Katarzyna Chałubińska-Jentkiewicz*

Cyberbezpieczeństwo – zagadnienia definicyjne

Streszczenie

W obecnych warunkach prawnych podejście regulatorów do zagadnienia cyberbezpieczeństwa wynika z utożsamiania tego rodzaju zjawiska z potrzebą przeciwdziałania atakom przede wszystkim nakierowanym na sieci teleinformatyczne. Stanowisko takie wydaje się jednak nieuzasadnione, zwłaszcza w kontekście analizy pojęcia cyberprzestrzeni i zagrożeń z nią związanych. Cyberbezpieczeństwo jest pojęciem odnoszącym się do zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają cyberprzestrzeni, jak i funkcjonowania w cyberprzestrzeni a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji. Na rzecz tego stanowiska przemawia również charakterystyka pojęcia cyberprzestępczości, obejmującego generalnie swoim zakresem zagrożenia, jakie pojawiają się w cyberprzestrzeni. Jednak powszechnie przyjmuje się, że świat cyfrowy powinien być uregulowany tak jak świat rzeczywisty. W artykule podjęto próbę uzasadnienia wskazanego powyżej stanowiska.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, informacja, inwigilacja, terroryzm

* Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, e-mail: kasiachalubinska@gmail.com.

Pojęcie cyberprzestrzeni

Współczesny świat opiera się na wymianie informacji, komunikacji interpersonalnej i indywidualizacji przekazu. Informacja zyskała całkiem nowe znaczenie, stała się ważnym czynnikiem w obiegu cyfrowym. Dotarcie do źródeł wiedzy stało się prostsze. Taki stan rzeczy doprowadził do wyodrębnienia się nowych pojęć w obszarze prawnym takich jak sieć teleinformatyczna oraz cyberprzestrzeń. Za autora tego pojęcia uznaje się Wiliama Gibsona. W swojej powieści zatytułowanej „Neuroromancer" napisał „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"[1]. Sieć teleinformatyczną można określić przez syntezę dwóch pojęć legalnych zawartych w polskim ustawodawstwie, są to: system teleinformatyczny i sieć telekomunikacyjna. Definicję systemu teleinformatycznego określa ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[2]. Według tej definicji system teleinformatyczny to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla tego rodzaju sieci telekomunikacyjnego urządzenia końcowego", natomiast pojęcie sieć telekomunikacyjna zostało zdefiniowane w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[3]. W myśl tej ustawy przez sieć telekomunikacyjną rozumiemy „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju"[4]. Można zatem powiedzieć, że sieć teleinformatyczna to wszelkiego rodzaju oprogramowanie, obsługiwane przez urządzenia posiadające do niego dostęp, które umożliwiają tworzenie, wymianę danych oraz informacji.

1 W. Gibson, *Neuromancer*, Warszawa 2009.
2 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz. 1204 ze zm.).
3 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2014 r., poz. 243 ze zm.), dalej pr.tel.
4 Art. 2 pr.tel.

Natomiast jedną z powszechnie stosowanych definicji cyberprzestrzeni jest ta sformułowana przez Departament Obrony USA. Według tej definicji 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 procesy oraz kontrolery”[5]. Definicja ta pozbawiona jest czynnika ludzkiego i skupia się wyłącznie na aspektach technicznych i technologicznych. Polska definicja pojęcia cyberprzestrzeni znajduje się w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[6]. Kolejną definicję legalną pojęcia cyberprzestrzeni zawiera ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym[7]. Według powyższej ustawy przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[8], wraz z powiązaniami pomiędzy nimi, oraz relacjami z użytkownikami[9]. Taką samą definicję legalną zawiera ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[10]. Ustawy te odnoszą się do zachowań w płaszczyźnie wirtualnej, w jakiej poruszają się podmioty prawa w momencie wystąpienia jednego z trzech stanów nadzwyczajnych. Przyjęta w Założeniach Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej koncepcja krajowego systemu cyberbezpieczeństwa obejmuje m.in. przebudowanie definicji cyberprzestrzeni i jej rozciągnięcie na sferę kluczowych operatorów funkcjonujących w sferze gospodarczej.

