Teka Kom. Praw. – OL PAN, t. XI, 2018, nr 2, 101–120

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

Mariusz Czyżak

Urząd Komunikacji Elektronicznej
Polska
https://orcid.org/0000-0003-0869-3713

Streszczenie. W artykule omówiono zagadnienie bezpieczeństwa w cyberprzestrzeni. Przedstawiono pojęcia bezpieczeństwa i cyberprzestrzeni, a także wybrane kategorie zagrożeń w cyberprzestrzeni. Wskazano, że odpowiedzialność za utrzymanie właściwego poziomu cyberbezpieczeństwa spoczywać powinna na instytucjach publicznych, przedsiębiorcach i indywidualnych użytkownikach cyberprzestrzeni.

Słowa kluczowe: bezpieczeństwo, cyberprzestrzeń, cyberprzestępczość

UWAGI WSTĘPNE

Wraz z postępującym rozwojem technicznym i powszechnym wykorzystywaniem technologii teleinformatycznych w każdym niemal obszarze życia społecznego i gospodarczego, odmiennego znaczenia nabiera w ostatnich latach również pojęcie bezpieczeństwa, zwłaszcza tego jego wymiaru, który odnosi się do nowego obszaru aktywności ludzkiej zwanego cyberprzestrzenią. W dalszych rozważaniach podjęta zostanie próba nakreślenia przynajmniej niektórych aspektów bezpieczeństwa związanych z cyberprzestrzenią, rzutujących w szczególności na kształt prawnego instrumentarium służącego ochronie dóbr istotnych dla państwa i jednostki. Punktem wyjścia dla nich będą zaś zarówno poglądy doktryny nauk o bezpieczeństwie i nauk prawnych na współczesne postrzeganie pojęcia bezpieczeństwa i cyberprzestrzeni, jak i treść aktów normatywnych różnej rangi i należących do różnych gałęzi prawa, a odnoszących się do tego wymiaru bezpieczeństwa, którym jest bezpieczeństwo w cyberprzestrzeni.

I. POJĘCIE BEZPIECZEŃSTWA

Bezpieczeństwo jest pojęciem złożonym i wielowymiarowym. Definiowane jest bądź jako pewien stan, tj. poczucie bezpieczeństwa osiągnięte przez dany podmiot, bądź jako proces polegający na zapewnianiu poczucia bezpieczeństwa określonego podmiotu, odzwierciedlający rzeczywisty, dynamiczny charakter tego zjawiska. Bezpieczeństwo tego podmiotu stanowić będzie zatem wówczas taką dziedzinę jego aktywności, „której treścią jest zapewnianie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku [np. w cyberprzestrzeni – M.Cz.], w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”[1].

Na gruncie nauk o bezpieczeństwie stan ów bywa przy tym klasyfikowany m.in. na bezpieczeństwo międzynarodowe i narodowe. W ramach tego pierwszego doktryna wyodrębnia wówczas bezpieczeństwo globalne, regionalne i zbiorowe. W obrębie drugiej kategorii wyróżnia się zaś bezpieczeństwo państwa, społeczeństwa, poszczególnych grup społecznych i jednostki. Samo bezpieczeństwo narodowe składać się może z kolei z takich elementów wyodrębnionych przedmiotowo, jak bezpieczeństwo polityczne, ekonomiczne, społeczno-kulturowe, ekologiczne, militarne i inne (np. informacyjne)[2].

W polskim porządku prawnym trudno doszukać się definicji legalnej pojęcia „bezpieczeństwo narodowe”. Wspomnieć wypada jednak, że Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.[3] posługuje się pojęciem „bezpieczeństwo obywateli”, wskazując je jako jeden z elementów bezpieczeństwa, który zapewnić ma Rzeczpospolita Polska (art. 5 Konstytucji RP), „bezpieczeństwo państwa” w kontekście przesłanek wyłączenia jawności rozprawy sądowej (art. 45 ust. 2 Konstytucji RP), „bezpieczeństwo ekologiczne” – konstytuując spoczywający na władzach publicznych obowiązek ochrony środowiska i prawo do bezpieczeństwa ekologicznego (art.

[1] S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe” 18 (2) 2011, s. 20.

[2] Por. Z. Nowakowski, H. Szafran, R. Szafran, *Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw*, Politechnika Rzeszowska, Rzeszów 2009, s. 72.

[3] Dz. U. Nr 78, poz. 483 z późn. zm. [dalej cyt.: Konstytucja RP].

74 ust. 1 Konstytucji RP), a także „bezpieczeństwo wewnętrzne państwa" i „bezpieczeństwo zewnętrzne państwa" w odniesieniu do obowiązków spoczywających na Radzie Ministrów (art. 146 ust. 4 pkt 7 i 8 Konstytucji RP). Akty normatywne rangi ustawowej wskazują natomiast m.in. na bezpieczeństwo publiczne (np. wraz z pojęciem porządku publicznego w ustawie z dnia 6 kwietnia 1990 r. o Policji[4]) lub bezpieczeństwo wewnętrzne i zewnętrzne (np. jako obszary aktywności Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[5].

Dodać należy, że bezpieczeństwo narodowe jest pojęciem obejmującym zarówno bezpieczeństwo obywateli, bezpieczeństwo wewnętrzne, jak i bezpieczeństwo zewnętrzne[6]. Bezpieczeństwo wewnętrzne jest zatem kategorią bezpieczeństwa węższą znaczeniowo od pojęcia bezpieczeństwa narodowego. P. Majer wiąże, pojmowane uniwersalnie, bezpieczeństwo wewnętrzne ze „stanem niezakłóconego funkcjonowania państwa, związanym z bezpieczeństwem jego organów oraz stabilnością życia społecznego, wynikającą z bezpieczeństwa osobistego i bezpieczeństwa egzystencji jego obywateli", przy czym bezpieczeństwo organów państwa utożsamia z porządkiem konstytucyjnym lub ustrojowym, bezpieczeństwo osobiste traktuje jako następstwo dominujących w danym państwie stosunków społecznych, obowiązującego tam systemu prawnego oraz stopnia gotowości tegoż państwa do ochrony interesów (praw i wolności) jednostki, zaś za treść bezpieczeństwa egzystencji uznaje wrażliwość państwa na sprawy bytu. Złożoność zjawiska bezpieczeństwa wewnętrznego implikuje z kolei konieczność jego rozpatrywania w trzech wymiarach – instytucjonalnym (struktury organów władzy publicznej, których liczba i zakres działalności związany jest ze wzrastającymi powinnościami państwa), normatywnym (przepisy prawne regulujące sferę bezpieczeństwa wewnętrznego w ujęciu przedmiotowym i odnoszące się nie tylko do ochrony instytucji publicznych, ale tworzące również gwarancje dla bezpieczeństwa osobistego i egzystencji), a także funkcjonalnym (sposób wdrażania regulacji dotyczących bezpieczeństwa wewnętrznego przez wła-

