Andrzej Pieczywok*

Polityczno-prawne strategie i dyrektywy przeciwdziałania cyberzagrożeniom

Streszczenie

Treść artykułu wskazuje na istotny obszar bezpieczeństwa człowieka, dotyczy bowiem cyberprzestrzeni. Cyberprzestrzeń to środowisko wymiany informacji za pomocą sieci i systemów komputerowych. Obszar ten jest narażony na wiele różnych zagrożeń, takich, jak: cyberkryzysy i cyberkonflikty, cyberprzemoc, cyberprotesty czy cyberdemonstracje, w tym także groźba wywołania cyberwojny. Dlatego też jedną z form przeciwdziałania cyberzagrożeniom są polityczno-prawne strategie i dyrektywy zarówno unijne, jak i polskie. Artykuł składa się z czterech części: wstępu, charakterystyki najważniejszych zagrożeń w cyberprzestrzeni, unijnych i krajowych możliwości prawnych w zakresie przeciwdziałania zagrożeniom oraz zakończenia.

Słowa kluczowe: cyberzagrożenia, polityczno-prawne aspekty, strategie, dyrektywy

* Dr hab. Andrzej Pieczywok, prof. uczelni, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

Wstęp

W obliczu globalizacji bezpieczeństwo cyberprzestrzeni stało się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. Ostatnie lata były naznaczone pandemią oraz wciąż trwającą wojną w Ukrainie, a w ich konsekwencji znacznym wzrostem zagrożeń i cyberzagrożeń.

Pojęcia „bezpieczeństwo"[1] i „cyberprzestrzeń"[2] są zaliczane do kategorii określeń niezwykle ważnych w przestrzeni funkcjonowania człowieka i często pojawiają się w teorii oraz w języku potocznym. Bezpieczeństwo jest rozumiane jako stan braku zagrożenia, ale też zagrożenie i proces kształtowania oraz umacniania tego stanu. Jest też procesem, który daje poczucie pewności, i gwarantuje szanse swobodnego rozwoju. Cyberprzestrzeń to przestrzeń komunikacyjna otwarta przez połączenie wszystkich komputerów za pośrednictwem internetu. Obejmuje obszary publiczne (blog) i prywatne (wiadomości, firmowy intranet itp.). Cechą cyberprzestrzeni jest zniesienie odległości i granic państwowych.

Najbardziej znana i powszechnie cytowana definicja cyberprzestrzeni została sformułowana przez Departament Obrony Stanów Zjednoczonych na potrzeby opracowania jednolitego słownika terminologii wojskowej. Zgodnie z nią cyberprzestrzeń to globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory i kontrolery[3]. W polskojęzycznej literaturze przedmiotu istnieje wiele definicji tego pojęcia. Według Ryszarda Tadeusiewicza cyberprzestrzenią jest ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia,

1 Zob.: A. Pieczywok, *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018, s. 13; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018, s. 7; J. Gierszewski, A. Pieczywok, *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9, s. 10–17; A. Pieczywok, *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021, s. 20–21.

2 Zob.: M. Górka, *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017, s. 20; A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, nr 2, s. 62.

3 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 227.

przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do zdobywania i pogłębiania wiedzy oraz do komunikacji z innymi ludźmi[4]. Warto nadmienić, że w definicji tej równocześnie podkreśla się, że najważniejszym, chociaż nie jedynym, składnikiem cyberprzestrzeni jest obecnie internet. Przytoczona definicja jest dwuaspektowa, na co wskazują Jakub Rzucidło i Justyna Węgrzyn[5], ponieważ ujmuje cyberprzestrzeń nie tylko jako pewną infrastrukturę techniczną, lecz także jako obszar relacji ludzi z tą infrastrukturą i interakcje między ludźmi związane z jej wykorzystaniem. Często w wyniku tych interakcji pojawiają się cyberzagrożenia.

Cyberprzestrzeń i cyberzagrożenia odnoszą się do obszaru wiedzy związanej z cyberbezpieczeństwem[6], które polega na ochronie systemów komputerowych przed złośliwymi atakami lub szpiegostwem. Obejmuje wszystkie techniki i narzędzia stosowane w celu ochrony infrastruktury, ale także poufności, integralności i dostępności danych, które są przechowywane lub wymieniane w cyfrowym świecie.

