Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 65–76

DOI: 10.17951/teka.2018.13.2.65-76

BEZPIECZEŃSTWO CYBERPRZESTRZENI W REGULACJACH UE

Krzysztof Gawkowski

Wydział Zarządzania i Logistyki
Uczelnia Techniczno-Handlowa
im. Heleny Chodkowskiej w Warszawie
ORCID ID: https://orcid.org/0000-0002-4025-5927
e-mail: krzysztof.gawkowski@uth.edu.pl

Streszczenie: Cyberprzestrzeń z roku na rok jest coraz większa, a jej wpływ na życie ludzkie coraz bardziej widoczny. Właściwa ochrona wszystkich procesów, które mogą negatywnie wpływać na życie ludzi, jest zatem niezbędnym elementem, który powinien towarzyszyć szybkiemu rozwojowi informacyjno-komunikacyjnemu. Bezpieczna cyberprzestrzeń jest również ściśle związana z wewnętrznym i zewnętrznym bezpieczeństwem każdego kraju. Przygotowanie odpowiednich międzynarodowych gwarancji bezpieczeństwa w cyberprzestrzeni jest nie tylko wyzwaniem dla poszczególnych krajów, ale przede wszystkim dla globalnych instytucji zapewniających pokój.

Unia Europejska i Rada Europy powinny być liderami w tym zakresie. Brak przepisów prawnych dotyczących bezpiecznej cyberprzestrzeni to możliwość narażenia ludzi na przejęcie kontroli nad ich prywatnością, kradzieżą danych lub innymi przestępstwami. Dlatego wdrażanie norm europejskich powinno mieć zastosowanie w każdym kraju. Rządy powinny dodatkowo podkreślać edukację społeczną i rozpowszechniać wiedzę o zagrożeniach w cyberprzestrzeni. Koordynacja tych dwóch działań daje nadzieję, że rozwijająca się cyberprzestrzeń w przyszłości nie zniszczy życia ludzi.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo, Unia Europejska, prawo

WPROWADZENIE

Rozwój cywilizacyjny ostatnich dekad spowodował, że nowoczesne technologie oraz cyberprzestrzeń miały olbrzymi wpływ na wszystkie aspekty funkcjonowania zarówno jednostki, jak i całego społeczeństwa. Niemalże wszystkie sfery życia, poczynając od pracy, zakupów czy snu, a kończąc na rozwoju biznesu, administracji, gospodarce, czy prawach podstawowych, są uzależnione od

sprawnie funkcjonujących technologii informacyjno-komunikacyjnych. Otwarta i wolna cyberprzestrzeń usunęła bariery między państwami, społecznościami czy obywatelami, jednocześnie pozwalając na wymianę informacji oraz pomysłów w globalnej skali. Cyberprzestrzeń stanowi więc forum wymiany doświadczeń, umiejętności czy idei. W niektórych przypadkach daje jednostkom lub społeczeństwom szansę na walkę o bardziej demokratyczne i sprawiedliwe rządy, jak podczas Wiosny Ludów w krajach arabskich, kiedy główną areną początkowej fazy powstania był właśnie internet. Biorąc pod uwagę wszechobecność cyberprzestrzeni, nie możemy jednak zapominać o konieczności zabezpieczenia danych i informacji, które są tam gromadzone i przetwarzane. Najlepszym przykładem mogą być działania firmy analitycznej Cambridge Analytica, która wykorzystując skomplikowane algorytmy oraz wiedzę o użytkownikach Facebooka, próbowała wpłynąć (i wszystko na to wskazuje, że wpłynęła) na wynik wyborów prezydenckich w USA. Gwarancja bezpiecznej cyberprzestrzeni jest zatem elementem kluczowym dla zachowania zarówno jej otwartości, jak i skutecznej walki ze wszelkimi naruszeniami ogólnie przyjętych zasad.

Świat wokół nas nieustannie ewoluuje i zmiany te wiążą się nie tylko z poprawą jakości życia, ale też niejednokrotnie z nowymi zagrożeniami, one zaś zmniejszają poczucie bezpieczeństwa. W wielu ujęciach bezpieczeństwo jest traktowane jako potrzeba pierwotna, elementarna i naczelna. W dosłownym znaczeniu oznacza brak zagrożeń i poczucie pewności, ale podobnie jak wiele innych kategorii teoretycznych w naukach społecznych nie posiada jednej, spójnej definicji [Malak 2007: 91–95], szczególnie w odniesieniu do sfery cyberprzestrzeni. Biorąc pod uwagę strukturę klasyfikacji bezpieczeństwa, jednym z fundamentalnych jego aspektów jest bezpieczeństwo publiczne i porządek publiczny. Oba pojęcia często występują łącznie, przenikają się i wzajemnie uzupełniają. W dostępnej literaturze prezentowane są stanowiska, które zarówno bezpieczeństwo publiczne, jak i porządek publiczny definiują jako stan pożądany [Brodie 1949: 477]. Jeszcze w przedwojennej definicji bezpieczeństwo publiczne jest charakteryzowane jako stan, w którym ogół społeczeństwa i jego interesy oraz państwo wraz ze swymi celami mają zapewnioną ochronę przed szkodami zagrażającymi im z jakiegokolwiek źródła [Kawka 1939, s. 3–5]. Najczęściej bezpieczeństwo publiczne jest jednak łączone ze stanem funkcjonowania państwa oraz jego obywateli, podczas gdy porządek publiczny z ograniczoną sferą przestrzegania norm oraz utrzymywaniem sprawności instytucji publicznych [Wiśniewski, Zalewski, Podleś, Kozłowska 2006: 21–22]. Oba pojęcia na pewno mają charakter administracyjny, czyli dotyczą zagadnień związanych z wdrażaniem i przestrzeganiem zasad obowiązujących w danym państwie.