[4] Dz. U. z 2017 r., poz. 2067 z późn. zm.
[5] Dz. U. z 2018 r., poz. 2387 z późn. zm.
[6] M. Nowiński, *Pojęcie bezpieczeństwo narodowe w prawie europejskim i międzynarodowym w kontekście uprawnień służb specjalnych*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. P. Burczaniuk, Agencja Bezpieczeństwa Wewnętrznego, Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota", Warszawa 2017, s. 11.

ściwe instytucje publiczne)[7]. Analogicznie, węższe znaczenie ma również pojęcie bezpieczeństwa zewnętrznego, które powiązane jest z odpornością na zagrożenia zlokalizowane poza tymże państwem.

II. ISTOTA CYBERPRZESTRZENI I CYBERBEZPIECZEŃSTWA

Do jakiej kategorii bezpieczeństwa należałoby zaliczyć bezpieczeństwo cyberprzestrzeni? Dla podjęcia próby nakreślenia jego istoty wypada pokrótce przypomnieć znaczenie samej cyberprzestrzeni. Na gruncie doktryny nauk prawnych, nauk o bezpieczeństwie, czy też nauk o zarządzaniu, a na samym początku literatury, wypracowano szereg różnorodnych definicji pojęcia „cyberprzestrzeń", stąd też nie sposób byłoby przywołać ich wszystkich. Niemniej wspomnieć trzeba, że W. Gibson w powieści *Neuromancer* posłużył się jako jeden z pierwszych, opisem następującym: „To jest cyberprzestrzeń, konsensualna, halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność"[8]. Dodatkowo, dla porządku przedmiotowych rozważań przypomnieć należy przynajmniej kilka spośród definicji cyberprzestrzeni: „Globalna domena środowiska informacyjnego składająca się z 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 oraz kontrolery"; „Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata"; „Cyberprzestrzeń jest wirtualną przestrzenią wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej. Fundament cyberprzestrzeni stanowi Internet jako uniwersalna oraz powszechnie dostępna sieć oferująca połączenia oraz transport, która może być uzupełniania oraz rozszerzana dalej przez dowolną ilość dodatkowych sieci danych. Systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni"[9].

---

[7] P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 7 (2012), s. 16–17.

[8] Zob. W. Gibson, *Neuromancer*, Wydawnictwo Książnica, Katowice 2009, s. 59.

[9] Cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 9 (2013), s. 227–230.

Próbę zdefiniowania pojęcia cyberprzestrzeni podjął również polski ustawodawca na gruncie prawodawstwa dotyczącego stanów nadzwyczajnych, a także organy władzy publicznej w obrębie dokumentów o charakterze planistycznym i strategicznym. W „Krajowych ramach polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”[10] cyberprzestrzeń zdefiniowana została, na wzór definicji legalnych zawartych w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[11], ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym[12], jak również ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[13], jako „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”[14].

Cyberprzestrzeń ma postać przestrzeni wirtualnej, która służy komunikowaniu się, a nie zmaterializowanej wyodrębnionej przestrzeni fizycznej, ale pamiętać trzeba przy tym, że jej byt jako obszaru wymiany informacji uzależniony jest od istnienia urządzeń technicznych natury fizycznej, zlokalizowanych na terytorium określonego państwa, przynależnych niekiedy nawet do określonych instytucji publicznych. Dlatego też nie sposób odebrać jej jednak również charakteru swego rodzaju komponentu przestrzeni państwa, gdzie państwo to pełni swoje funkcje, jeśli cyberprzestrzeń tworzą systemy teleinformatyczne podlegające jurysdykcji tegoż państwa ze względu na rozmieszczenie na jego terytorium lub fakt, że pozostają w dyspozycji organów władzy do niego przynależnych[15].

---

[10] Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 [dalej cyt.: Krajowe ramy polityki cyberbezpieczeństwa].

[11] Dz. U. z 2017 r., poz. 1932 z późn. zm.

[12] Dz. U. z 2017 r., poz. 1928 z późn. zm.

[13] Dz. U. z 2017 r., poz. 1897 z późn. zm.

[14] W rozumieniu art. 2 ust. 1b ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, analogicznie brzmiącym art. 2 ust. 1b ustawy o stanie wyjątkowym, jak również art. 3 pkt 4 ustawy o stanie klęski żywiołowej, cyberprzestrzeń to „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”.

[15] M. Czyżak, *Prawna ochrona cyberprzestrzeni państwa*, „Horyzonty Bezpieczeństwa” 8 (2017), s. 7, 9.

Wspomniane już Krajowe ramy polityki cyberbezpieczeństwa posługują się takimi równoznacznymi pojęciami odnoszącymi się do materii bezpieczeństwa w cyberprzestrzeni, jak „bezpieczeństwo sieci i systemów teleinformatycznych", „cyberbezpieczeństwo" i „bezpieczeństwo teleinformatyczne". Uznają je za pewien stan, tj. „odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne" (Krajowe ramy cyberbezpieczeństwa, pkt 11 ppkt 3). Dodać wypada, że wskazano tam również wyraźnie, iż „W cyberprzestrzeni tworzymy i kształtujemy relacje społeczne, a Internet stał się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej. Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni, czy to o charakterze globalnym, czy lokalnym, będzie miało wpływ na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe" (Krajowe ramy cyberbezpieczeństwa, pkt 1). Założono przy tym, iż „W roku 2022 Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni. Dzięki synergii działań wewnętrznych i międzynarodowych cyberprzestrzeń RP stanowić będzie bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli" (Krajowe ramy cyberbezpieczeństwa, pkt 4.1.).

