uwagę, państwo powinno być przygotowane zarówno na odparcie takich ataków, jak i zwalczanie jego skutków" [Przedstawiony przez Prezydenta Rzeczypospolitej Polskiej projekt…]. Konsekwencją nowych, bardzo realnych zagrożeń współczesnego świata jest konieczność stworzenia jednolitej prawnej definicji cyberprzestrzeni także na potrzeby ustaw regulujących stany nadzwyczajne.

Pojęcie cyberprzestrzeni pojawia się często w obowiązującym prawie – tak międzynarodowym, jak i krajowym. Występuje ono także w innych poza przepisami regulującymi stany nadzwyczajne aktami prawnymi, z których na uwagę zasługuje przede wszystkim Konwencja o cyberprzestępczości z dnia 23 listopada 2001 r., implementowana do prawa polskiego Ustawą z dnia 18 marca 2004 r. o zmianie ustawy „Kodeks karny", ustawy „Kodeks postępowania karnego" oraz ustawy „Kodeks wykroczeń" [Ustawa z dnia 18 marca 2004 r. …][5]. Należy ponadto zwrócić uwagę na fakt, że Polska jest sygnatariuszem wielu aktów prawa międzynarodowego mających znaczenie dla bezpieczeństwa teleinformatycznego.

[5] Do podstawowych aktów prawnych w zakresie bezpieczeństwa zasobów teleinformatycznych należą: [Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. …, Ustawa z dnia 6 czerwca 1997 r. „Kodeks karny"…, Ustawa z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne"…, Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu…, Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego…, Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym…, Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne…, Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych…, Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych…, Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych…, Ustawa z dnia 29 sierpnia 1997 r. „Prawo bankowe"…].

W tym miejscu warto także przywołać Program sztokholmski na lata 2010––2014 (2010/C115/01), który wraz z Planem działania (COM (2010)/171) stanowi dokument unijny zalecający opracowanie strategii bezpieczeństwa wewnętrznego Unii Europejskiej, koncentrując się m.in. na cyberprzestępczości [*Program sztokholmski…* 2010]. W pkt 4.4.4 tego dokumentu podkreślono, że Internet znacznie ułatwił komunikację, ale jednocześnie za jego sprawą pojawiły się nowe wyzwania w postaci cyberprzestępczości, ponieważ grupy przestępcze zaczęły skutecznie korzystać z technologii. Unia Europejska powinna zatem propagować politykę i prawodawstwo zapewniające możliwie najwyższy poziom bezpieczeństwa sieci oraz umożliwiające szybsze reagowanie w przypadku zakłóceń i ataków cybernetycznych. W dokumencie wezwano również do zintensyfikowania analizy strategicznej w zakresie cyberprzestępczości oraz uproszczenia przepisów dotyczących jurysdykcji i ram prawnych mających zastosowanie do cyberprzestrzeni w UE. W tym miejscu przywołać można również nową koncepcję strategiczną NATO, przyjętą na szczycie w Lizbonie, w której wskazano ataki cybernetyczne jako jedno z istotnych zagrożeń bezpieczeństwa państw członkowskich Sojuszu Północnoatlantyckiego. Efektem prac nad tą strategią jest dokument NATO zatytułowany *Tallinn Manual on the International Law Applicable to Cyber Warfare*, który stanowi rodzaj instrukcji dotyczących stosowania prawa międzynarodowego podczas cyberwojny. Jak wskazuje jego autor M.N. Schmitt [2013, s. 106], jest to zbiór zasad, którymi państwa członkowskie NATO powinny kierować się w sytuacji cyberataku. Dla niniejszego opracowania zasadnicze znaczenie ma zasada 30 dokumentu, w której zdefiniowano cyberatak jako cyberoperację (a więc operację w cyberprzestrzeni) o charakterze ofensywnym lub defensywnym, która może spowodować realne szkody, śmierć osób albo uszkodzenie lub zniszczenie obiektów [Schmitt 2013, s. 110]. Różne operacje w cyberprzestrzeni mogą być integralną częścią szerszych cyberoperacji składających się na cyberatak. Z tego też względu należy podkreślić, że cyberprzestrzeń nie jest strefą „wolną" od prawa, w której każdy może prowadzić wrogą działalność bez zasad lub jakichkolwiek ograniczeń [Schmitt 2012, s. 15]. Cyberatak czy cyberprzestępstwo mogą więc uzasadniać konieczność wprowadzenia jednego ze stanów nadzwyczajnych uregulowanych w Konstytucji RP.