BEZPIECZEŃSTWO W ŚWIECIE NOWYCH TECHNOLOGII

Bez względu jednak na to, jak postrzegamy bezpieczeństwo i porządek publiczny, największą obecnie obawą są gwarancje bezpieczeństwa w cyberprzestrzeni, która stała się codziennością dla miliardów ludzi. Poczucie bezpieczeństwa zarówno państwa, jak i jego obywateli spada gwałtownie, zwłaszcza na myśl o ujawnieniu danych personalnych, szczególnie zaś tzw. danych wrażliwych. Dane personalne od lat stanowią atrakcyjny zasób dla różnych oszustów i złodziei, a dzięki nim są możliwe okradanie kont bankowych, wyłudzanie kredytów czy inne oszustwa internetowe. Duże obawy rodzi również nasilająca się fala wycieków danych z instytucji przechowującej dane prywatne, intymne czy zdrowotne, którymi ludzie nie mają ochoty się dzielić z innymi: o zarobkach, chorobach, poglądach politycznych, orientacji seksualnej, wyznaniu itp. Do sieci dostają się również dane ze szpitali, zdjęcia z klinik chirurgii plastycznej, informacje z ośrodków pomocy społecznej czy urzędów administracji publicznej, a hakerzy włamują się do komputerów instytucji politycznych, wyznaniowych czy kancelarii prawnych. Rynek danych nigdy w historii nie był tak cenny jak obecnie. Na świecie jego szacunkowa wartość wynosiła w roku 2018 ponad 20 mld dolarów, a w kolejnym wzrośnie o ponad 26% do poziomu 26 mld dolarów. Trend potwierdza także Polska, gdzie tylko w tym roku na dane o internautach firmy wydadzą 21 mln dolarów, a w roku 2019 już o 16,2 mln dolarów więcej.

Kilkadziesiąt lat temu wrażliwymi danymi dysponowali tylko urzędnicy, lekarze czy prawnicy, a utrzymanie tajemnicy zawodowej było wpisane w zakres ich obowiązków. Granice bezpieczeństwa były jasne i przejrzyste. Dostępność cyberprzestrzeni diametralnie zmieniła ten krajobraz i obecnie wszelkie poufne dane zostały potencjalnie upublicznione w bazach danych różnych instytucji, z których coraz częściej wyciekają do internetu, gdzie handlują nimi mniej lub bardziej niebezpieczni przestępcy. O tym zaś, że możliwość taka nie jest jedynie teoretyczna, przekonali się w 2017 roku użytkownicy poczty internetowej, którzy przy okazji wycieku do sieci ok. 10 mln haseł do polskich kont [Kotowski 2017] zrozumieli, co znaczy w obecnych czasach gwarancja bezpieczeństwa w cyberprzestrzeni. Podobne doświadczenia spotkały osoby zapisane w polskich bazach InPost [*Poważny*...], pacjentów sieci litewskich klinik chirurgicznych, których zdjęcia hakerzy publikowali w sieci lub od których w zamian za nieopublikowanie tych zdjęć żądali zapłaty [*Hakerzy*… 2017]. Nie oszczędzono także popularnego dostarczyciela usług transportowych – Ubera, któremu skradziono ponad 50 mln danych pasażerów oraz 7 mln informacji o kierowcach [*Uber*...].

W sytuacji rosnącego zapotrzebowania środowiska przestępczego na różne dane trudno oczekiwać, że słysząc o kolejnych wyciekach informacji, będziemy czuli się bezpiecznie. Tym bardziej iż nie mamy pojęcia, o ilu włamaniach i kradzieżach danych nie jesteśmy w ogóle informowani. Pocieszające może być w tej sytuacji jedynie to, że wraz z pojawianiem się nowych zagrożeń wdrażane są równocześnie różne mechanizmy przeciwdziałania, np. w przypadku oszustw

kredytowych tworzone są systemy pozwalające przynajmniej częściowo kontrolować ewentualne sytuacje kryzysowe. Jednym z takich systemów jest baza Ognivo [*Czym…*], czyli międzybankowa formuła danych pozwalająca na bezpłatne sprawdzenie, w jakich bankach i oddziałach SKOK istnieją konta założone na nasze nazwisko. Dodatkowo istnieją również serwisy, w których można sprawdzić własną wiarygodność finansową, a więc również dowiedzieć się np. o wyłudzonych przez „siebie" kredytach [Ziętal 2009] czy BIK-Pass [Skorupa 2014], takie jak międzybankowa baza kredytów, w której możemy prześledzić własną historię kredytową i upewnić się, że nie mamy tam zaciągniętych przez oszustów na nasze konto zobowiązań, o których nic nie wiemy.