Należy stwierdzić, że ostatnio lawinowo rośnie liczba przestępstw internetowych, których ofiarami stają się zwykli obywatele, a mimo to w latach 2019–2021 krajowy system cyberbezpieczeństwa pomijał tę najliczniejszą grupę użytkowników sieci, i koncentrował się na wzmocnieniu ochrony instytucji i przedsiębiorstw uznawanych za kluczowe dla funkcjonowania państwa.

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

5 J. Rzucidło, J. Węgrzyn, *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego" 2015, nr 5, s. 142.

6 Na temat cyberbezpieczeństwa zob. także: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, nr 2; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, nr 3; M. Karpiuk, *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, nr 1; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, nr 2; M. Karpiuk, *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, nr 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, nr 2; M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, nr 2; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, nr 2; M. Karpiuk, *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, nr 3; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, nr 1.

Najważniejsze zagrożenia w cyberprzestrzeni

Najbardziej uciążliwym zagrożeniem w cyberprzestrzeni są cyberataki i cyberprzestępczość. Stają się one w całej Europie coraz bardziej wyrafinowane. Można uznać, że tendencja ta będzie się w przyszłości nasilać. Według prognoz w 2025 rok aż 41 mld urządzeń będzie na całym świecie podłączonych do internetu. Cyberataki przeprowadzane przez państwa są szczególnie niebezpieczne, dlatego że ich celem jest osłabienie lub zniszczenie infrastruktury transportowej w celach politycznych lub militarnych. Firmy muszą coraz bardziej kompleksowo zabezpieczać się przed atakami hakerskimi. Według badania przeprowadzonego przez Cybersecurity Ventures cyberprzestępczość kosztuje każdego roku na całym świecie ponad 6 bln dolarów – więcej niż jakakolwiek inna przyczyna przed nią.

W dzisiejszych czasach cyberzagrożenia stają się coraz poważniejszym problemem dla firm. Ataki hakerów i wirusy to tylko niektóre z zagrożeń, z którymi muszą zmagać się np. przedsiębiorstwa.

Innym zagrożeniem jest ransomware, czyli rodzaj ataku, podczas którego cyberprzestępcy zaszyfrowują dane w systemach informatycznych i żądają okupu za ich odblokowanie. Phishing to zagrożenie polegające na wyłudzaniu poufnych informacji poprzez podszywanie się pod wiarygodne instytucje.

Wolna, otwarta i bezpieczna cyberprzestrzeń jest istotnym elementem gospodarki kraju, aktywności społecznej, demokracji i bezpieczeństwa narodowego. Dane osobowe, gospodarka czy usługi publiczne są w coraz większym stopniu zdigitalizowane. Jednakże wrażliwe systemy komputerowe mogą być przedmiotem złośliwych ataków. Polska stoi w obliczu zagrożeń cyberbezpieczeństwa związanych zarówno z podmiotami państwowymi, jak i niepaństwowymi. Ochrona kraju i jej infrastruktury cybernetycznej przed złośliwymi podmiotami jest poważnym wyzwaniem i ciągłą działalnością.

Od 2020 roku obserwujemy wzrost ataków phishingowych nakierowanych na złamanie tego zabezpieczenia. Stale rosnąca cyberprzestępczość pokazuje jak trudno jest wypełnić liczne luki w zabezpieczeniach, które są wspólne dla prawie wszystkich systemów.

Ponadto nie można zapominać, że podatność infrastruktury krytycznej na ataki cybernetyczne pozostanie istotnym problemem nawet wtedy, kiedy można byłoby (prawie) wykluczyć zagrożenie terrorystyczne. Państwa nie tylko uświadomiły sobie swoje słabe punkty, lecz także możliwości, jakie otwiera przed nimi cyberprzestrzeń w realizacji celów polityki bezpieczeństwa i obrony.

Obecnie poczta elektroniczna jest najczęstszym celem ataków, szczególnie dla cyberprzestępców chcących szybko zarobić pieniądze, preferujących prostsze techniki, jak phishing. Wyspecjalizowani cyberprzestępcy odpowiedzialni za zagrożenia zawsze starają się wyprzedzać trendy w zakresie możliwości przeprowadzania ataków. Obecnie istnieje ryzyko, że bezpieczeństwo druku będzie nadal pomijanym elementem ogólnych działań na rzecz cyberbezpieczeństwa. Jednocześnie wraz z większą liczbą drukarek podłączonych do sieci korporacyjnych z powodu pracy hybrydowej ryzyko ataku wzrasta.