Definicji cyberbezpieczeństwa, analogicznej do przywołanej powyżej, doszukać można się także na gruncie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[16]. Ustawa ta wdrożyła ma do polskiego porządku prawnego dyrektywę 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[17]. Cyberbezpieczeństwo określa wspomniana ustawa jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związa-

[16] Dz. U. z 2018 r., poz. 1560 [dalej cyt.: u.k.s.c.]
[17] Dz. Urz. UE L 194 z 19.07.2016, s. 1.

nych z nimi usług oferowanych przez te systemy" (art. 2 pkt 4 u.k.s.c.). Celem krajowego systemu cyberbezpieczeństwa ma zaś być „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów" (art. 3 u.k.s.c.).

W „Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej" opracowanej przez Biuro Bezpieczeństwa Narodowego i wprowadzonej w dniu 22 stycznia 2015 r.[18] posłużono się z kolei pojęciem „cyberbezpieczeństwa RP (bezpieczeństwa RP w cyberprzestrzeni)", rozumianym jako „proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni" (Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, s. 7–8), jak również odrębnie „bezpieczeństwa cyberprzestrzeni RP", za które uznano „część cyberbezpieczeństwa państwa, obejmującą zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych" (Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, s. 8).

Jeżeli cyberprzestrzeń wymyka się dotychczasowemu, klasycznemu postrzeganiu określonego wyodrębnionego fizycznie wymiaru przestrzeni, to problem z dookreśleniem odnosi się i do samego stanu bezpieczeństwa w cyberprzestrzeni oraz narzędzi, które służą jego zapewnieniu. Charakteryzując istotę bezpieczeństwa cyberprzestrzeni J. Wasilewski wyraził następujący pogląd: „Istotę cyberprzestrzeni tworzy koncepcja powołania do życia swojego rodzaju równoległego środowiska, które jest nowym wymiarem dla ludzkich działań. […] Skoro cyberprzestrzeń jest nową domeną ludzkiej aktywności, zapewnienie należytego poziomu jej ochrony powinno w naturalny sposób być jednym z obowiązków państwa wobec obywateli. Przyjęcie określonego sposobu definiowania cyberprzestrzeni wywiera istotny wpływ na sposób określania zakresu przedmiotowego obszaru bezpieczeństwa cy-

[18] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015, w: https://www.bbn.gov.pl

berprzestrzeni. O ile zatem z definicji domeny cyfrowej wyłącza się jej użytkowników, bezpieczeństwo tak ujętej cyberprzestrzeni będzie skupiać się na zapewnieniu ochrony elementów infrastrukturalnych. Z kolei dodanie do przedmiotowej definicji relacji pomiędzy użytkownikami a podbudowującym cyberprzestrzeń sprzętem oraz relacji pomiędzy samymi użytkownikami (użytkownik – cyberprzestrzeń jako medium – użytkownik) narzuca konieczność pojmowania bezpieczeństwa tego obszaru w sposób zdecydowanie bardziej dynamiczny, zwłaszcza że jest on pełny ludzkich działań o najróżniejszych konotacjach prawnych”[19]. Ochrona bezpieczeństwa w cyberprzestrzeni obejmować musi zatem ochronę praw i wolności jednostki, ale w sposób odpowiadający wymogom wynikającym z jej wirtualnej natury.

III. ZAGROŻENIA W CYBERPRZESTRZENI

Mając na względzie rozmaite aspekty postrzegania cyberprzestrzeni stwierdzić trzeba, że przybierać może ona wymiar socjologiczny, prawny, politologiczny, techniczny, militarny, itp. Raz będzie sferą aktywności społecznej jednostki, poszczególnych grup społecznych, czy też zawodowych, ale też wspólnoty międzynarodowej i struktur państwowych. Innym razem będzie to – podlegająca ochronie prawnokarnej – płaszczyzna wymiany gospodarczej i dokonywanych w jej obrębie transakcji handlowych, środowisko informatyczne wymagające zastosowania specjalnych rozwiązań z zakresu bezpieczeństwa IT, a także element struktury państwa strzeżony przez służby ochrony bezpieczeństwa powszechnego i porządku publicznego, a nawet teatr działań wojennych podejmowanych przez siły zbrojne. Niezależnie jednak od odmiennej jej percepcji, elementem nieodłącznie towarzyszącym materii cyberprzestrzeni jest kwestia bezpieczeństwa podmiotów (jednostki, podmiotów o charakterze korporacyjnym, czy też państwa, sojuszy wojskowych lub wspólnoty międzynarodowej) w jej obrębie funkcjonujących. Różny też charakter mieć będą zagrożenia w niej występujące.

Zapewnienie bezpieczeństwa w wymiarze militarnym kojarzone jest przede wszystkim z ochroną nienaruszalności granic państwa i jego suwerenności. Niemniej cyberprzestrzeń stała się jednym z potencjalnych obszarów agresji, a w konsekwencji i teatrem działań wojennych. Stąd też, w opracowanej w Ministerstwie Obrony Narodowej „Koncepcji Obronnej Rzeczypospolitej Polskiej” z maja 2017 r., w części dotyczącej środowiska bez-

[19] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, s. 231–232.

pieczeństwa Polski, w szczególności w odniesieniu do zagrożeń i wyzwań stwierdzono wyraźnie: „Choć w przyszłości wojny będą wciąż prowadzone przede wszystkim za pomocą środków kinetycznych, znaczenie będą zyskiwać również inne metody walki. Cyberprzestrzeń oraz pole walki informacyjnej, już teraz stają się frontem nowego rodzaju, pozbawionym wielu ograniczeń (np. prawnych), a także umożliwiającym bardziej wyrównaną konkurencję państwom o zróżnicowanym potencjale militarnym. Jest to sfera, w której szczególnie łatwo będzie zatrzeć granice między stanami pokoju i wojny. Utrzymane zostanie wysokie tempo rozwoju narzędzi walki radioelektronicznej i informacyjnej. Zwiększone możliwości w dziedzinie analizy dużych zbiorów danych zrewolucjonizują zarządzanie bezpieczeństwem państwa w wielu aspektach". Jednocześnie, w części dotyczącej docelowego modelu Sił Zbrojnych RP 2032 wskazano, iż „Stałą osłonę zapewnią wojska cybernetyczne, koordynujące zabezpieczenie i walkę w cyberprzestrzeni. Wysokie tempo rozwoju narzędzi walki radioelektronicznej i informacyjnej. Zwiększone możliwości w dziedzinie analizy dużych zbiorów danych zrewolucjonizują zarządzanie bezpieczeństwem państwa w wielu aspektach"[20].