Poczuciu bezpieczeństwa obywatela skomputeryzowanego kraju i świata zagrażają też różne przejawy istnienia wirtualnego świata, w którym trudno jest odróżnić prawdę od fikcji. I chodzi tu nie tylko o głośne zjawisko *fake newsów* [Makowski 2017], czyli nieprawdziwych lub nie do końca prawdziwych informacji, najczęściej polityczno-gospodarczych, zalewających sieć, ale przede wszystkim o zjawisko kreowania świata, który w rzeczywistości nie istnieje. Najprostszym przykładem takiej kreacji są niektóre profile w mediach społecznościowych – ludzie dla zdobycia sympatii, popularności lub dokonania zaplanowanego przestępstwa udają tam kogoś, kim nie są, wymyślają swoje życie, okłamując innych użytkowników internetu [Kuchta 2017]. Z raportu Roberta Gorwa na temat fikcyjnych kont na portalach społecznościowych w naszym kraju wynika, że skala procederu jest olbrzymia. Tylko jedna z opisanych firm zarządza 40 tys. fikcyjnych tożsamości, z których każda ma kilka kont na różnych portalach. Szacuje się, że tego rodzaju profili może być nawet milion [Gorwa 2017]. Śmiało można wskazać, że jest to pierwszy krok do budowy fikcyjnego świata, bo od kilku lat wśród blogerów i influencerów [Becker 2017], a nawet sportowców [*Kolejny*…] pojawiają się idole, których nigdy nie było [Kuchta 2018], stworzeni jedynie po to, by coś wypromować lub sprzedać. Korzystając z łatwości tworzenia fikcyjnych postaci i przedmiotów, oszuści naciągają ludzi, tworząc fałszywe sklepy [Bodył 2018], a nawet fałszywe profile osób potrzebujących pomocy [*Dziecko…* 2017].

Generalnie zagrożenia występujące w cyberprzestrzeni można podzielić na dwa rodzaje, gdzie jednym z ich źródeł jest technika, np. awarie sprzętu, zasilania itp., a drugim – ludzie. Do drugiej z tych grup zalicza się nie tylko zagrożenia spowodowane przez ludzkie błędy wynikające np. z nieświadomości użytkowników lub lekceważenia obowiązków przez personel przedsiębiorstw i instytucji, lecz także wiele rodzajów działań, wynikających z różnych motywacji, np. chęci wzbogacenia się na sprzedaży poufnych danych. Konwencja Rady Europy wprowadza klasyfikację cyberprzestępstw [Siwicki 2012], dzieląc je na przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych, tj. nielegalny dostęp do danych, nielegalne ich przechwytywanie lub naruszenie ich integralności, naruszenie integralności systemu czy niewłaściwe użycie urządzeń. Druga sekcja to przestępstwa komputerowe, a w tym komputerowe fałszerstwa i oszustwa. Kolejnym elementem są przestępstwa uznane za działalność przestęp-

czą ze względu na ich charakter lub treść informacji, np. pornografia dziecięca, treści rasistowskie lub ksenofobiczne, groźby i zniewagi motywowane rasizmem lub ksenofobią. Natomiast ostatnią część stanowią przestępstwa polegające na naruszeniu praw autorskich i praw pokrewnych.

Analizując zatem gwarancje bezpieczeństwa w cyberprzestrzeni, można postawić nieco paradoksalny wniosek, że tym, co sprzyja poczuciu społecznego bezpieczeństwa, jest masowy dostęp do wiedzy i informacji, umożliwiony przez rozwój nowoczesnych technologii; jednocześnie ów powszechny dostęp do danych stanowi najpoważniejsze zagrożenie bezpieczeństwa wynikające z rozwoju technologicznego. Niemniej jednak tak właśnie przedstawia się nasze poczucie bezpieczeństwa oraz jego gwarancje w cyfrowym świecie. Ma ono dwa odmienne oblicza, niczym dwie strony tej samej monety. Pozytywnym aspektem w kontekście poczucia bezpieczeństwa jest to, że wciąż poszerza się zakres potrzebnych, pomocnych i łatwo dostępnych informacji oraz wciąż są tworzone narzędzia i procedury oraz regulacje prawne chroniące obywateli przed niewłaściwym użyciem danych i nieuprawnionym dostępem do nich.