Należy również nadmienić, że wprowadzenie regulacji cyberprzestępczości do ustaw normujących stany nadzwyczajne jest zgodne z *Rządowym programem ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*. W dokumencie tym wskazano, że w obliczu globalizacji ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa, a obiektem cyberwojny i cyberataków stały się także elementy infrastruktury cywilnej. Programem objęto przede wszystkim systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, organy władzy

ustawodawczej, władzy sądowniczej, samorządu terytorialnego, jak również inne strategiczne z perspektywy bezpieczeństwa państwa podmioty, w tym szczególnie podmioty działające w obszarze bankowości oraz przedsiębiorców i użytkowników indywidualnych cyberprzestrzeni.

W przywołanym wyżej dokumencie wprowadzono definicje kluczowych pojęć z zakresu bezpieczeństwa w cyberprzestrzeni, takich jak [*Rządowy program*… 2010, s. 6]:

– cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami,

– cyberprzestrzeń RP – cyberprzestrzeń w obrębie terytorium państwa polskiego i w lokalizacjach poza jego terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe),

– cyberprzestępstwo – czyn zabroniony, popełniony w obszarze cyberprzestrzeni,

– cyberterroryzm – cyberprzestępstwo o charakterze terrorystycznym,

– cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników; umożliwia ono ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu,

– ochrona cyberprzestrzeni – zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni.

Cyberprzestrzeń została zdefiniowana w ustawach o stanie wojennym, o stanie wyjątkowym oraz o stanie klęski żywiołowej. Art. 2 ust. 1a ustawy o stanie wojennym stanowi, że przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji, tworzoną przez systemy teleinformatyczne określone w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Zgodnie z treścią przywołanego art. 3 pkt 3 system teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów Ustawy z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne". Tak samo definiuje się cyberprzestrzeń w ustawie o stanie wojennym i ustawie o stanie klęski żywiołowej. W ostatniej z nich wprowadzono ponadto zapis, że katastrofę naturalną lub awarię techniczną mogą wywołać również zdarzenia w cyberprzestrzeni (art. 3 ust. 2).

Niektórzy eksperci twierdzą, że przytoczona definicja wiąże się z dużą dowolnością interpretacyjną (można „podciągnąć" pod nią praktycznie każdy system teleinformatyczny), dlatego też zarzucają jej ogólnikowość i nieprecyzyjność[6].

Jedną z największych zatem przeszkód stojących na drodze formalno-prawnego uregulowania kwestii bezpieczeństwa w cyberprzestrzeni, zarówno na poziomie państwowym, jak i międzynarodowym, są według M. Grzelaka i K. Liedela [2012, s. 129] trudności ze spójnym zdefiniowaniem podstawowych terminów z tego zakresu. Problem stanowi nawet uzgodnienie definicji samej cyberprzestrzeni.

2.2. Globalna sieć Internet – zagrożenia we współczesnym świecie

W czasie, gdy cyberprzestrzeń staje się wirtualnym odzwierciedleniem fizycznej rzeczywistości, przenikają do niej również negatywne formy ludzkiej działalności. Słusznie zauważają przywoływani już wyżej M. Grzelak i K. Liedel [2012, s. 126], że konstrukcja stworzonej z myślą o współpracy naukowej sieci internetowej daje duże poczucie anonimowości, wykorzystywana jest przez przestępców, terrorystów, a także niektóre państwa do prowadzenia nielegalnej działalności lub agresji wobec innych podmiotów.

Istnieje wiele form przestępstw komputerowych czy też przestępstw dokonywanych w cyberprzestrzeni. Na oficjalnych stronach Komendy Głównej Policji znaleźć można następujący katalog tego typu zagrożeń [*Cyberprzestępczość…* 2014]:

– *hacking* komputerowy – uzyskanie nieautoryzowanego dostępu do zasobów sieci komputerowej lub systemu komputerowego poprzez ominięcie jego zabezpieczeń,

– podsłuch komputerowy – nieuprawnione przechwycenie wszelkich informacji (obejmujące także uzyskanie danych stanowiących tajemnicę państwową lub służbową),