Kolejny problem to niedofinansowanie. Mimo potrzeb poszczególne jednostki policji rezygnowały z zakupów sprzętu i oprogramowania, a także z inwestycji czy z organizacji szkoleń z dziedziny cyberbezpieczeństwa. Na to nakładały się jeszcze problemy strukturalne i organizacyjne – wydziały do walki z cyberprzestępczością podlegały komendantom wojewódzkim (w przypadku Warszawy – komendantowi stołecznemu) i były w praktyce niezależne od Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. W reakcji na te problemy w KGP powstał pomysł utworzenia nowej jednostki – Centralnego Biura Zwalczania Cyberprzestępczości (CBZC), która ma zintegrować wydziały terenowe i zatrudnić do końca 2025 roku 1,8 tys. odpowiedniej klasy specjalistów. W ocenie NIK to działania celowe, ale obarczone ryzykami, które mogą negatywnie wpływać na proces formowania nowej jednostki. Izba dostrzega zwłaszcza problem z zatrudnieniem tak dużej liczby specjalistów w tak krótkim czasie.

Unijne i krajowe możliwości prawne przeciwdziałania zagrożeniom w cyberprzestrzeni

Bez wątpienia wybuch wojny w Ukrainie oraz działania rosyjskich hakerów to jeden z głównych aspektów tego, co się dzieje w cyberprzestrzeni. Phishing, ataki ransomware, w tym na infrastrukturę krytyczną, wpisały się na dobre w krajobraz nie tylko Ukrainy, lecz także polskiej rzeczywistości. Sytuacji nie sprzyja kwestia uregulowań prawnych i ogólne zamieszanie związane z implementacją unijnych przepisów oraz ich zgodność z prawem krajowym. Dostosowanie dokumentów i wdrożenie spójnej polityki cyberbezpieczeństwa okazuje się sporym wyzwaniem.

Unia Europejska w swojej historii borykała się z licznymi kryzysami i stopniowo wprowadzała zmiany polityczne i instytucjonalne, żeby lepiej radzić sobie z kolejnymi sytuacjami nadzwyczajnymi.

W ostatnich latach odnotowano w Unii Europejskiej wzrost liczby incydentów zagrażających funkcjonowaniu sieci i systemów informatycznych. Odpowiedzią prawodawcy unijnego na tego typu zajścia była dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS)[7].

Dyrektywa reguluje pięć głównych grup zadań związanych z cyberbezpieczeństwem: 1) nakłada na wszystkie państwa członkowskie obowiązek przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych; 2) tworzy grupę współpracy złożoną z przedstawicieli państw członkowskich, Komisji Europejskiej i Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA); 3) tworzy sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT); 4) ustanawia dla operatorów usług kluczowych i dostawców usług cyfrowych wymogi dotyczące bezpieczeństwa i zgłaszania incydentów; 5) wyznacza właściwe organy krajowe, w tym pojedyncze punkty kontaktowe, mające realizować zadania związane z bezpieczeństwem sieci i systemów informatycznych[8].

W 2017 roku w ramach przeglądu strategii cyberbezpieczeństwa UE zainicjowano działania do ustanowienia tzw. pakietu cyberbezpieczeństwa UE, który obejmuje zestaw działań skupiony na trzech głównych zagadnieniach: odporności, prewencji i obronie.

W grudniu 2020 roku Komisja Europejska i Europejska Służba Działań Zewnętrznych (ESDZ) przedstawiły nową unijną strategię cyberbezpieczeństwa. Ma ona zwiększyć odporność Europy na cyberzagrożenia i zapewnić wszystkim obywatelom i firmom możliwość korzystania z wiarygodnych narzędzi i usług cyfrowych. Strategia zawiera konkretne propozycje zastosowania instrumentów regulacyjnych, inwestycyjnych i politycznych. Obejmuje bezpieczeństwo podstawowych usług takich, jak: szpitale, sieci energetyczne i koleje, a także bezpieczeństwo coraz większej liczby połączonych obiektów w domach, biurach i fabrykach.