INSTYTUCJE I STANDARDY ZABEZPIECZAJĄCE CYBERPRZESTRZEŃ

Liderem w tworzeniu międzynarodowych gwarancji bezpiecznej cyberprzestrzeni jest Unia Europejska. Podmioty zrzeszone we wspólnocie mogą liczyć na pomoc w dziedzinie tworzenia ram prawnych dla cyberochrony i cyberobrony oraz na wsparcie działających na tym polu instytucji unijnych. Jedna z pierwszych agencji mających wspierać i pracować nad ponadpaństwowym wsparciem gwarancji w cyberprzestrzeni powstała już w 2004 r. i jest to Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). Działa ona na podstawie rozporządzenia WE nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r., a na podstawie rozporządzenia Parlamentu Europejskiego i Rady UE nr 526/2013 z dnia 21 maja 2013 r. rozszerzono zakres jej działalności. Pierwotnie powołano ją głównie do zadań analitycznych i badawczych, których wyniki miały pomóc przy tworzeniu polityk cyberbezpieczeństwa w UE oraz tworzeniu dobrych praktyk i ustanawianiu standardów w tej dziedzinie. Obecnie swoimi działaniami wspiera proces tworzenia skutecznych rozwiązań z zakresu cyberbezpieczeństwa państw członkowskich Unii Europejskiej i innych organów unijnych. Opracowuje również plany międzynarodowych ćwiczeń z ochrony cyberprzestrzeni oraz je przeprowadza. Od roku 2012 rozpoczęto regularne szkolenie dla sektora bankowego, a od 2014 dla sektorów telekomunikacyjnego oraz energetycznego. W roku 2016 rozpoczęła się edukacja dostawców internetu oraz firm z sektora bezpieczeństwa IT. Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji została wyznaczona jako punkt, do którego należy przekazywać informacje o incydentach naruszenia bezpieczeństwa i integralności sieci telekomunikacyjnych, zebrane przez organy poszczególnych państw członkowskich od dostawców usług teleinformatycznych.

Bardzo ważnym elementem międzynarodowej współpracy oraz tworzenia gwarancji cyberbezpieczństwa jest powstałe na wniosek Europejskiej Agendy Cyfrowej w 2013 r. Europejskie Centrum Cyberprzestępczości (ang. *European Cybercrime Centre* – EC3), które działa przy EUROPOL i ma zapewnić wymianę informacji oraz współpracę między policjami państw członkowskich UE oraz świadczyć dla nich usługi laboratoryjne z zakresu cyberprzestępczości. Centrum ma trzypoziomowe podejście do walki z cyberprzestępczością w podziale na kryminalistykę, strategię i operacje [*European*…]. W części dotyczącej kryminalistyki działania skupiają się na wypracowaniu metod i środków zbierania oraz analizowania informacji o działaniach przestępczych w cyberprzestrzeni. Przygotowując założenia strategiczne, analizie są poddawane przede wszystkim nowe obszary, w których mogą działać cyberprzestępcy. Natomiast na poziomie operacji koncentruje się na cyberprzestępstwach, które są popełniane przez zorganizowane grupy przestępcze, szczególnie na tych generujących duże zyski przestępcze, jak np. oszustwa internetowe, mogą poważnie zaszkodzić ofiarom, np. wykorzystywanie seksualne dzieci, oraz mogą wpływać na krytyczną infrastrukturę i systemy informacyjne w UE, np. ataki komputerowe.

Unia Europejska stworzyła także Centrum ds. Cyberprzestępczości w Zakresie Doskonalenia Szkoleń, Badań i Edukacji (ang. *Cybercrime Centre of Excellence Network for Training, Research and Education* – 2CENTRE) [Dereń, Rabiak 2014] oraz Europejską Grupę ds. Szkolenia i Edukacji w Zakresie Cyberprzestępczości (ang. *European Cybercrime Training and Education Group* – ECTEG), czyli międzynarodowe stowarzyszenie non profit zrzeszające organy ścigania z państw UE oraz Europejskiego Obszaru Gospodarczego. Istotną rolę w walce z przestępczością w Europie odgrywa także Eurojust [*History*...], zajmując się m.in. pomocą właściwym organom państw członkowskich w przypadku poważnych przestępstw transgranicznych i zorganizowanych, takich jak np. cyberprzestępczość, terroryzm czy handel ludźmi oraz narkotyki. Może również świadczyć usługi logistyczne, np. pomoc w tłumaczeniu, interpretacji i organizacji spotkań. Ponadto współpracuje i konsultuje się z Europejską Siecią Sądową – EJN.

Gwarancjami bezpieczeństwa w cyberprzestrzeni oraz przestrzegania uzgodnionych norm zajmuje się także Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania CEPOL. Celem agencji jest opracowanie, wdrożenie i koordynacja szkoleń dla urzędników odpowiedzialnych za egzekwowanie prawa [*About us* (b)]. Łączy ona sieć instytucji szkoleniowych dla funkcjonariuszy organów ścigania w państwach członkowskich UE oraz wspiera ich w zakresie wstępnego szkolenia dotyczącego priorytetów w zakresie bezpieczeństwa, współpracy w egzekwowaniu prawa i wymiany informacji. CEPOL współpracuje również z organami UE, organizacjami międzynarodowymi i krajami trzecimi, aby działania dotyczące najbardziej poważnych dla bezpieczeństwa zagrożeń były podejmowane wspólnie.