Ogromne możliwości stworzone przez rozwój nowych technologii i możliwość funkcjonowania człowieka w cyberprzestrzeni wpływają również, nie zawsze korzystnie, na zachowanie człowieka jako członka społeczeństwa. W świecie wirtualnym posiada on poczucie anonimowości, które związane jest z deindywiduacją i przekonaniem o własnej bezkarności z uwagi na trudno identyfikowalną tożsamość w cyberprzestrzeni. Niezwykle łatwy dostęp do danych i brak barier uniemożliwiających dostęp do niektórych treści może zagrażać prawidłowemu rozwojowi człowieka. Funkcjonowanie w cyberprzestrzeni w postaci dodatkowego bytu prowadzić może do pewnej dezintegracji tożsamości osoby. Ogromne możliwości komunikacyjne sprawiają, że człowiek z jednej strony zwiększa częstotliwość i liczbę kontaktów, ale pozbawione są one takiej ekspresji emocjonalnej, jaka towarzyszy osobistym kontaktom. W konsekwencji osoby odnajdujące się w świecie wirtualnym, nie zawsze radzą sobie w życiu poza cyberprzestrzenią, nie rozumiejąc praw rządzących światem realnym, m.in. tych, które dotyczą norm społecznych,

[20] Koncepcja Obronna Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej, Maj 2017, s. 34–35, 44–45.

a w następstwie tego naturalnych konsekwencji swojego zachowania i istoty relacji interpersonalnych[21].

Przypomnieć warto przy tym również ustalenia Najwyższej Izby Kontroli [dalej: NIK] dokonane w ramach kontroli pn. „Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży" przeprowadzonej w okresie od 9 stycznia do 18 kwietnia 2017 r. w Ministerstwie Edukacji Narodowej, Ministerstwie Cyfryzacji oraz wybranych Komendach Wojewódzkich Policji, Komendach Powiatowych Policji i szkołach (lata szkolne 2013/2014-2016/2017). Wyniki badań ankietowych przeprowadzonych przez NIK w trakcie przedmiotowej kontroli wskazały, że 26,7% ankietowanych uczniów przyznało, iż dotknęło ich zjawisko cyberprzemocy. Równocześnie 24,5% ankietowanych rodziców potwierdziło, że ich dziecko stało się bezpośrednio ofiarą cyberprzemocy. W informacji NIK o wynikach kontroli wskazano, że działania klasyfikowane jako „cyberprzemoc" wypełniać mogą znamiona takich czynów zabronionych poddanych odpowiedzialności na gruncie ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[22] oraz ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń[23], jak: zniesławienie (art. 212 § 1 i 2 k.k.), zniewaga (art. 216 § 1 i 2 k.k.), kradzież tożsamości (art. 268a § 1 k.k.), groźba karalna (art. 190 § 1 k.k.), uporczywe nękanie oraz podszywanie się pod inną osobę lub wykorzystywanie jej wizerunku (art. 190a § 1 i 2 k.k.), zmuszanie do określonego zachowania lub znoszenia (art. 191 § 1 k.k.), utrwalanie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej albo rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody (art. 191a § 1 k.k.), kradzież informacji (art. 267 § 1 k.k.), naruszenie integralności informacji i prawa do niezakłóconego dostępu do niej osoby uprawnionej (art. 268 § 1 i 2 k.k.) oraz naruszenie spokoju człowieka (art. 107 k.w.) i naruszenie obyczajności (art. 141 k.w.)[24].

Nie sposób pominąć w konsekwencji całego zjawiska cyberprzestępczości, skierowanego nie tylko przeciwko dzieciom i młodzieży, a stanowiącego najpoważniejsze zagrożenie dla bezpieczeństwa w cyberprzestrzeni. Skala

[21] B. Kałdon, *Cyberprzestrzeń jako zagrożenie człowieka XXI wieku*, „Seminare" 2 (2016), s. 89–90.
[22] Dz. U. z 2018 r., poz. 1600 z późn. zm. [dalej cyt.: k.k.].
[23] Dz. U. z 2018 r., poz. 618 z późn. zm. [dalej cyt.: k.w.].
[24] Najwyższa Izba Kontroli, Delegatura w Kielcach, Informacja o wynikach kontroli „Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży", LKI.410.002.00.2017, Nr ewid. 16/2017/P/17/071/LKI, w: www.nik.gov.pl, s. 11.