---

[6] W tym kontekście warto przywołać uwagi skierowane dnia 30 października 2012 r. przez firmę BIODO (Bezpieczeństwo Informacji i Ochrona Danych Osobowych) do Ministerstwa Administracji i Cyfryzacji. W uwagach tych odniesiono się do definicji cyberprzestrzeni zawartej w *Projekcie polityki bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej* i zarzucono, że „nie obejmuje ona komputerów obywateli RP – komputer lub inny sprzęt obywatela, przedsiębiorcy połączony przez router, modem firmy telekomunikacyjnej do Internetu nie jest częścią cyberprzestrzeni i tym samym nie obejmują tych urządzeń pojęcia cyberataku, cyberprzestępstwa. Pojęcie cyberprzestrzeni zostało sztucznie zawężone do zasobów technicznych opisanych w przepisach prawa polskiego. Pojęcia użyte w dokumencie nie są jasne i zrozumiałe dla każdego obywatela RP i tworzą niepotrzebny bałagan prawny". Na stronie internetowej BIODO wskazano, że „celem firmy jest zapewnienie profesjonalnego wsparcia dla podmiotów gospodarczych, administracji publicznej oraz osób fizycznych w zakresie szeroko rozumianego zarządzania bezpieczeństwem informacji" – za: http://www.biodo.pl/.

– sabotaż komputerowy – zakłócanie lub paraliżowanie funkcjonowania systemów informatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli,

– szpiegostwo komputerowe – włączenie się do sieci komputerowej w celu uzyskania wiadomości o charakterze tajemnicy państwowej lub służbowej, której udzielenie obcemu wywiadowi może wyrządzić szkodę RP,

– bezprawne niszczenie informacji – naruszenie integralności komputerowego zapisu informacji, które może nastąpić w wyniku bezprawnego niszczenia, uszkadzania, usuwania lub zmiany zapisu istotnej informacji albo udaremniania czy utrudniania osobie uprawnionej zapoznanie się z nią,

– zakłócenie automatycznego przetwarzania informacji związane ze sprowadzeniem niebezpieczeństwa powszechnego – dotyczące większej liczby osób lub mienia w znacznych rozmiarach.

W Polsce podstawowym aktem prawnym, na którym opiera się walka z cyberprzestępczością, jest kodeks karny [Ustawa z dnia 6 czerwca 1997 r. …]. Uregulowano w nim wskazane wyżej oraz inne przestępstwa komputerowe, tj. *hacking* – art. 267, podsłuch komputerowy (*sniffing*) – art. 267 § 3, udaremnienie uzyskania informacji – art. 268, sabotaż komputerowy – art. 269, rozpowszechnianie złośliwych programów oraz *cracking* – art. 269a, posługiwanie się narzędziami hackerskimi – art. 269b, oszustwo komputerowe – art. 287. Wśród innych aktów prawnych dotyczących cyberprzestępczości można wymienić Ustawę z dnia 27 lipca 2001 r. o ochronie baz danych [Ustawa z dnia 27 lipca 2001 r. …], Ustawę z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną, opartych lub polegających na dostępie warunkowym [Ustawa z dnia 5 lipca 2002 r. …], a także Ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [Ustawa z dnia 18 lipca 2002 r. …].

Na oficjalnym policyjnym portalu zamieszczono także następującą informację: „Polska w ostatnich latach stała się jednym z lepiej nasyconych i rozwijających się w Europie rynków komputerowych. Komputery i urządzenia cyfrowe oraz Internet odgrywają coraz większą rolę w prowadzeniu nielegalnej działalności lub też w znaczny sposób pomagają w jej prowadzeniu, poprzez możliwości, które oferują m.in. pirackie oprogramowanie, różnego rodzaju oszustwa oraz przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. To wszystko czyni z komputerów i globalnej sieci Internet potężne narzędzie do popełniania przestępstw. Przestępstwa komputerowe leżą w zainteresowaniu zarówno zorganizowanych grup przestępczych, które wykorzystują Internet i systemy komputerowe jako nowy instrument prowadzenia nielegalnej działalności, jak i pojedynczych cyberprzestępców. Przestępstwa komputerowe obejmują przestępstwa, w których przetwarzanie danych jest przedmiotem czynności wykonawczych (przestępstwa komputerowe *sensu stricto*), oraz przestępstwa, w których komputer jest jedynie

środkiem do jego popełnienia (przestępstwa komputerowe *sensu largo*)" [*Zwalczaj cyberprzestępczość…* 2014]. Z uwagi na prognozowany wzrost przestępczości popełnianej z wykorzystaniem Internetu i zaawansowanych technologii oraz potrzebę bezpośredniej i szybkiej wymiany informacji pomiędzy organami ścigania a społeczeństwem Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Służby Kryminalnej Komendy Głównej Policji utworzył punkt kontaktowy przeznaczony do przekazywania drogą elektroniczną (na adres poczty elektronicznej: cyber-kgp@policja.gov.pl) informacji pomocnych w zwalczaniu cyberprzestępczości.