Innym podmiotem, zajmującym się cyberprzestępczością i jej eliminowaniem jest Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowy-

mi Systemami Teleinformatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości – EU-LISA [*About us* (a)]. Agencja jest odpowiedzialna za zarządzanie technologiami informacyjno-komunikacyjnymi i promowanie ich jako kluczowego czynnika sukcesu w zakresie wdrażania unijnych polityk w dziedzinie wymiaru sprawiedliwości, bezpieczeństwa i wolności. Odpowiada m.in. za zarządzanie operacyjne trzema systemami informacyjnymi, tj. systemem informacyjnym Schengen [*System…*], wizowym systemem informacyjnym VIS oraz Eurodac, tj. Europejskim Zautomatyzowanym Systemem Rozpoznawania Odcisków Palców [*Eurodac*].

W ramach działań wspólnotowych już w grudniu 2012 r. ministrowie obrony UE uzgodnili regulacje związane z *Cyber Defence on the Pooling & Sharing agenda*, które dotyczą wskazówek dla dowódców operacyjnych dla zachowań w cyberprzestrzeni. W marcu 2013 r. wzbogacono ją o *EU Cyber Defence Capability Requirements Statement*, natomiast w lutym 2013 r. UE ogłosiła *Cyber Security Strategy – An Open, Safe and Secure Cyberspace*, która kompleksowo podchodzi do kwestii cyberbezpieczeństwa, zajmując się zarówno jego aspektami cywilnymi, jak i militarnymi w ramach wspólnej polityki bezpieczeństwa i obrony [Röhrig, Smeaton 2016]. W części cywilnej strategia jako kluczowy element wskazuje utrzymanie wolnej, otwartej i chronionej cyberprzestrzeni, która jest wyzwaniem na skalę światową, i któremu Unia musi stawić czoła z największą intensywnością. Działania takie mają być podejmowane i koordynowane wraz z odpowiednimi partnerami i organizacjami międzynarodowymi, sektorem prywatnym i społeczeństwem obywatelskim. Dodatkowo w dokumencie podkreślono, że odpowiedzialność za zwiększenie bezpieczeństwa w cyberprzestrzeni spoczywa na wszystkich podmiotach tworzących globalne społeczeństwo informacyjne, począwszy od obywateli aż po administracje rządowe. Część obronna strategii obejmuje cztery główne obszary działań, tj. tworzenie ram polityki unijnej w dziedzinie cyberobrony, budowanie przez państwa członkowskie Unii zdolności obronnych w cyberprzestrzeni, budowę i promowanie cywilno-wojskowego dialogu oraz dialog z międzynarodowymi partnerami, np. z NATO. Większość państw członkowskich wspólnoty stara się wdrażać postanowienia strategii, zawracając jednak uwagę, że konieczność zabezpieczenia i ochrony cyberprzestrzeni na szczeblu regionalnym i krajowym nie powinna usprawiedliwiać jakiegokolwiek ograniczania praw i swobód w przestrzeni cybernetycznej i informatycznej.

Pomimo rozbudowanej struktury agend i instytucji mających gwarantować bezpieczeństwo międzynarodowe w cyberprzestrzeni, ściganie i karanie naruszeń prawa często utrudnia problem określenia miejsca popełnienia przestępstwa, ponieważ przestępczość teleinformatyczną cechują często transgraniczność i wielomiejscowość [Stępniewska 2014: 16–19]. Tymczasem od miejsca popełnienia przestępstwa zależy to, jakie prawo zostanie wobec przestępcy zastosowane. Co prawda w takich przypadkach na ogół stosuje się tzw. zasadę terytorialności, czyli zgodnie z art. 5 Kodeksu karnego wobec sprawcy, który popełnia przestępstwo

na terenie Polski albo na pokładzie polskiego samolotu lub statku, stosuje się polskie przepisy, ale są od tej zasady wyjątki. Polskie prawo w tym względzie jest zbieżne z Konwencją Rady Europy o cyberprzestępczości i z dyrektywą 2013/40 Parlamentu Europejskiego i Rady dotyczącą ataków na systemy informatyczne, o czym więcej w dalszej części artykułu. Konwencja Rady Europy reguluje także zasady współpracy między państwami, które ją ratyfikowały. Podmioty takie są zobowiązane do udzielania wzajemnej pomocy prawnej przy ściganiu cyberprzestępców oraz prowadzeniu przeciwko nim postępowań. Prawo do odmowy wspomnianej pomocy przysługuje w sytuacji, gdy państwo uzna, że sprawa dotyczy przestępstwa politycznego lub gdy udzielenie pomocy może stanowić zagrożenie dla suwerenności, bezpieczeństwa, porządku publicznego albo innych istotnych interesów państwa będącego stroną Konwencji.