Przy tworzeniu wskazanej powyżej strategii przyjęto, iż dotychczasowa definicja cyberprzestrzeni jest ograniczona do sektora publicznego. Jednak wskazana powyżej definicja odnosi się do systemów teleinformatycznych,

5 *Słownik terminów wojskowych oraz powiązanych*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf tłumaczenie za: J. Wasielewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9, s. 225.

6 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).

7 Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).

8 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).

9 Art. 2 ust. 1a ustawy o stanie wyjątkowym.

10 Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).

które jak już wskazano stanowią zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Zatem definicja ta dotyczy wszystkich sytuacji odnoszących się do przetwarzania danych za pomocą systemów, a dodatkowo stanowi obszar powiązań systemów oraz relacji z użytkownikami, co wskazuje na szeroki zakres działania wszystkich użytkowników sieci i samych sieci. Oczywiście ustawodawca odniósł się do definicji samego systemu, przyjmując tę definicję za generalną.

Należy tu zauważyć, że definicja systemu teleinformatycznego na gruncie przepisów ustawy o świadczeniu usług drogą elektroniczną jest tożsama z definicją przyjętą w ustawie o informatyzacji[11], która reguluje kwestie stosunków cywilnoprawnych w handlu elektronicznym. Projektodawca założeń proponuje, aby definicja została wprowadzona do ustawy o krajowym systemie cyberbezpieczeństwa bądź ustawy o świadczeniu usług drogą elektroniczną, jednak równie właściwym miejscem byłaby przede wszystkim ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[12], gdzie w art. 3 ust. 2 zdefiniowano infrastrukturę krytyczną, przez którą należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna pojęciowo obejmuje także systemy sieci teleinformatycznych.

Można powiedzieć, że ład prawny i porządek publiczny przenikają do świata wirtualnego, i próbują znaleźć tam swoje odzwierciedlenie w formule cyfrowej. Pojęcie cyberprzestrzeni można bowiem sformułować jako syntezę wszystkich fizycznych i technicznych środków pozwalających na wymianę cyfrową drogą elektroniczną, oraz relacji użytkowników posiadających dostęp do jej zasobów. Całość tych zjawisk dzieje się w równoległej przestrzeni, która stanowi nowe pole dla ludzkich działań, na którą są przenoszone zachowania

11 System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu pr.tel.

12 Dz.U. z 2013 r., poz. 1166.

i rozwiązania stosowane w świecie realnym. Prawodawcy z różnych szczebli – zarówno międzynarodowego, jak i krajowego wprowadzają nowe regulacje. Doprowadziło to do dezaktualizacji zjawiska, jakim była bezkarność nielegalnego działania w sieci. Jednak podkreślić trzeba, iż cyberprzestrzeń pod względem przyjmowania czy tworzenia wzorców jest bardziej elastyczna niż rzeczywistość. Jej podatność niesie ze sobą udogodnienia, jak i zupełne wyzwania dla regulatora. Udogodnieniem jest łatwość wprowadzania regulacji adekwatnie do tych obowiązujących w świecie rzeczywistym, jednak przepisy tak ustalone często spotykają się z blokowaniem lub zwyczajną ignorancją ze strony użytkowników sieci teleinformatycznej, w szczególności ze względu na brak instrumentów dochodzenia roszczeń czy ścigania przestępczości. Każde społeczeństwo jest świadome możliwych zagrożeń, co powiązane jest z szeregiem doświadczeń i obserwacji, podczas gdy, w przypadku cyberprzestrzeni, która jest obszarem stosunkowo nowym wciąż nie jest możliwe określenie zamkniętego katalogu zagrożeń ani skonkretyzowanie grupy osób zagrożonych. Te zjawiska stanowią konsekwencję funkcjonowania w tzw. społeczeństwie informacyjnym. M. Castells przyjmuje, że jedną z ważniejszych cech społeczeństwa informacyjnego jest „nacisk na spersonalizowane urządzenia, interaktywność, sieciowość i bezustanne poszukiwanie nowych rozwiązań technologicznych[13]". Natomiast według J. Oleńskiego „Podstawowe cechy społeczeństwa informacyjnego, to m.in. globalny i totalny zakres procesów i systemów informacyjnych oraz możliwości globalnego i totalnego oddziaływania na społeczeństwa i gospodarki przez informacje"[14]. Przez obecność społeczeństwa informacyjnego w sieci teleinformatycznej zachodzi tzw. zjawisko transparentności jednostki, co oznacza, że przez wymianę informacji można bezproblemowo prześledzić aktywność konkretnej jednostki, co wzmaga jej podatność na zjawisko, jakim jest cyberprzestępczość[15]. Cyberprzestrzeń (cyberspace) już samą nazwą jest związana z cybernetyką tj. nauką o procesach sterowania oraz przekazywania i przekształcania informacji w systemach (maszynach, organizmach żywych i społeczeństwach)[16]. Analiza cech tej cybernetycznej przestrzeni prowadzi do wniosku, że jest to swoisty technosystem globalnej komunikacji społecznej,