22 marca 2021 roku Rada przyjęła konkluzje w sprawie strategii cyberbezpieczeństwa, w których podkreśliła, że cyberbezpieczeństwo ma zasadnicze znaczenie dla budowania odpornej, ekologicznej i cyfrowej Europy. Unijni ministrowie za podstawowy cel obrali zapewnienie autonomii strategicznej

7 *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje*, Kraków 2019, s. 45.
8 Ibidem, s. 45–46.

z jednoczesnym zachowaniem otwartej gospodarki. Obejmuje to zwiększenie zdolności dokonywania samodzielnych wyborów w obszarze cyberbezpieczeństwa w celu wzmocnienia cyfrowego przywództwa UE i jej strategicznych zdolności.

Żeby zwiększyć odporność na przyszłe wyzwania, UE stara się usprawnić międzysektorowe i transgraniczne zarządzanie kryzysowe. Ponadto poprawia komunikację kryzysową i intensyfikuje walkę z dezinformacją. Szczególnie istotnymi obszarami w unijnych narzędziach i przepisach w dziedzinie zarządzania kryzysami i wzmacniania odporności są m.in.: mechanizm ochrony ludności, zintegrowane reagowanie na szczeblu politycznym w sytuacjach kryzysowych, gotowość i reagowanie na stany zagrożenia zdrowia, ochrona sieci i systemów informacyjnych, ochrona infrastruktury krytycznej.

W tym kontekście Rada zatwierdziła w maju 2023 roku konkluzje o cyberobronie, w których podkreśliła, że UE i jej państwa członkowskie muszą jeszcze bardziej wzmocnić swoją odporność na zagrożenia cyberbezpieczeństwa i zwiększyć wspólne cyberbezpieczeństwo i cyberobronę przed szkodliwymi zachowaniami i aktami agresji w cyberprzestrzeni.

Przykładem wdrożenia dyrektywy NIS jest polska ustawa z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Ustawa powołuje do życia działające na poziomie krajowym trzy zespoły reagowania na incydenty bezpieczeństwa komputerowego: 1) prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego – CSIRT GOV; 2) prowadzony przez Ministra Obrony Narodowej – CSIRT MON; 3) prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy – CSIRT NASK.

Ustawa określa organy właściwe do wyznaczania operatorów usług kluczowych, zasady ich wyznaczania, a także szczegółowe obowiązki operatorów, do których należą m.in.: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych uwzględniających najnowszy stan wiedzy; 3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; 6) stosowanie środków

łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwo[9].

„Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polski na lata 2017–2022" to dokument, który wpisuje się w kontynuację działań podejmowanych w przeszłości przez administrację rządową mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP, w tym przyjętą przez rząd w 2013 roku „Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej". Zarówno krajowe strategie rozwoju, jak i te odnoszące się do sfery porządku publicznego i bezpieczeństwa narodowego uzależniają swoje powodzenie od zastosowania systemów teleinformatycznych.

Zamierzeniem niniejszego dokumentu jest określenie ramowych działań mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. „Krajowe Ramy Polityki Cyberbezpieczeństwa..." są spójne z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej wykorzystujących systemy teleinformatyczne oraz uwzględniają potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej Polskiej.

Obecnie w Polsce i w Unii Europejskiej trwają prace nad ponad 50 aktami prawnymi zaliczanymi do źródeł prawa nowych technologii dotyczącymi cyberbezpieczeństwa, e-prywatności, handlu elektronicznego, innowacji, internetu, telekomunikacji, własności intelektualnej oraz zarządzania danymi.

Skuteczne zabezpieczenie cyberprzestrzeni jest jednym z priorytetów nie tylko narodowych, lecz także sojuszniczych. Coraz częstsze ataki na serwery urzędów i wojska w wielu krajach, wojna prowadzona przez Rosjan i Ukraińców w cyberprzestrzeni, groźby ataków wodza Korei Północnej na najważniejsze dla państwa oraz gospodarki amerykańskiej instytucje uświadamiają, że narodziła się kolejna płaszczyzna walki w sferze dla nas do niedawna w ogóle nieznanej.

9 Ibidem, s. 47.

Zakończenie

Oprócz polityczno-prawnych strategii i dyrektyw dotyczących przeciwdziałania cyberzagrożeniom istotną kwestią jest kształcenie i wychowywanie obywateli do odpowiedzialności – najpierw w środowisku rodzinnym, potem szkołach i placówkach opiekuńczo-wychowawczych, uczelniach, poprzez mass media, działania polityków, kulturę itp.