Inspirując się rozwiązaniami Rady Europy i Unii Europejskiej w polskim parlamencie również toczą się prace dotyczące bezpieczeństwa w cyberprzestrzeni. W ustawie o krajowym systemie cyberbezpieczeństwa, która weszła w życie w drugiej połowie 2018 roku, zapisano powstanie zespołu, w skład którego wejdą m.in. instytucje administracji rządowej i samorządowej oraz najwięksi przedsiębiorcy z kluczowych sektorów gospodarki. Będą tam także operatorzy usług kluczowych (OUK), czyli m.in. największe banki, firmy z sektora energetycznego czy przewoźnicy lotniczy oraz dostawcy usług kluczowych (DUC), czyli m.in. internetowych platform handlowych. Ponadto powstaną trzy zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego utworzone w Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV), Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (CSIRT NASK) oraz Ministerstwie Obrony Narodowej (CSIRT MON). Wszystko to dla sprawnego koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Polsce w sektorze zarówno publicznym, jak i prywatnym.

Unia Europejska w ramach wspólnotowych gwarancji ochrony cyberprzestrzeni bardzo poważnie traktuje również zagrożenie tzw. wojną hybrydową, czyli plany i strategie wojenne, które łączą działania konwencjonalne, nieregularne i cybernetyczne. Takie zdarzenia, postrzegane czasem jako wojna, są prowadzone bez oficjalnego wypowiedzenia i jej charakter często pozwala agresorowi na bezkarność. 6 kwietnia 2016 r. ogłoszono wspólny komunikat Parlamentu Europejskiego i Rady *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym odpowiedź Unii Europejskiej*, a 19 lipca 2017 r. sprawozdanie Parlamentu Europejskiego i Rady z realizacji wspólnych ram dotyczących przeciwdziałaniu zagrożeniom hybrydowym. Ponadto postanowiono, że w Helsinkach powstanie centrum do walki z zagrożeniami hybrydowymi, które działa od września 2017 roku. Jest to wspólna inicjatywa Unii Europejskiej i NATO, a wśród państw sygnatariuszy są Polska, Stany Zjednoczone, Wielka Brytania, Francja, Niemcy, Szwecja, Finlandia, Łotwa i Litwa [*UE i NATO…*].

Unia Europejska odnosi się także do kwestii związanych z zarządzaniem cyberprzestrzenią obejmujących m.in. problem neutralności sieciowej na rynku

komunikacji elektronicznej, przydzielanie adresów i nazw w internecie, działania związane z prawem autorskim czy niechcianą korespondencją. W lutym 2014 r. Komisja Europejska wystosowała do Parlamentu Europejskiego, Rady Europy, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów komunikat dotyczący zarządzania internetem, polityki wobec Internetu, a także roli Europy w kształtowaniu przyszłości zarządzania internetem [Chmielewski 2016]. W dokumencie rekomendowano model wielopłaszczyznowego i wielopodmiotowego zarządzania internetem, w którym żaden podmiot decydujący o kształcie sieci nie ma pozycji dominującej. Model taki uznają za najbardziej optymalny również Stany Zjednoczone Ameryki.

Dwa najistotniejsze obszary działań UE w zakresie międzynarodowego bezpieczeństwa i gwarancji nienaruszalności cyberprzestrzeni to regulacje ukierunkowane na zwalczanie cyberataków oraz mające na celu ochronę infrastruktury informatycznej. Działania w obu tych obszarach przewiduje przyjęta przez Parlament Europejski w lipcu 2016 r. Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (2016/1148/UE), zwana też dyrektywą NIS [Grzybowski 2016]. W życie weszła w sierpniu 2016 r., a państwa członkowskie mają dwadzieścia jeden miesięcy na jej implementację [Cuch 2017]. Zakres dyrektywy ogranicza się do dwóch typów podmiotów, tj. dostawców usług cyfrowych, w tym dostawców internetowych platform handlowych, wyszukiwarek internetowych i przetwarzania w chmurze oraz operatorów usług kluczowych [Żółw, Sawicka 2017].

Dyrektywa NIS nie odnosi się w sposób bezpośredni do bezpieczeństwa obywateli Unii Europejskiej, choć pośrednio niemal każdy obywatel w przypadku dokonania cyberprzestępstwa może ponosić konsekwencje niezabezpieczenia tych dwóch grup interesariuszy na swoim terenie. Dostawcy usług cyfrowych są wybierani bezpośrednio przez UE. Operatorów usług kluczowych wskazują natomiast państwa członkowskie samodzielnie, według listy sektorów wymienionych w dyrektywie, w sześciostopniowym procesie identyfikacji – albo wraz z implementacją dyrektywy, albo bezpośrednio po niej. Do obowiązków obu tych grup będzie należeć zastosowanie technicznych i organizacyjnych środków ochrony, adekwatnych do poziomu ryzyka oraz raportowanie o istotnych incydentach dotyczących naruszenia bezpieczeństwa.