13 M. Castells, *Społeczeństwo sieci*, Warszawa 2008, s. 23.
14 J. Oleński, *Ekonomika informacji*, Warszawa 2003, s. 33.
15 J. Sobczak, *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek (red.), *Demokracja w dobie globalizacji*, t. 2, *Aspekty teoretyczne*, Katowice 2008, s. 52–79; J. Sobczak, *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007, s. 193–213.
16 J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Warszawa 2008.

który odznacza się interaktywnością i multimedialnością. Został on ukształtowany w wyniku trzech procesów: integracji form przekazu i prezentacji informacji, która przyniosła ucyfrowienie i powstanie tzw. infosfery, konwergencji systemów informatycznych i telekomunikacyjnych oraz mediów elektronicznych, integracji tzw. technosfery, która doprowadziła w rezultacie do powstania globalnej zintegrowanej platformy teleinformatycznej[17]. Cyberprzestrzeń stanowi zatem swego rodzaju przestrzeń komunikacyjną tworzoną przez system powiązań internetowych. Jest obszarem zarówno kooperacji pozytywnej, prowadzącej do rozwoju w sferze edukacji, komunikacji społecznej, gospodarki narodowej, bezpieczeństwa powszechnego itp., jak i zjawisk negatywnych. Ta ostatnia aktywność może przybierać różną postać: 1) cyberinwigilacji (obostrzonej kontroli społeczeństwa za pośrednictwem narzędzi teleinformatycznych w państwach autorytarnych i totalitarnych); 2) cyberprzestępczości (wykorzystania cyberprzestrzeni do celów kryminalnych, w szczególności w ramach przestępczości zorganizowanej i przestępczości o charakterze ekonomicznym); 3) cyberterroryzmu (wykorzystania cyberprzestrzeni w działaniach terrorystycznych); 4) cyberwojny (użycia cyberprzestrzeni jako czwartego, obok ziemi, morza i powietrza, wymiaru prowadzenia działań wojennych[18].

Definicja cyberbezpieczeństwa

Jedna z definicji bezpieczeństwa przyjmuje, że „bezpieczeństwo jest pewnym stanem obiektywnym, polegającym na braku zagrożenia, odczuwanym subiektywnie przez jednostki i grupy. Oznacza to, że bezpieczeństwo składa się z dwóch elementów, obiektywnego i subiektywnego. Pierwszy z nich, mający charakter obiektywny, jest zewnętrzny w stosunku do jednostki, grupy społecznej, zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa[19]". Natomiast w ujęciu potocznym bezpieczeństwo m.in. oznacza stan, w którym jednostka ma poczucie pewności w sprawnie działającym systemie prawnym. Przeciwieństwem bezpieczeństwa jest stan zagrożenia. Bezpieczeństwa nie powinno się traktować jako zmiennej niezależnej,

17 P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
18 Ibidem.
19 H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Kraków 2004, s. 9–11.

gdyż ma ono charakter: dynamiczny i procesualny – ulega ciągłym zmianom pod wpływem złożonych i wieloczynnikowych zjawisk; subiektywny i obiektywny. Wynika to z faktu, iż postawy społeczne wobec bezpieczeństwa tworzą się wskutek wpływu danego zjawiska na jednostkę, grupę społeczną, społeczeństwo; uszeregowany, strukturalizowany; relatywny – zależny od szeregu czynników[20]. Wpływ na bezpieczeństwo mają wszystkie interakcje społeczne, a sama kultura bezpieczeństwa określa jaki jest stosunek danej społeczności do ryzyka, zagrożeń i bezpieczeństwa oraz ,jakie wartości w tym zakresie uważane są za istotne.