Warto też zwrócić uwagę na Dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW. Celem tej dyrektywy jest „zbliżenie prawa karnego państw członkowskich UE w dziedzinie ataków na systemy informatyczne, przez ustanowienie zasad minimalnych dotyczących definicji przestępstw i odpowiednich kar, oraz poprawa współpracy między właściwymi organami, w tym policją i innymi wyspecjalizowanymi organami ścigania w państwach członkowskich, a także właściwymi wyspecjalizowanymi agencjami i organami Unii, takimi jak Eurojust, Europol i należące do niego Europejskie Centrum ds. Walki z Cyberprzestępczością oraz Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)" [Dyrektywa Parlamentu Europejskiego …].

Zgodnie z danymi firmy konsultingowej Deloitte cyberprzestępczość znalazła się na trzecim miejscu wśród globalnych zagrożeń (w latach 2012–2013 awansowała z dwunastego miejsca). Według jednego ze starszych menedżerów działu zarządzania ryzykiem Deloitte „ten swoisty awans to efekt nagłośnienia wielu groźnych ataków w sieci, których dopuścili się przestępcy wobec największych i najbardziej liczących się organizacji na świecie. W tej chwili mogą one dotknąć każdego, bez względu na wielkość czy lokalizację danej firmy" [*Cyberprzestępczość na 3. miejscu…* 2013]. W związku z tym na całym świecie wydawane są coraz większe pieniądze, aby zapewnić odpowiednią ochronę systemom teleinformatycznym. Według prognoz firmy Gartner w 2016 r. będzie to już 86 mld dolarów [*Cyberprzestępczość na 3. miejscu…* 2013]. Pojawiają się też coraz liczniejsze głosy o potrzebie włączenia się decydentów w walkę z atakami w sieci i holistycznego podejścia do tego problemu. Zdaniem ekspertów Deloitte regulacje, jak choćby przyjęta 4 lipca 2013 r. przez Parlament Europejski propozycja nowej dyrektywy mającej pomóc w zwalczaniu cyberprzestępczości, są godną odnotowania, choć niewystarczającą inicjatywą. Zwraca uwagę brak spójności pomiędzy podejmowanymi na tym polu działaniami.

3. Istota wprowadzenia stanów nadzwyczajnych a cyberzagrożenie

Zgodnie z Konstytucją RP z 1997 r. wprowadzenie stanów nadzwyczajnych jest dopuszczalne w sytuacjach wskazanych w art. 228 ust. 1, mianowicie w warunkach „szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające". Zgodnie natomiast z ust. 5 tego artykułu czynności organu wprowadzającego stan nadzwyczajny „muszą odpowiadać stopniowi zagrożenia i powinny zmierzać do jak najszybszego przywrócenia normalnego funkcjonowania państwa".

Jak wskazują K. Prokop [2005, s. 17 i nast.] oraz T. Bryk [2011, s. 224], z art. 228 Konstytucji wysnuć można wniosek, że wszystkie stany nadzwyczajne charakteryzować się muszą następującymi zasadami: wyjątkowości, legalności, proporcjonalności, celowości, ochrony podstaw systemu prawnego i ochrony organów przedstawicielskich. Zasady te są wspólnymi elementami stanów nadzwyczajnych. T. Bryk [2011, s. 225] precyzuje, iż „zasada wyjątkowości polega na tym, że stan wyjątkowy wprowadzić można wyłącznie w przypadku szczególnego zagrożenia, gdy inne środki nie wystarczają. Z kolei zasada legalności wynika z tego, że stan nadzwyczajny wprowadzony może zostać tylko na podstawie ustawy w formie rozporządzenia, które podane zostaje do publicznej wiadomości. Z faktu, że działania podejmowane podczas stanu nadzwyczajnego powinny odpowiadać istniejącym zagrożeniom, wynika zasada proporcjonalności. Zasada celowości zakłada, że działania podjęte w czasie jego trwania, zmierzać powinny do jak najszybszego przywrócenia normalnego działania państwa". Z zasady ochrony podstaw systemu prawnego wynika zakaz zmieniania podczas stanu nadzwyczajnego m.in. Konstytucji czy samej ustawy o stanach nadzwyczajnych.

Należy również zaznaczyć, że wydanie rozporządzenia prezydenta RP i Rady Ministrów o wprowadzeniu danego rodzaju stanu nadzwyczajnego uzależnione jest zawsze od oceny stopnia zagrożenia bezpieczeństwa państwa. Trudno jest bowiem jednoznacznie wskazać, na czym polega szczególne zagrożenie w cyberprzestrzeni i jakie działania w tejże powinny niezwłocznie skutkować wprowadzeniem stanu nadzwyczajnego. Ponadto cyberprzestrzeń powinna podlegać ciągłemu monitorowaniu. Mimo tych wątpliwości objęcie bezpieczeństwa w cyberprzestrzeni szczególną ustawową ochroną i powiązanie go z bezpieczeństwem narodowym jest w pełni uzasadnione, jednakże wymaga doprecyzowania.