popełnianych w cyberprzestrzeni lub z jej wykorzystaniem przestępstw rośnie lawinowo z wielu powodów. Jednym z nich jest dynamiczny rozwój narzędzi IT, które mogą być wykorzystywane w celach przestępczych przez nawet niezaawansowanego pod względem technicznym użytkownika, a mogą zapewnić mu ukrycie tożsamości i rzeczywistej lokalizacji (np. narzędzia anonimizujące sieć), innym – rosnąca liczba punktów darmowego dostępu do Internetu (*hot spot*), jeszcze innym – transgraniczność Internetu, zapewniająca łatwy dostęp do usług świadczonych przez podmioty mające siedzibę w innym kraju. Nie można też zapominać również o rosnącej liczbie faktycznych użytkowników Internetu i wzroście ilości środków finansowych będących przedmiotem transakcji dokonywanych w sposób elektroniczny[25]. W samym 2017 r. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL (utworzony 1 lutego 2008 r. w ramach Agencji Bezpieczeństwa Wewnętrznego), który pełni rolę głównego Zespołu CERT odpowiadającego za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze administracji rządowej oraz infrastruktury krytycznej, odnotował 28 281 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych w sieciach, które znajdowały się w zakresie jego kompetencji, co stanowi znaczący wzrost wobec 19 954 zgłoszeń zarejestrowanych w 2016 r.[26] Z badania przeprowadzonego przez KPMG pn. „Barometr cyberbezpieczeństwa" na grupie ponad 100 dużych, średnich i małych przedsiębiorstw wynika, że 82% spośród przedsiębiorstw odnotowało w 2017 r. co najmniej 1 cyberincydent, a 37% zaobserwowało wzrost liczby cyberataków. Jako źródło tego rodzaju ataków wskazano zorganizowane grupy przestępcze (62%) lub pojedynczych hakerów (61%). Za największe ryzyka dla organizacji uznano takie działania cyberprzestępcze, jak: zaawansowane ataki kierunkowe (APT – *Advanced Persistent Attacks*), wycieki danych za pomocą złośliwego oprogramowania (*malware*), kradzież danych przez pracowników, ogólne kampanie *ransomware* (ograniczenia w dostępie do komputera uzależnione od opłacenia „okupu"), wyłudzanie danych uwierzytelniających (*phishing*)[27].

Mechanizmy kształtowania należytego poziomu przywołanych powyżej części składowych bezpieczeństwa narodowego – bezpieczeństwa politycz-

[25] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny. Czasopismo Centrum Szkolenia Policji w Legionowie" 4 (2017), s. 21–23.

[26] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2017, Warszawa, kwiecień 2017, w: cert.gov.pl, s. 11.

[27] Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym, styczeń 2018, w: kpmg.pl, s. 4, 7.

nego, ekonomicznego, społeczno-kulturowego, ekologicznego, militarnego bądź informacyjnego, uwzględniać muszą nie tylko teoretycznie możliwe, ale występujące realnie zjawiska godzące w prawa i wolności osobiste, polityczne, czy też ekonomiczne, socjalne i kulturalne, a zagrażające bezpieczeństwu w cyberprzestrzeni, takie jak np.: cyberataki podczas wyborów w państwach demokratycznych (np. przed wyborami prezydenckimi w Stanach Zjednoczonych w 2016 r.[28]), zagrożenia towarzyszące obrotowi gospodarczemu w Internecie (np. ataki na systemy bankowe[29]), zagrożenia wymierzone przeciwko infrastrukturze transportowej (np. cyberatak na serwer portu lotniczego w Modlinie w listopadzie 2017 r.[30]), cyberterroryzm (np. atak hakerów na elektrownie atomowe w Stanach Zjednoczonych[31]), cyberwojna (np. atak na Izrael w 2006 r. w czasie operacji przeciwko Hezbollahowi, tzw. pierwsza cyberwojna przeciwko Estonii w kwietniu 2007 r.[32]), itd.

IV. OCHRONA CYBERPRZESTRZENI W ŚWIETLE REGULACJI UNIJNYCH I MIĘDZYNARODOWYCH

Mając na uwadze powyższe, instrumentarium służące przeciwdziałaniu i zwalczaniu zjawisk patologicznych musi zawierać z natury rzeczy szerokie spektrum środków, w szczególności tych o charakterze prawnym, ale umożliwiające stałą współpracę międzynarodową właściwych organów i instytucji publicznych oraz podmiotów komercyjnych. Lektura preambuły do Konwencji Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości[33] pozwala stwierdzić, że wspólnota międzynarodowa identyfikuje uwarunkowania towarzyszące zagrożeniom dla bezpieczeństwa cyberprzestrzeni, dostrzegając potrzebę „prowadzenia, jako kwestii priorytetowej, wspólnej polityki

[28] *USA: nowe sankcje na Rosję za cyberoperacje przed wyborami z 2016 r.*, w: http://www.pap.pl/aktualnosci/news,1331276,usa-nowe-sankcje-na-rosje-za-cyberoperacje-przed-wyborami-z-2016-r.html [dostęp: 15.03.2018].

[29] *Polski sektor bankowy zaatakowany. Hakerzy zaatakowali kilka banków i KNF*, w: https://www.money.pl/gospodarka/wiadomosci/artykul/atak-na-banki-hakerzy-abw-wlamania-do-bankow,220,0,2256604.html [dostęp: 8.05.2018].

[30] *Cyberatak na lotnisko w Modlinie. Port bezpieczny*, w: http://biznesalert.pl/cyberatak-lotnisko-modlinie-port-bezpieczny [dostęp: 30.03.2018].

[31] *Hakerzy zaatakowali elektrownie atomowe w USA*, w: https://businessinsider.com.pl/wiadomosci/atak-hakerow-na-elektrownie-atomowe-w-usa/t26prq6 [dostęp: 8.05.2018].

[32] Zob. M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations" 44 (2011), s. 142 n.

[33] Dz. U. z 2015 r., poz. 728.