KONKLUZJE

Optymalna struktura międzynarodowych gwarancji bezpieczeństwa w cyberprzestrzeni to wyzwanie, które musi być priorytetem dla wszystkich państw chcących chronić swoich obywateli przed cyberprzestępczością, cyberterroryzmem czy cyberwojnami. Wyzwaniami stojącymi przed współczesnym światem w dziedzinie cyberbezpieczeństwa jest konieczność intensyfikacji współpracy międzynarodowej, międzyresortowej oraz wypracowanie metod współdziała-

nia sektora rządowego z prywatnym. Ważnym elementem jest również budowa cybersuwerenności poszczególnych państw, tj. wyznaczenie granic, po których swobodnie i bezpiecznie będą mogli poruszać się obywatele.

Najważniejszym jej elementem powinna być powszechna edukacja w zakresie współczesnych rodzajów zagrożeń cyberprzestrzeni ze szczególnym uwzględnieniem kształcenia dzieci, młodzieży czy szkoleń pracowniczych oraz odpowiednia polityka kadrowa w sektorze zabezpieczeń teleinformatycznych. Poważne zaangażowanie w budowę ponadgranicznych gwarancji i norm stwarza szansę ograniczenia strat finansowych i niefinansowych oraz budowy systemu wspierającego działania poszczególnych państw, instytucji oraz osób w dziedzinie przeciwdziałania cyberprzestępczości. W powyższym zakresie wyzwania międzynarodowych wspólnot są jednym z najważniejszych elementów mogących zapewnić komfort życia wszystkim obywatelom, a budowa odpowiedzialnej i reagującej na postęp technologiczny ceberpolityki jest priorytetem, któremu trzeba sprzyjać i dawać podstawy do ciągłego rozwoju.

Title: International Safety Guarantees in Cyberspace

Summary: The development of cyberspace in the world and its impact on human life is more and more visible. Proper protection of all processes that can negatively affect people's lives is therefore an indispensable element that should accompany this development. Safe cyberspace is also closely related to the internal and external security of each country. The preparation of appropriate, international security guarantees in cyberspace is not only a challenge for individual countries, but above all for global institutions that provide peace. In Europe, the European Union and the Council of Europe should be the leaders in this respect. Lack of legal regulations regarding safe cyberspace is the possibility of exposing people to taking control over their privacy, data theft or other crimes. The implementation of European standards should therefore apply in every country. Governments should additionally emphasize social education and disseminate knowledge about threats in cyberspace. Coordinating these two activities gives hope that the expanding cyberspace in the future will not destroy people's lives.

Keywords: cyberspace, safety, European Union, legal regulations

BIBLIOGRAFIA

1. *About us* (a), http://www.eulisa.europa.eu/ [dostęp: 21.03.2018].
2. *About us* (b), https://www.cepol.europa.eu/who-we-are/european-union-agency-law-enforcement-training/about-us [dostęp: 21.03.2018].
3. *Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji* (ENISA), https://europa.eu/european-union/about-eu/agencies/enisa_pl [dostęp: 21.03.2018].
4. Becker K., *Jaka jest różnica między blogerką a influencerką*, 17.06.2017, https://www.harpersbazaar.pl/moda/3306/jaka-jest-roznica-miedzy-blogerka-a-influencerka [dostęp: 15.02.2018].
5. Bodył T., *Internet jest pełen naciągaczy. Nie daj się wykiwać*, 29.01.2018, https://www.money.pl/gospodarka/wiadomosci/artykul/internet-jest-pelen-naciagaczy-nie-daj-sie,7,0,2397191.html [dostęp: 10.02.2018].