4. Bezpieczeństwo finansowe

4.1. Bezpieczeństwo

Bezpieczeństwo w doktrynie definiowano na wiele sposobów. Jak wskazuje S. Koziej [2012, s. 20], „najczęściej bezpieczeństwo definiuje się zarówno jako stan (osiągnięte poczucie bezpieczeństwa danego podmiotu), jak i proces (zapewnienie poczucia bezpieczeństwa podmiotu). Bardziej praktyczne jest podejście drugie. W tym sensie bezpieczeństwo danego podmiotu to ta dziedzina jego aktywności, której treścią jest zapewnienie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystanie szans (okoliczności sprzyjających), stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów. Podmiotem bezpieczeństwa mogą być pojedyncze osoby, różne grupy społeczne, narody, społeczności międzynarodowe". W. Fehler i I.T. Dziubek [2010, s. 9] z kolei podkreślają, że „bezpieczeństwo, chociaż rozmaicie określane i rozumiane, jest zawsze umieszczane na czołowym miejscu listy wartości pożądanych i chronionych tak przez jednostki, jak i podmioty zbiorowe. Kwestia uzyskania i utrzymania optymalnego w danych warunkach stanu bezpieczeństwa stanowi w związku z tym jeden z zasadniczych celów ludzkiego działania. Wiadomo jednocześnie, że bezpieczeństwo absolutne i powszechne może mieć tylko charakter ideału wyobrażonego i pożądanego, lecz w praktyce jest nieosiągalne. Bezpieczeństwo stanowi pewien oczekiwany stan, ale i ciągle trwający proces, a jego poziom i perspektywa utrzymania podlegają stałym dynamicznym przeobrażeniom stosownie do występujących zmian jego uwarunkowań. Bezpieczeństwo nie jest zatem wartością stałą i niezmienną, dlatego też jednym z ważniejszych elementów działań w zakresie uzyskiwania odpowiedniego poziomu zaspokojenia potrzeby bezpieczeństwa na poziomie państwowym jest systematyczne obserwowanie, diagnozowanie i modyfikowanie uwarunkowań i instrumentów służących do jego optymalizacji".

Wśród różnych rodzajów bezpieczeństwa jako podstawowe wymienia się dwa – bezpieczeństwo zewnętrzne i bezpieczeństwo wewnętrzne. W następnych punktach skupiono się na aspekcie wewnętrznym bezpieczeństwa oraz na bezpieczeństwie finansowym.

4.2. Bezpieczeństwo wewnętrzne

W ekspertyzie dotyczącej bezpieczeństwa wewnętrznego Polski do 2020 r. cytowani wyżej autorzy W. Fehler i I.T. Dziubek wskazali, że w wyniku prze-

prowadzonej analizy nie stwierdzono poprawnego i spójnego zdefiniowania tego pojęcia w aktach prawnych i dokumentach strategicznych [Fehler i Dziubek 2012, s. 11–12]. W związku z tym zaproponowali oni wypracowanie uniwersalnej definicji bezpieczeństwa wewnętrznego. Autorzy ekspertyzy stwierdzili, że pojęcie bezpieczeństwa wewnętrznego państwa jest powszechnie używane zarówno w języku potocznym, jak i w terminologii fachowej, ale bardzo rzadko podejmuje się próby jego definiowania czy odpowiedniego opisu. Pojęciem bezpieczeństwa posługuje się polski ustawodawca w art. 135 Konstytucji, gdzie mowa jest o Radzie Bezpieczeństwa Narodowego jako o organie doradczym prezydenta w zakresie bezpieczeństwa wewnętrznego i zewnętrznego. Z kolei art. 146 ust. 4 pkt 7 Konstytucji stanowi o tym, że Rada Ministrów zapewnia bezpieczeństwo wewnętrzne państwa i porządek publiczny. W art. 230 natomiast pojęcie to nie pojawia się wprost, ale wymienione są w kontekście ochrony przed zagrożeniami jego istotne składniki (takie jak ustrój państwa, bezpieczeństwo obywateli, porządek publiczny). Pojęcia bezpieczeństwa wewnętrznego użyto też w Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu[7], które są agencjami właściwymi w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. W związku z brakiem jednoznacznego rozumienia tego pojęcia W. Fehler i I.T. Dziubek [2012, s. 18] stworzyli następującą definicję: „bezpieczeństwo wewnętrzne państwa to taki zakotwiczony w porządku ustrojowym stan stosunków i procesów wewnątrz państwa, który zapewniając skuteczną i harmonijną realizację interesów państwa i jego obywateli, jednocześnie tworzy potencjał zdolności do sprawnego diagnozowania i reagowania w przypadkach pojawiających się zagrożeń godzących w te interesy".