kryminalnej mającej na celu ochronę społeczeństwa przed cyberprzestępczością, między innymi poprzez przyjęcie właściwych przepisów prawnych i wspieranie międzynarodowej współpracy; […] współpracy między państwami i przemysłem prywatnym w zwalczaniu cyberprzestępczości oraz potrzebę ochrony prawnie uzasadnionych interesów w stosowaniu i rozwoju technologii informatycznych; zdając sobie sprawę, że skuteczna walka z cyberprzestępczością wymaga zwiększonej, szybkiej i dobrze funkcjonującej współpracy międzynarodowej w sprawach karnych […]". Dlatego też sama konwencja wśród narzędzi przeciwdziałania cyberprzestępczości wymienia różnego rodzaju środki o charakterze krajowym, obejmujące narzędzia o charakterze materialnokarnym, procesowym i odnoszące się do jurysdykcji państw nad cyberprzestępstwami (rozdział II Konwencji o cyberprzestępczości), a także środki dotyczące współpracy międzynarodowej, obejmujące m.in. wzajemną pomoc prawną (rozdział III Konwencji o cyberprzestępczości). Warto wspomnieć, że wskazuje się w tym akcie normatywnym chociażby na obowiązek podejmowania przez poszczególne państwa działań prowadzących do zagwarantowania poniesienia odpowiedzialności (karnej, cywilnej lub administracyjnej) nie tylko przez osoby fizyczne przestępstw tego rodzaju się dopuszczające, ale i przez osoby prawne za przestępstwa objęte przedmiotową konwencją, popełnione dla ich korzyści przez osobę fizyczną, działającą samodzielnie będącą członkiem organu osoby prawnej, a zajmującą w niej pozycję wiodącą z uwagi na uprawnienia do reprezentowania osoby prawnej, uprawnienia do podejmowania decyzji w imieniu osoby prawnej lub uprawnienia do wykonywania wewnętrznej kontroli w ramach osoby prawnej (art. 12 Konwencji o cyberprzestępczości).

Jakkolwiek cyberprzestrzeń to specyficzny, odmienny niż fizyczny, wymiar aktywności jednostki i społeczeństwa, to w pewnym sensie narzędzia ochrony cyberprzestrzeni, a ściślej – dóbr istotnych społecznie, w tym praw i wolności człowieka, które mogą w niej zostać naruszone, muszą być – poza instrumentami o charakterze technologicznym – tożsame z „klasycznymi" narzędziami ochrony prawnej, współpracy międzynarodowej, itp. We wspólnym komunikacie do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 7 lutego 2013 r. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń"[34], wskazano wyraźnie: „Aby cyberprzestrzeń pozostała otwarta i wolna, w środowisku internetowym po-

[34] JOIN (2013) 1 final.

winny mieć zastosowanie te same normy, zasady i wartości, które UE wspiera w świecie rzeczywistym. W cyberprzestrzeni należy zapewnić ochronę praw podstawowych, demokracji i praworządności. Nasza wolność i nasz dobrobyt w coraz większym stopniu uzależnione są od sprawnego i innowacyjnego internetu, który nadal będzie odgrywał kluczową rolę, jeżeli sektor prywatny i społeczeństwo obywatelskie będą w dalszym ciągu stymulować jego rozwój. Wolność w środowisku internetowym wymaga jednak również bezpieczeństwa i ochrony. Cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami, przy czym znaczącą rolę w zapewnieniu wolnej i bezpiecznej cyberprzestrzeni odgrywają administracje rządowe. Mają one szereg zadań: zapewnienie dostępu i otwartości, poszanowanie i ochronę praw podstawowych w internecie oraz utrzymanie niezawodności i interoperacyjności internetu. Znaczne części cyberprzestrzeni są jednak w posiadaniu i użytku sektora prywatnego i dlatego wszelkie inicjatywy w tej dziedzinie, jeśli mają prowadzić do sukcesów, muszą uwzględniać jego wiodącą rolę".

Nadmienić trzeba dodatkowo, że niezwykle istotne znaczenie ma ochrona danych osobowych w cyberprzestrzeni. Stąd też nie można zapominać również o rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[35], które weszło w życie z dniem 25 maja 2018 r., a którego art. 32 ust. 1 nakłada na administratora danych osobowych, jak i podmiot te dane przetwarzający, obowiązek wdrożenia stosownych – uwzględniając poziom ryzyka – środków technicznych i organizacyjnych, które mają zapewniać właściwy poziom bezpieczeństwa przetwarzania. Prawodawca unijny wskazał przy tym na przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu tego celu, wymieniając w szczególności: pseudonimizację i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; czy też regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Mowa tutaj zatem m.in. o uodpornieniu systemów informa-

[35] Dz. Urz. UE. L Nr 119, s. 1.

tycznych lub procesów przetwarzania wykonywanych za ich pośrednictwem na ataki z zewnątrz (np. z wykorzystaniem odpowiedniego oprogramowania)[36].

V. ORGANY OCHRONY BEZPIECZEŃSTWA CYBERPRZESTRZENI

Zadania związane z ochroną cyberprzestrzeni wpisują się na gruncie krajowego porządku prawnego w kompetencje wielu instytucji zajmujących się ochroną szeroko rozumianego bezpieczeństwa powszechnego i porządku publicznego. Krąg podmiotów wyposażonych przez ustawodawcę w kompetencje służące ochronie cyberbezpieczeństwa (bezpieczeństwa teleinformatycznego) obejmuje zarówno organy administracji publicznej, jak również organy ochrony prawnej, a wreszcie służby specjalne i siły zbrojne. Wskazać trzeba na chociażby niektóre spośród nich.

Rozpocząć wypada od organów administracji łączności – ministra właściwego do spraw informatyzacji (obecnie Minister Cyfryzacji) oraz Prezesa Urzędu Komunikacji Elektronicznej [dalej: Prezes UKE]. W myśl art. 12a ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej[37], dział „informatyzacja" obejmuje m.in. sprawy bezpieczeństwa cyberprzestrzeni, a sam minister właściwy do spraw informatyzacji nadzoruje państwowy instytut badawczy – Naukowa Akademicka Sieć Komputerowa, do którego zadań należy m.in. działalność badawczo-rozwojowa dotycząca opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Prezes UKE jest natomiast centralnym organem administracji rządowej właściwym w sprawach regulacji rynku usług telekomunikacyjnych. Odpowiada m.in. za nadzorowanie wykonywania przez dostawców publicznie dostępnych usług telekomunikacyjnych i operatorów publicznej sieci telekomunikacyjnej, obowiązków dotyczących podejmowania środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów w związku ze świadczonymi usługami, zgodnie z zasadami określonymi w dziale VIIa ustawy z dnia

[36] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Wydawnictwo C.H. Beck, Warszawa 2018, komentarz do art. 32, teza 2.

[37] Dz. U. z 2018 r., poz. 762 z późn. zm. [dalej cyt.: u.dz.a.rz.].