W przypadku zachowań związanych z funkcjonowaniem cyberprzestrzeni, również ze względu na jej globalny charakter taka zależność wydaje się nieoczywista. Bowiem działania w przestrzeni wirtualnej cechuje własna, specyficzna kultura zachowań jej użytkowników – społeczności wirtualnej. Dlatego należy przyjąć, że nowe zjawisko, jakim jest bezpieczeństwo wymagane w kontekście funkcjonowania sieci teleinformatycznych stwarza potrzebę uwzględnienia sytuacji, które nie muszą mieć odzwierciedlenia w świecie poza cyberprzestrzenią. Samo ustalone już pojęcie cyberbezpieczeństwa odnosić się może do ściśle określonego obszaru działań związanych z bezpieczeństwem informacji (zawartości sieci), bezpieczeństwem komunikowania (przekazu) oraz bezpieczeństwem samej sieci umożliwiających komunikowanie, jednak nie wyczerpuje wszystkich kwestii związanych z potrzebami ochrony przed niepożądanymi działaniami w cyberprzestrzeni.

Podstawowa konstrukcja internetu opiera się na otwartości zarówno architektury jego infrastruktury, jak i kultury jego twórców i użytkowników. Prostota i łatwość łączenia różnych komputerów pozwoliła na ogromne rozszerzenie liczby użytkowników, a otwarta filozofia jego kształtowania stworzyła z niego ogromnie atrakcyjne, interakcyjne na wielu poziomach medium[21]. Dlatego definicja cyberbezpieczeństwa wymaga uwzględnienia wielu zjawisk już zdefiniowanych. Takimi pojęciami pomocniczymi w definiowaniu cyberbezpieczeństwa są: bezpieczeństwo informacyjne, cyberprzestępczość.

20 J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] P. Tyrała (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000, s. 166.
21 T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

Bezpieczeństwo informacyjne w systemie cyberbezpieczeństwa

Bezpieczeństwem informacyjnym lub informacji możemy nazwać, według L. Ciborowskiego „obronę informacyjną, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych[22]". Kolejna definicja bezpieczeństwa informacyjnego M. Jabłońskiego i M. Mielus, została skonstruowana poprzez przedsięwzięcia, jakie należy zastosować, aby uzyskać stan bezpieczeństwa i składają się na nie: zapobieganie, odstraszanie, wskazywanie i ostrzeganie, wykrywanie, przygotowanie na sytuację awaryjną oraz reakcja na ewentualny atak[23]. Z kolei według M. Kaliskiego, A. Kierkowskiej oraz G. Tomaszewskiego „Bezpieczeństwo informacji to nie tylko zabezpieczenia fizyczne i techniczne zasobów informatycznych. Bezpieczeństwo informacji to przede wszystkim dążenie do zapewnienia i utrzymania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności informacji i systemów, w których są one przetwarzane. To także odpowiednio przeszkolony i świadomy zagrożeń personel, to odpowiednio zdefiniowane umowy z dostawcami, to również sformalizowane plany ciągłego działania i procedury postępowania. Bezpieczeństwo to proces – i jak każdy proces – wymaga ciągłego doskonalenia[24]". Bezpieczeństwem informacyjnym jest również każde działanie, system lub metoda, które zmierzają do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięci komputerów oraz sieci teleinformatycznych[25]. Obok pojęcia bezpieczeństwa informacyjnego wykształciło się pojęcie cyberbezpieczeństwa, które można zdefiniować jako wszelkie działania – metody, procedury, rozwiązania prawne – podejmowane przez właściwe w tym względzie podmioty, które to zmierzają do integralności zgromadzonych, przechowywanych i przetwarzanych

22 L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 186.
23 M. Jabłoński, M. Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej* [w:] M. Kwieciński (red.), *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, Kraków 2010, s. 25.
24 M. Kaliski, A. Kierkowska, G. Tomaszewski, *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] J. Kaczmarek, M. Kwieciński (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 34.
25 Ibidem, s. 71.

zasobów informacyjnych, zmierzające do ich ochrony przed niepożądanym, nieuprawnionym ujawnieniem, zmianą lub zniszczeniem[26]. Jednak, wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji a nie odnosi się do wielu innych zagrożeń, które nie muszą być związane bezpośrednio z jakimkolwiek nielegalnym wykorzystaniem informacji a mogą dotyczyć działań przestępczych wykorzystujących narzędzia informatyczne lub samą informację. Sytuacja taka może dotyczyć obrotu towarami zakazanymi, pornografii dziecięcej czy wyłudzania pieniędzy. Zatem, w pierwszej kolejności należy ustalić czym jest cyberprzestępczość i jakich sytuacji dotyczy.