4.3. Stabilność finansów w sieci

W 2012 r. CERT Polska opublikowało analizę incydentów naruszających bezpieczeństwo teleinformatyczne. Z raportu wynika m.in., że systematycznie rośnie liczba incydentów polegających na tworzeniu stron „podszywających się" pod strony banków, jak i incydentów związanych ze złośliwym oprogramowaniem potrafiącym modyfikować zawartość stron bankowych odwiedzanych przez użytkownika [*Raport 2012 CERT Polska*… 2013]. Można z tego wysnuć jednoznaczny wniosek, że bezpieczeństwo finansowe obywateli jest zagrożone.

[7] „Art. 1. Tworzy się Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej »ABW«, właściwą w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Art. 2. Tworzy się Agencję Wywiadu, zwaną dalej »AW«, właściwą w sprawach ochrony bezpieczeństwa zewnętrznego państwa" [Ustawa z dnia 24 maja 2002 r. …].

W systemie prawa stanowionego nie sposób znaleźć bezpośredniej definicji bezpieczeństwa finansowego. Można ją natomiast wywieść z różnego rodzaju materiałów wskazujących, co należy rozumieć pod tym pojęciem.

Powszechnie uważa się, że stan stabilności systemu finansowego należy uznać za dobro publiczne. W literaturze przedmiotu to „brak zagrożenia wystąpienia kryzysu jest najkrótszą definicją stabilności finansowej. Wspieranie i ochrona stabilności systemu finansowego jest zadaniem złożonym. Polega ono na zdolności do zapobiegania sytuacjom kryzysowym oraz do zarządzania kryzysem, jeżeli do niego dojdzie. Dlatego szczególne zadania związane z realizacją tej funkcji skupiają się w gestii specjalnych instytucji, które tworzą tzw. siatki bezpieczeństwa finansowego (*safety net*). Banki centralne są jednym z filarów systemu bezpieczeństwa finansowego. Inne urzędy publiczne, takie jak instytucje nadzoru finansowego, fundusze gwarantowania depozytów czy wreszcie rząd, dzielą z bankiem centralnym tę odpowiedzialność" [Szczepańska, Sotomska-Krzysztofik i Pawliszyn 2004, s. 8].

Jak wskazuje P. Zapadka [2010, s. 159], „funkcjonujący w Unii Europejskiej model sieci bezpieczeństwa finansowego (*safety net*) wyrażony jest dwojako. Po pierwsze, w formie przyjętych przez państwa członkowskie planów/koncepcji wspólnych działań. Po drugie zaś, wspólnotowe *safety net* wynika z szeroko rozumianego systemu normatywnego Unii Europejskiej (*acquis communautaire*), który przewiduje określone rozwiązania odnośnie do wspólnotowego *utilitas*, jakim jest zapewnienie bezpieczeństwa funkcjonowania rynku usług finansowych". Jednym z komponentów systemu *safety net* jest nadzór ostrożnościowy, który obejmuje m.in. zasady i instrumenty techniczne nadzoru. Dyrektywy unijne nie wskazują jednakże jednoznacznych instrukcji, co organy nadzoru powinny czynić, aby realizować *safety net* – pozostawiono to ustawodawstwom krajowym. Nie istnieje więc jedna kompleksowa regulacja prawa unijnego, która normowałaby zasady funkcjonowania *safety net* w skali Unii Europejskiej. *Safety net* według P. Zapadki [2010, s. 168–169] „jest to system zintegrowanych działań instytucji odpowiedzialnych za pewne obszary stabilności finansowej zarówno w skali »mikro«, jak i »makro«, funkcjonuje przede wszystkim w wymiarze krajowym (na podstawie regulacji prawa krajowego)".

Traktując w uproszczeniu bezpieczeństwo finansowe jako tożsame z pojęciem stabilności systemu finansowego w państwie, można uznać, że idea *safety net* powinna dotyczyć również ochrony bezpieczeństwa finansowego (stabilności finansowej) w cyberprzestrzeni. Łatwo bowiem wyobrazić sobie różne rodzaje cyberataków i podać przykłady cyberprzestępstw, które mogą stanowić tu poważne zagrożenie. W tym miejscu podkreślić należy, że jako jednego z adresatów *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* (na s. 8 dokumentu) wskazano Komisję Nadzoru Finansowego.