16 lipca 2004 r. – Prawo telekomunikacyjne[38] pt. „Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych".

Kolejna grupa podmiotów wykonujących zadania związane z ochroną cyberprzestrzeni to służby specjalne. Mowa tutaj w szczególności o Agencji Bezpieczeństwa Wewnętrznego i Służbie Kontrwywiadu Wojskowego. Zgodnie z przepisem art. 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, do zadań tej pierwszej służby należy m.in.: rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej. Pamiętać w tym miejscu należy również o szerokim zakresie kompetencji Szefa Agencji Bezpieczeństwa Wewnętrznego przewidzianych ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[39] odnoszących się w szczególności do zagrożeń o charakterze cyberterrorystycznym. Wśród zadań Służby Kontrwywiadu Wojskowego mieszczą się, zgodnie z art. 5 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego[40] – prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy.

Nie można zapominać o Ministrze Obrony Narodowej i Ministrze Spraw Wewnętrznych i Administracji oraz formacjach im podległych. Dział obrona narodowa (art. 19 ust. 1 u.dz.a.rz.) obejmuje, w czasie pokoju, sprawy obrony Państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej. Siły Zbrojne Rzeczypospolitej Polskiej zgodnie z art. 3 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej[41], stoją zaś na straży suwerenności i niepodległości Narodu Polskiego oraz jego bezpieczeństwa i pokoju, a ponadto mogą brać udział m.in. w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działaniach antyterrorystycznych i z zakresu ochrony mienia, akcjach poszukiwawczych oraz ratowania lub ochrony zdrowia i życia ludzkiego, a także w realizacji zadań z zakresu zarządza-

[38] Dz. U. z 2018 r., poz. 1954 z późn. zm.
[39] Dz. U. z 2018 r., poz. 452 z późn. zm.
[40] Dz. U. z 2017 r., poz. 1978 z późn. zm.
[41] Dz. U. z 2018 r., poz. 1459 z późn. zm.

nia kryzysowego. Działania te z oczywistych względów mogą być prowadzone również w związku z zagrożeniami występującymi w cyberprzestrzeni. Zgodnie z art. 29 u.dz.a.rz., dział sprawy wewnętrzne obejmuje natomiast m.in. sprawy ochrony bezpieczeństwa i porządku publicznego oraz zarządzania kryzysowego, a minister właściwy do spraw wewnętrznych sprawuje nadzór m.in. nad działalnością Policji, która wykonuje czynności wpisujące się w ochronę cyberbezpieczeństwa. Zgodnie z art. 1 ustawy o Policji, do podstawowych zadań Policji należy m.in.: ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra; ochrona bezpieczeństwa i porządku publicznego; inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi; prowadzenie działań kontrterrorystycznych w rozumieniu ustawy o działaniach antyterrorystycznych; wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców. Dodać warto, że z dniem 1 grudnia 2016 r. decyzją Komendanta Głównego Policji i Ministra Spraw Wewnętrznych i Administracji w strukturach Policji utworzono wyspecjalizowane Biuro do walki z Cyberprzestępczością[42].

Wspomnieć wreszcie wypada chociażby o Biurze Bezpieczeństwa Narodowego, urzędzie państwowym utworzonym na podstawie art. 11 ustawy o powszechnym obowiązku obrony i wspierającym Prezydenta Rzeczypospolitej w zakresie zadań związanych z bezpieczeństwem i obronnością, w tym w cyberprzestrzeni. Odpowiada ono m.in. za realizowanie powierzonych przez Prezydenta RP zadań w zakresie bezpieczeństwa i obronności, w tym inicjowanie i udział w przygotowaniu koncepcji oraz planów organizacji i funkcjonowania zintegrowanego systemu kierowania bezpieczeństwem narodowym, a także nadzór nad ich realizacją w imieniu Prezydenta RP; monitorowanie i analizowanie kształtowania się strategicznych warunków bezpieczeństwa narodowego (wewnętrznych i zewnętrznych); czy też monitorowanie, ocena i opiniowanie bieżącej działalności organów władzy publicznej i innych państwowych jednostek organizacyjnych w sferze bezpieczeństwa pozamilitarnego, w tym bezpieczeństwa publicznego i społecz-

[42] *Biuro do walki z Cyberprzestępczością Komendy Głównej Policji rozpoczęło działalność*, w: http://www.policja.pl/pol/aktualnosci/135801,Biuro-do-walki-z-Cyberprzestepczoscia-Komendy-Glownej-Policji-rozpoczelo-dzialal.html [dostęp: 30.03.2018].

no-gospodarczego, a do tych ostatnich zaliczyć trzeba i pewne aspekty bezpieczeństwa w cyberprzestrzeni.

UWAGI KOŃCOWE

Czym jest bezpieczeństwo w cyberprzestrzeni, kto za nie odpowiada, jak o nie dbać? Bezpieczeństwo w cyberprzestrzeni utożsamiać należy z procesem służącym zapewnieniu należytego poziomu bezpieczeństwa dla wszystkich (niezależnie od ich charakteru i statusu) użytkowników cyberprzestrzeni. Za jego utrzymanie na właściwym poziomie odpowiedzialne są zarówno instytucje publiczne (państwowe, rządowe, samorządowe), przedsiębiorcy, ale także i jego „zwykli" użytkownicy, korzystający z cyberprzestrzeni dla celów edukacyjnych, dokonujący transakcji finansowych, prowadzący korespondencję drogą elektroniczną, itp. Z uwagi na wielowymiarowość pojęcia cyberprzestrzeni i różnorodność zachodzących w niej aktywności, a także nie zawsze tożsame interesy użytkowników cyberprzestrzeni, instrumentarium narzędzi służących ochronie dóbr mogących podlegać naruszeniu w cyberprzestrzeni, czy też z jej wykorzystaniem, jest niezwykle bogate i jedynie w części sięga ono do środków o charakterze prawnym, którym zresztą trudno nadążyć za postępującym rozwojem technologicznym, stwarzającym ogromne możliwości naruszania praw i wolności człowieka. Stąd też podsumowując niniejsze rozważania trzeba przypomnieć niektóre z zaleceń skierowanych pod adresem rządów, organizacji międzynarodowych i sektora prywatnego, a odnoszące się do konieczności stałego podnoszenia poziomu bezpieczeństwa w cyberprzestrzeni. Zwraca się wśród nich uwagę m.in. na konieczność: wzrostu inwestycji w cyberbezpieczeństwo i stworzenia racjonalnego planu wykorzystania tych środków; stworzenia specjalnego systemu sankcji i zachęt dotyczących implementacji sektorowych standardów bezpieczeństwa, a także dobre zaprojektowanie systemu certyfikacji produktów i usług IT i ICT; współpracy sektora prywatnego i państwowego w zakresie budowania zdolności do działania w cyberprzestrzeni; docenienia wagi walki informacyjnej prowadzonej w cyberprzestrzeni jako istotnego zagrożenia dla demokracji; zwiększenia poziomu cyberbezpieczeństwa w NATO, tj. zapewnienia bezpieczeństwa operacji wojskowych i wzmocnienie cyberobrony krajów członkowskich Paktu Północnoatlantyckiego; jednoczesnego postrzegania sztucznej inteligencji (*Artificial Intelligence*) jako szansy i zagrożenia wymykającego się spod ludzkiej kontroli; wdrażania w kulturę cyberbezpieczeństwa efektywnego systemu cyberubezpieczeń; dalszego rozwoju bezpie-