Cyberprzestępczość

Ze względu na szczególny charakter tej sfery funkcjonowania społecznego wykształcił się nowy katalog czynów zabronionych określany pojęciem cyberprzestępczości[27]. Cyberprzestępczość definiowana jest jako rodzaj przestępczości, w której komputer jest albo narzędziem albo przedmiotem przestępstwa. Pojęcie to obejmuje wszelkie rodzaje przestępstw, które popełniono przy pomocy komputera lub sieci teleinformatycznych. Cyberprzestępstwo to czyn zabroniony popełniony w obszarze cyberprzestrzeni. Cyberatak jest to celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu. Sam atak na sieci informatyczne to działania podejmowane w celu zniekształcenia, uniemożliwienia wykorzystania, degradacji lub zniszczenia informacji przechowywanej w komputerze i/lub sieci komputerowej, albo komputera i/lub sieci komputerowej[28]. Pojęcie cyberprzestępczości, zwanej również „przestępczością internetową" jako określenie zabronionych prawem działań, dokonywanych za pomocą komputera w sieci internetowej lub przy jej wykorzystaniu, godzących m.in. w bezpieczeństwo wykorzystania technologii informatycznych, znalazło już swoje miejsce zarówno w doktrynie

26 P. Potejko, *Bezpieczeństwo informacyjne* [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009, s. 194.
27 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 351.
28 *Słownik terminów i definicji NATO*, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf, s. 105.

nauk prawnych, jak i wśród ekspertów zajmujących się bezpieczeństwem teleinformatycznym[29]. Można przyjąć, że cyberprzestępczość obejmuje trzy kategorie przestępstw: tradycyjne przestępstwa popełniane z wykorzystaniem sieci i systemów informatycznych, publikację nielegalnych treści w mediach elektronicznych, inne przestępstwa typowe dla sieci łączności elektronicznej. Dotychczas zidentyfikowano wiele ich postaci, a wśród nich[30]: 1) usługi finansowe on-line (m.in. propozycje udziału w wirtualnym hazardzie, tzw. oszustwa nigeryjskie); 2) cyberlaundering, tzn. wykorzystanie bankowości i handlu elektronicznego do tzw. „prania brudnych pieniędzy"; 3) naruszanie praw autorskich; 4) rozpowszechnianie pornografii i pedofilii; 5) praktyki nieuczciwej konkurencji (np. spamming); 6) nielegalny handel (np. antykami i dziełami sztuki, zagrożonymi gatunkami roślin i zwierząt, medykamentami, bronią, materiałami wybuchowymi, materiałami radioaktywnymi, wraz z instruktażem ich użytkowania); 7) szpiegostwo gospodarcze; 8) propagowanie treści nazistowskich, rasistowskich, itp.; 9) hacking – włamania do komputera; 10) nielegalne podsłuchy; 11) cybersquatting.

Niektóre czyny związane z cyberprzestępczością są odzwierciedleniem przestępstw i wykroczeń mających miejsce w świecie realnym, ale zostały odpowiednio zaadaptowane do warunków, jakie oferuje sieć teleinformatyczna[31]. Jednak zauważyć należy, że cyberprzestępczość nie musi być symptomem działania jednostki wyłącznie w sieci, bowiem jednostka może być narażona na zagrożenie w konsekwencji ataku na sieci teleinformatyczne. Zarówno sektor prywatny, jak i coraz bardziej obecne w sieci państwo i władza publiczna mogą stać się potencjalnymi ofiarami cyberprzestępczości. Państwo musi utrzymać tempo dynamicznej zmiany, podyktowanej rozwojem nowych technologii, ponieważ w ten sposób może ono realizować swoje zadania względem rozwoju gospodarczego i roli służebnej wobec obywatela[32]. Potrzeba informatyzacji, otwartość zasobów i dostęp do sieci i przetwarzanych przez nią danych i informacji to kluczowe procesy umożliwiające rozwój państwa i samej jednostki. Jednocześnie istotnym zadaniem władz publicznych jest zapewnienie bezpieczeństwa w sieci oraz tzw. cyberbezpieczeństwa, czyli sytuacji skutecznie wypierającej cyberprzestępczość.