W tym kontekście warto przytoczyć słowa członka Stowarzyszenia ds. Bezpieczeństwa Systemów Informacyjnych ISSA Polska A. Danieluka, który na pytanie, czy techniczne problemy systemów są jedynym słabym ogniwem w polityce bezpieczeństwa instytucji finansowych, odpowiedział: „potencjalnym źródłem wycieku informacji są ludzie. Świadome lub nieświadome działanie pracowników może stanowić zagrożenie. Wiele zależy od tego, co strona dążąca do wycieku informacji pragnie uzyskać. Bardzo poważnie jest traktowana kontrola poziomu dostępu konkretnych pracowników do pewnych informacji. Wbrew krążącym opiniom pracownik jest ryzykiem, które da się kontrolować" [Raciniewska 2013].

Należy zaznaczyć ponadto, że istnieją problemy z jasnym i spójnym zdefiniowaniem terminu „cyberterroryzm". Co więcej, czasami trudno jednoznacznie zakwalifikować konkretne cyberataki jako ataki o charakterze terrorystycznym. Ich spektakularnym przykładem były natomiast cyberataki na infrastrukturę teleinformatyczną Estonii w 2007 r., które doprowadziły m.in. do blokady dostępu obywateli do systemu bankowego.

5. Wnioski

Konkludując, najlepiej posłużyć się słowami przytoczonej już Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r.: „systemy informatyczne stanowią podstawowy element relacji politycznych, społecznych i gospodarczych. Zależność społeczeństwa od tego typu systemów jest bardzo wysoka i stale rośnie. Zapewnianie odpowiedniego poziomu ochrony systemów informatycznych powinno być realizowane w ramach ogółu skutecznych i kompleksowych środków profilaktycznych, jakie towarzyszą działaniom wobec cyberprzestępczości podejmowanym w obszarze prawa karnego. Zarówno na obszarze Unii, jak i globalnie rośnie zagrożenie atakami na systemy informatyczne, a zwłaszcza atakami dokonywanymi w ramach przestępczości zorganizowanej; narastają również obawy o możliwość ataków o charakterze terrorystycznym lub mających podłoże polityczne, ukierunkowanych na systemy informatyczne stanowiące element infrastruktury krytycznej państw członkowskich i Unii. Istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych i ponawianych ataków na wielką skalę dokonywanych na systemy informatyczne, które często mają zasadnicze znaczenie dla państw członkowskich lub poszczególnych funkcji w sektorze publicznym lub prywatnym. Tendencja ta występuje wraz z opracowywaniem coraz bardziej wyrafinowanych metod". Z tego względu niezmiernie ważne było wprowadzenie do prawa polskiego, w tym do ustaw regulujących stany nadzwyczajne, pojęcia cyberprzestępczości, która stanowi we współczesnym świecie bardzo realne zagrożenie.

W związku z powyższym konieczne wydaje się wprowadzenie bardziej jednolitych, a co najważniejsze – możliwie najskuteczniejszych rozwiązań prawnych oraz organizacyjnych, które zwiększą poziom cyberbezpieczeństwa. Regulacje te powinny być nieodłącznie związane z obowiązkiem raportowania wykrytych incydentów oraz stałym nadzorem cyberprzestrzeni przed możliwymi cyberatakami. Jest to istotne także z punktu widzenia bezpieczeństwa i stabilności systemu finansowego, który w obecnych czasach w dużej mierze funkcjonuje w cyberprzestrzeni.

Literatura

Bryk T. [2011], *Przegląd regulacji stanów nadzwyczajnych w przepisach Konstytucji RP*, „Przegląd Prawa Konstytucyjnego", nr 1.

Burdea G., Coiffet P. [2003], *Virtual Reality Technology*, Wiley, New Jersey.

Cyberprzestępczość [2014], http://www.policja.pl/portal/pol/1218/2960/Cyberprzestepczosc.html (dostęp: 8.07.2014).

Cyberprzestępczość na 3. miejscu wśród globalnych zagrożeń dla biznesu [2013], http://www.deloitte.com/view/pl_PL/pl/dla-prasy/eafd72df16d40410VgnVCM1000003256f70aRCRD.htm (dostęp: 5.08.2013).

Fehler W., Dziubek I.T. [2010], *Bezpieczeństwo wewnętrzne państwa. Ekspertyza przygotowana na zlecenie Ministerstwa Rozwoju Regionalnego*, Narodowa Strategia Spójności, Warszawa.