6. Brodie B. (1949), *Strategy as a Science*, „World Politics", vol. 1. DOI: https://doi.org/10.2307/2008833.
7. Chmielewski Z. (2016), *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej", nr 2 (10).
8. Cuch A., *ABC cyberbezpieczeństwa na podstawie dyrektywy NIS*, http://rcb.gov.pl/abc-cyberbezpieczenstwa-na-podstawie-wymogow-dyrektywy-nis/ [dostęp: 21.03.2018].
9. *Czym jest Ognivo?*, http://www.centralnainformacja.pl/o-usludze/czym-jest-ognivo/ [dostęp: 10.02.2018].
10. Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, 01.2014, https://www.researchgate.net/publication/272818724_NATO_a_aspekty_bezpieczenstwa_w_cyberprzestrzeni [dostęp: 21.03.2018].
11. *Dziecko nie istniało, choroby nie było. Wyłudził niemal pół miliona złotych, stanie przed sądem*, 29.12.2017, https://www.tvn24.pl/wroclaw,44/zorganizowal-zbiorke-dla-nieistniejacego-antosia-jest-akt-oskarzenia,802255.html [dostęp: 18.02.2018].
12. *ECTEG*, http://www.ecteg.eu/ [dostęp: 21.03.2018].
13. *European Cybercrime Centre – EC3*, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [dostęp: 21.03.2018].
14. Gorwa R. (2017), *Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere*, University of Oxford.
15. Grzybowski M., *9 faktów o Dyrektywie NIS, które powinieneś znać*, 15.11.2016, https://www.cybsecurity.org/pl/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/ [dostęp: 21.03.2018].
16. *Hakerzy opublikowali zdjęcia pacjentów klinik chirurgii plastycznej. Domagali się okupu*, http://www.polsatnews.pl/wiadomosc/2017-05-30/hakerzy-opublikowali-zdjecia-pacjentow-klinik-chirurgii-plastycznej-domagali-sie-okupu/ [dostęp: 10.02.2018].
17. *History of Eurojust*, http://eurojust.europa.eu/about/background/Pages/History.aspx [dostęp: 21.03.2018].
18. Kawka W. (1939), *Policja w ujęciu historycznym i współczesnym*, Zakład Administracji i Prawa Administracyjnego U.S.B., Wilno, s. 3–5.
19. *Kolejny nieistniejący piłkarz podbija Internet*, http://www.zczuba.sport.pl/Zczuba/1,138263,6367781,Kolejny_nieistniejacy_pilkarz_podbija_Internet.html [dostęp: 02.02.2018].
20. *Komitet Wojskowy Unii Europejskiej*, https://pl.wikipedia.org/wiki/Komitet_Wojskowy_Unii_Europejskiej [dostęp: 21.03.2018].
21. Kotowski A., *Do sieci wyciekło ponad 10 mln haseł do polskich kont email*, 18.12.2017, https://pclab.pl/news76477.html [dostęp: 10.02.2018].
22. Kuchta M., *Dlaczego kłamiemy w mediach społecznościowych*, 12.05.2017, https://socialpress.pl/2017/05/dlaczego-klamiemy-w-mediach-spolecznosciowych/ [dostęp: 18.02.2018].
23. Kuchta M., *Oto Miquela – influencerka modowa, która prawdopodobnie jest… nierealna*, 15.02.2018, https://socialpress.pl/2018/02/oto-miquela-influencerka-modowa-ktora-prawdopodobnie-jest-nierealna/ [dostęp: 18.02.2018].
24. Makowski M., *Za modnym określeniem „fake news" stoi zwyczajne kłamstwo*, 01.04.2017 http://telewizjarepublika.pl/makowski-za-modnym-okresleniem-fake-news-stoi-zwyczajne-klamstwo,46595.html [dostęp: 10.02.2018].
25. Malak K. (2007), *Bezpieczeństwo jako kategoria i zjawisko społeczne*, „Piotrkowskie Zeszyty Międzynarodowe", nr 2, s. 91–95.
26. *Poważny wyciek informacji z firmy InPost – dane ponad 50 tysięcy osób, hasła*, https://zaufanatrzeciastrona.pl/post/powazny-wyciek-informacji-z-firmy-inpost-dane-ponad-50-tysiecy-osob/ [dostęp: 10.02.2018].

27. Röhrig W., Smeaton R., *Cyber Security and Cyber Defence in the European Union. Opportunities, Synergies and Challenges*, http://www.cybersecurity-review.com/articles/cyber-security-and-cyber-defence-in-the-european-union/ [dostęp: 21.03.2018].
28. Siwicki M. (2012), *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo", nr 7–8.
29. Skorupa A., *Co to jest BIK-Pass i czy opłaca się go uzyskać?*, 05.06.2014, https://www.zpetlikredytowej.pl/co-to-jest-bik-pass-i-czy-oplaca-sie-go-uzyskac [dostęp: 10.02.2018].
30. Stępniewska A. (2014), *Ściganie przestępstw popełnionych w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo*, Wardyński i Wspólnicy (red.), Warszawa.
31. *System informacyjny Schengen II*, https://www.mswia.gov.pl/pl/aktualnosci/10771,dok.html [dostęp: 20.03.2018].
32. *Eurodac*, https://pl.wikipedia.org/wiki/Eurodac [dostęp: 16.03.2018].
33. *Sztab Wojskowy Unii Europejskiej*, https://pl.wikipedia.org/wiki/Sztab_Wojskowy_Unii_Europejskiej [dostęp: 21.03.2018].
34. Wiśniewski B., Zalewski S., Podleś D., Kozłowska K. (2006), *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa.
35. *Uber ujawnił kradzież danych 57 milionów użytkowników*, http://tvn24bis.pl/tech,80/uber-ujawnil-kradziez-danych-57-milionow-uzytkownikow,792217.html [dostęp: 10.02.2018].
36. *UE i NATO tworzą centrum do walki z zagrożeniami hybrydowymi,* http://www.cyberdefence24.pl/577632,ue-i-nato-tworza-centrum-do-walki-z-zagrozeniami-hybrydowymi [dostęp: 21.03.2018].
37. Ziętal N., *Teraz możesz sprawdzić czy jesteś na liście dłużników*, 20.11.2009, http://www.nowiny24.pl/wiadomosci/podkarpacie/art/6063653,teraz-mozesz-sprawdzic-czy-jestes-na-liscie-dluznikow,id,t.html [dostęp: 10.02.2018].
38. Żółw H., Sawicka K., *Dyrektywa NIS – nowe wymogi dotyczące cyberbezpieczeństwa dla firm z kluczowych obszarów gospodarki*, 1.02.2017, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/dyrektywa-nis-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html [dostęp: 21.03.2018].
39. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.