29 M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary. Automatyka. Kontrola" 2009, nr 7.
30 W. Filipkowski, *Internet – przestępcza gałąź gospodarki*, „Prokurator" 2007, nr 1.
31 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo…*, s. 351–352.
32 S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994, s. 16.

Cyberinwigilacja

Kolejnym pojęciem, które wpływa na definicję cyberbezpieczeństwa jest cyberinwigilacja. Jest to również zjawisko pokrewne cyberterroryzmowi. Za jedną z postaci terroryzmu uznawany jest bowiem terroryzm państwowy, którego istotą, a zarazem celem działań terrorystycznych, jest wymuszenie posłuszeństwa wobec aparatu władzy[33]. Jest oczywiste, że proceder taki nie jest możliwy bez inwigilacji społeczeństwa, w szczególności członków opozycji niedemokratycznego reżimu. Obecnie, cyberprzestrzeń i elektroniczne środki komunikacji to instrument działań aparatu bezpieczeństwa. Może on przyjąć zarówno formę ograniczenia obywatelom dostępu do internetu i jego zawartości (np. spowolnienie sieci, brak dostępu do wyszukiwarek oraz stron światowych, cenzura stron internetowych, profilowanie), jak i stosowania środków teleinformatycznych w procesie inwigilacji masowej (np. podsłuchy, inwigilacja zachowań w sieciach telekomunikacyjnych). Obie techniki stanowią obecnie doskonałe narzędzie kontroli społeczeństwa lub jednostki. Początkowo wykorzystywane do działań marketingowych, dzisiaj stanowią źródło zagrożeń i stan niepewności funkcjonowania w cyberprzestrzeni. W konsekwencji cyberbezpieczeństwo będzie sytuacją, w której zarówno jednostka, jak i całe społeczeństwo i poszczególne jego grupy będą wolne od cyberinwigilacji.

Cyberterroryzm

Cyberterroryzm to zagrożenie szczególne cywilizacji, społeczeństwa informacyjnego, bezpieczeństwa narodowego i obywateli, wymaga przeciwdziałania i zdecydowanego zwalczania. Współczesny terroryzm odznacza się trzema charakterystycznymi cechami[34]. Po pierwsze, akty terrorystyczne są przeprowadzane w sposób umożliwiający uzyskanie przez nie międzynarodowego rozgłosu. Po drugie, cechuje je wysoki stopień zorganizowania grup terrorystycznych. Po trzecie wreszcie, organizacje terrorystyczne dysponują obecnie pokaźnym zasobem środków ekonomicznych i technicznych, wykorzystując na masową skalę narzędzia teleinformatyczne, w tym internet, do działań skierowanych przeciwko społeczeństwu oraz aparatowi państwowemu wrogich

33 K. Sławik, *Terroryzm. Aspekty prawno-międzynarodowe, kryminalistyczne i policyjne*, Poznań 1993, s. 114–130.
34 Ibidem.