Dość ważną czynnością jest profilaktyka dotycząca cyberprzemocy, która powinna obejmować takie działania, jak: prowadzenie zajęć z edukacji prawnej w szkołach i placówkach dotyczących m.in. konsekwencji prawnych stosowania przemocy i cyberprzemocy; realizacja przez szkoły i placówki programów edukacyjno-terapeutycznych; doskonalenie nauczycieli i wychowawców z przeciwdziałania cyberprzemocy i rozwiązywania konfliktów; podejmowanie interwencji profilaktycznych oraz reagowanie w sytuacjach kryzysowych.

Głównym zadaniem rodziców, opiekunów i nauczycieli powinno być promowanie zdrowego stylu życia, budowanie pozytywnego kontaktu z dzieckiem, stwarzanie okazji do rozwijania zajęć eliminujących spędzanie czasu przed komputerem, wskazywanie młodemu człowiekowi konsekwencji nadmiernego korzystania z mediów cyfrowych oraz codzienna kontrola dostępu dziecka do komputera.

W kontekście rozpatrywanej problematyki przeciwdziałania cyberprzemocy powszechne powinny być wszelkie działania profilaktyczne, uświadamiające i wprowadzające odpowiednie procedury reagowania na wypadek takiego zagrożenia. Potencjałem w działalności profilaktycznej, prewencji kryminalnej, tzw. miękkiej prewencji są organizacje pozarządowe (np. stowarzyszenia)[10].

Osoby działające w tych organizacjach są specjalistami w dziedzinie bezpieczeństwa i znają występujące obecnie rodzaje zagrożeń. Poświęcają swój wolny czas, jako wolontariusze[11] przygotowują, opracowują i wdrażają programy profilaktyczne w szkołach, świetlicach środowiskowych, świetlicach osiedlowych, podczas festynów, spotkań panelowych, konferencji i innych możliwych okazji spotkania z dziećmi i młodzieżą z bezpieczeństwa w dziedzinie cyberprzestępstw i cyberzagrożeń.

10 Ustawa z 7 kwietnia 1989 r. – Prawo o stowarzyszeniach, Dz.U. 1989, nr 20, poz. 104, z późn. zm.

11 Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i wolontariacie, ibidem 2003, nr 96, poz. 873, z późn. zm.

Pierwszym miejscem, w którym indywidualni użytkownicy internetu szukają pomocy po cyberataku, jest policja. Wielu policjantów nie miało nawet podstawowej wiedzy, która umożliwiłaby sprawne przyjmowanie zgłoszeń i skuteczne zabezpieczenie materiału dowodowego. Nie stworzono też jasnych procedur ani dla zgłaszających przestępstwo użytkowników internetu, ani dla przyjmujących zgłoszenia funkcjonariuszy.

Banki, jako instytucje zaufania publicznego, powinny szczególnie zwracać uwagę na cyberbezpieczeństwo. Żeby chronić się przed zagrożeniami w tym obszarze banki spółdzielcze i zrzeszające muszą inwestować w nowoczesne systemy ochrony danych, wdrażać odpowiednie procedury bezpieczeństwa oraz stale edukować pracowników i klientów z cyberbezpieczeństwa.

Bibliografia

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, nr 2.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, nr 3.

Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, nr 2.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, nr 2.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Gierszewski J., Pieczywok A., *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018.

Górka M., *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017.

Karpiuk M., *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, nr 1.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, nr 1.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.

Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, nr 2.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, nr 2.

Karpiuk M., *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, nr 2.

Karpiuk M., *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, nr 3.

Pieczywok A., *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018.

Pieczywok A., *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021.

Pieczywok A., *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, nr 2.

Rzucidło J., Węgrzyn J., *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego" 2015, nr 5.

Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Political and legal strategies and directives for countering cyber threats

Abstract

The article indicates an important area of human security relating to cyberspace. Cyberspace is a domain where information is exchanged via computer networks and systems. This area is exposed to a variety of threats, such as cyber crises and cyber conflicts, cyber violence, cyber protests and cyber demonstrations, including the threat of cyber warfare. Therefore, political and legal strategies and directives, both EU and Polish, are a form of countering cyber threats. The article is composed of four sections: an introductory section, characteristics of the most important threats in cyberspace, EU and national legal options for countering the threats, and a concluding section.

Key words: cyber threats, political and legal aspects, strategies, directives