Grzelak M., Liedel K. [2012], *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe", nr 22.

Koziej S. [2012], *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe", nr 18.

Program sztokholmski. Otwarta i bezpieczna Europa dla dobra i ochrony obywateli [2010], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010XG0504(01):PL:NOT (dostęp: 25.05.2014).

Prokop K. [2005], *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej*, Temida 2, Białystok.

Przedstawiony przez Prezydenta Rzeczypospolitej Polskiej projekt ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw z dnia 10 czerwca 2011 r., druk sejmowy nr 4355.

Raciniewska A. [2013], *Cyberprzestępczość, czyli jak banki dbają o bezpieczeństwo swoich klientów. Rozmowa z Adamem Danielukiem ze Stowarzyszenia ISSA*, http://wgospodarce.pl/opinie/5849-cyberprzestepczosc-czyli-jak-banki-dbaja-o-bezpieczenstwo-swoich-klientow (dostęp: 5.08.2013).

Raport 2012 CERT Polska: Analiza incydentów naruszających bezpieczeństwo teleinformatyczne [2013], NASK, Warszawa.

Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016 [2010], http://bip.msw.gov.pl/bip/programy/19057,dok.html (dostęp: 8.07.2014).

Schmitt M.N. [2012], *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, „Harvard International Law Journal", vol. 54.

Stepaniuk K. [2011], *Wirtualne zwiedzanie w opinii internautów w Polsce*, „Economy and Management", nr 3.
Schmitt M.N. [2013], *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge.
Szczepańska O., Sotomska-Krzysztofik P., Pawliszyn M. [2004], *Banki centralne wobec kryzysów w systemie bankowym*, Materiały i Studia, nr 179, NBP, Warszawa.
Szpunar M. [2004], *Społeczności wirtualne jako nowy typ społeczności – eksplikacja socjologiczna*, „Studia Socjologiczne", nr 2 (173).
Zapadka P. [2010], *Gwarancje bezpieczeństwa finansowego w prawie unijnym* [w:] *Konstytucja gospodarcza Unii Europejskiej. Aksjologia*, red. A. Nowak-Far, C.H. Beck, Warszawa.
Zwalczaj cyberprzestępczość [2014], http://www.policja.pl/portal/pol/1350/83643/Zwalczaj_cyberprzestepczosc.html (dostęp: 8.07.2014).

Akty normatywne

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW, Dz.Urz. UE, L218/8 z dnia 14 sierpnia 2013 r.
Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U., nr 78, poz. 483, z późn. zm.
Ustawa z dnia 6 czerwca 1997 r. „Kodeks karny", Dz.U., nr 88, poz. 553, z późn. zm.
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2002 r., nr 101, poz. 926, z późn. zm.
Ustawa z dnia 29 sierpnia 1997 r. „Prawo bankowe", Dz.U. z 2012 r., poz. 1376.
Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych, Dz.U., nr 128, poz. 1402.
Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz.U., nr 62, poz. 558, z późn. zm.
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, Dz.U. z 2010 r., nr 74, poz. 676, z późn. zm.
Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U., nr 113, poz. 985, z późn. zm.
Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U., nr 156, poz. 1301, z późn. zm.
Ustawą z dnia 18 marca 2004 r. o zmianie ustawy „Kodeks karny", ustawy „Kodeks postępowania karnego" oraz ustawy „Kodeks wykroczeń", Dz.U., nr 69, poz. 626.
Ustawa z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne", Dz.U., nr 171, poz. 1800, z późn. zm.
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U., nr 64, poz. 565, z późn. zm.
Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, Dz.U., nr 104, poz. 709, z późn. zm.
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U., nr 89, poz. 590.
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U., nr 182, poz. 1228, z późn. zm.
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.

The Threat of Cyberspace Activity to Public Order and Safety as a Condition for the Introduction of Emergency States with a Particular Emphasis on Financial Security

This paper outlines issues related to the possibility of introducing one of the states of emergency specified by the Polish Constitution in response to cyber activity and cyber attacks that threaten public safety and security. To examine the issue, the definition of cyberspace is analysed. The author also highlights the danger of the cyberspace threat in today's globalised world. In this context, both national and international regulations are discussed. The paper also focuses on the concept of financial security in the country. Because the term "financial security" is not defined explicitly in either the Constitution or subordinate legislation, an attempt is made to produce an appropriate definition. Cyber operations and cyber attacks that may cause a direct threat to a country's financial system, ultimately posing a threat to the financial security of citizens, are of particular interest.

Keywords: cyber attack, security, regulation, public order finance.