czeństwa w obszarze biznesu; budowania regionalnych centrów kompetencyjnych opartych na silnej i efektywnej współpracy pomiędzy uczestnikami ekosystemu (np. Globalna Platforma Innowacji dla Cyberbezpieczeństwa, Global EPIC)[43]. Poddając analizie zasadność wdrożenia wspomnianych powyżej rekomendacji należy pamiętać, iż zagrożenia stanowiące konsekwencję niewłaściwego wykorzystania w wirtualnej cyberprzestrzeni godzą w rzeczywistości w te same prawa i wolności jednostki, które mogą być naruszone w sposób konwencjonalny w środowisku fizycznym, ale ich ochrona jest nieporównanie trudniejsza i wymaga poważniejszych przedsięwzięć organizacyjnych i nakładów finansowych, a także stałego podążania regulacji prawnych za postępem rozwiązań technologicznych.

PIŚMIENNICTWO

2016. „Biuro do walki z Cyberprzestępczością Komendy Głównej Policji rozpoczęło działalność." W http://www.policja.pl/pol/aktualnosci/135801,Biuro-do-walki-z-Cyberprzestepczoscia-Komendy-Glownej-Policji-rozpoczelo-dzialal.html [dostęp: 30.03.2018].

2017. „Cyberatak na lotnisko w Modlinie. Port bezpieczny." W http://biznesalert.pl/cyberatak-lotnisko-modlinie-port-bezpieczny [dostęp: 30.03.2018].

2017. „Hakerzy zaatakowali elektrownie atomowe w USA." W https://businessinsider.com.pl/wiadomosci/atak-hakerow-na-elektrownie-atomowe-w-usa/t26prq6 [dostęp: 8.05.2018].

2017. „Polski sektor bankowy zaatakowany. Hakerzy zaatakowali kilka banków i KNF." W https://www.money.pl/gospodarka/wiadomosci/artykul/atak-na-banki-hakerzy-abw-wlamania-do-bankow,220,0,2256604.html [dostęp: 8.05.2018].

2018. „USA: nowe sankcje na Rosję za cyberoperacje przed wyborami z 2016 r." W http://www.pap.pl/aktualnosci/news,1331276,usa-nowe-sankcje-na-rosje-za-cyberoperacje-przed-wyborami-z-2016-r.html [dostęp: 15.03.2018].

Chilmon, Eryk. 2018. „9 wyzwań dla bezpieczeństwa cyfrowego." *IT w administracji* 3:49.

Czyżak, Mariusz. 2017. „Prawna ochrona cyberprzestrzeni państwa." *Horyzonty Bezpieczeństwa* 8:5–15.

Gibson, Wiliam. 2009. *Neuromancer*. Katowice: Wydawnictwo Książnica.

Kałdon, Barbara. 2016. „Cyberprzestrzeń jako zagrożenie człowieka XXI wieku." *Seminare* 2:87–101.

Koziej, Stanisław. 2011. „Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja." *Bezpieczeństwo Narodowe* 18(2):19–39.

Lakomy, Miron. 2011. „Cyberwojna jako rzeczywistość XXI wieku." *Stosunki Międzynarodowe – International Relations* 44:141–161.

Litwiński, Paweł (red.). 2018. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Majer, Piotr. 2012. „W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego." *Przegląd Bezpieczeństwa Wewnętrznego* 7:11–18.

[43] E. Chilmon, *9 wyzwań dla bezpieczeństwa cyfrowego*, „IT w administracji" 3 (2018), s. 49.

Nowakowski, Zdzisław, Hieronim Szafran, i Robert Szafran. 2009. *Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw*. Rzeszów: Politechnika Rzeszowska.

Nowiński, Marcin. 2017. „Pojęcie bezpieczeństwo narodowe w prawie europejskim i międzynarodowym w kontekście uprawnień służb specjalnych." W *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, red. Piotr Burczaniuk, 11–22. Warszawa: Agencja Bezpieczeństwa Wewnętrznego, Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota".

Stefanowicz, Mariusz. 2017. „Cyberprzestępczość – próba diagnozy zjawiska." *Kwartalnik Policyjny. Czasopismo Centrum Szkolenia Policji w Legionowie* 4:19–23.

Wasilewski, Janusz. 2013. „Zarys definicyjny cyberprzestrzeni." *Przegląd Bezpieczeństwa Wewnętrznego* 9:225–234.

CYBERSPACE SECURITY

Summary. In the article the problem of cyberspace security was thoroughly discussed. The terms concerning security issues, cyberspace as well as chosen categories of dangers in cyberspace were introduced. It was pointed out that the responsibility for the proper level of security should be held by public institutiones, companies and individual users of cyberspace.

Key words: security, cyberspace, cybercrime