krajów. Zdaniem amerykańskiego eksperta do spraw cyberbezpieczeństwa D.E. Denninga, „Cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien on skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczające szkody aby wywoływac poczucie strachu[35]". Zjawisko to jest przy tym obecnie najmniej przewidywalne, m.in. z uwagi na powszechne zastosowanie sieci teleinformatycznej będącej instrumentem oddziaływania zorganizowanych grup terrorystycznych na funkcjonowanie infrastruktury krytycznej państwa, a więc krajowych systemów cyberbezpieczeństwa: łączności, energetyki, transportu, zaopatrzenia w wodę, finansowych, itd. Metody korzystania przez zorganizowane grupy przestępcze i indywidualnych przestępców w działaniach cyberterrorystycznych to m.in. włamania do komputerów (hacking), włamania do systemów informatycznych dla osiągnięcia korzyści (cracking), wykorzystanie programu umożliwiającego wejście do serwera z pominięciem zabezpieczeń (back door), podsłuchiwanie pakietów między komputerami i przechwytywanie haseł i loginów (sniffing), podszycie się pod inny komputer (IP spoofing), wirusy i robaki komputerowe, bomby logiczne, wyłudzanie poufnych informacji (phishing)[36]. teleinformatycznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni. Jest oczywiste, że ze względu na szczególną szkodliwość społeczną cyberterroryzmu i zagrożenie, jakie stwarza dla współczesnego świata, spotyka się z wyraźną reakcją prawnokarną zarówno na gruncie prawa międzynarodowego, jak i ustawodawstwa krajowego. Zgodnie z art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[37] zdarzeniem o charakterze terrorystycznym jest sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[38], lub zagrożenie zaistnienia takiego przestępstwa. Zgodnie z § 20 przestępstwem

35 J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Warszawa 2008.

36 J. Szafrański, *Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.

37 Dz.U. z 2016 r., poz. 796.

38 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2019 r., poz. 1950 ze zm.).

o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: 1) poważnego zastraszenia wielu osób; 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu. Istotną grupę stanowią przestępstwa komputerowe, których podstawa prawna może stanowić podstawę odpowiedzialności za działania cyberterrorystyczne. W szczególności trzeba tutaj zwrócić uwagę na przestępstwa udaremniania lub znacznego utrudniania dostępu do informacji zapisanej na komputerowym nośniku informacji osobie do tego uprawnionej (sprawca podlega pozbawienia wolności do lat 3), oraz sabotażu komputerowego. W Kodeksie karnym został określony również typ przestępstwa polegającego na niszczeniu, uszkadzaniu, usunięciu lub bezprawnej zmianie zapisu istotnej informacji na komputerowym nośniku informacji, którym jest materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej[39]. W przypadku sabotażu komputerowego, przedmiotem ochrony prawnokarnej jest informacja, która jest dobrem szczególnie ważnym w dobie społeczeństwa informacyjnego. Za taki czyn należy uznać znaczenie powszechnej informacji dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, samorządowej lub innego organu państwowego, która musi mieć wymiar szczególny, a dotyczyć może: rozmieszczenia elementów infrastruktury obronnej państwa, systemów kierowania komunikacją kolejową, lotniczą, drogową i wodną. Czyn ten polega na niszczeniu, uszkadzaniu, usuwaniu lub zmianach zapisu informacji. Zatem w znaczeniu ścisłym pojęciem cyberterroryzmu należy określić działalność terrorystyczną prowadzoną wobec systemów teleinformatycznych, w celu zniszczenia lub modyfikacji zasobów informacyjnych znajdujących się w tych systemach, a w konsekwencji utraty życia, zdrowia lub mienia przez ofiary ataku terrorystycznego. Cyberterroryzm może też mieć miejsce w przypadku wykorzystywania cyberprzestrzeni i sieci teleinformatycznej do działań o charakterze terrorystycznym. W ujęciu szerokim natomiast, trzeba go utożsamiać z wszelkimi działaniami względem cyberprzestrzeni, w tym

39 M. Czyżak, *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1–2, s. 45.

również fizycznymi zamachami na infrastrukturę teleinformatyczną oraz aktywnością ideologiczną w internecie[40]. W konsekwencji zapewnieniem cyberbezpieczeństwa będzie ochrona cyberprzestrzeni, czyli zespół przedsięwzięć organizacyjno-prawnych, mający na celu zwalczanie cyberterroryzmu.

Zakończenie

Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[41] cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Jednak na pojęcie bezpieczeństwa w sieci czy cyberbezpieczeństwa składa się ochrona zasobów – danych, informacji, a ogólnie treści cyfrowych, ochrona sieci teleinformatycznych, urządzeń czyli komputerów, a także ochrona przesyłu treści za pomocą sieci, a więc samego procesu komunikowania. Należy dodać tu jeszcze czynnik ludzki, czyli ochronę użytkownika sieci i komputerów. Wciąż kluczem do działań stwarzających wszelkiego typu zagrożenia w cyberprzestrzeni jest kwestia wykorzystywania luk i błędów w narzędziach programistycznych. Z całą pewnością należy podkreślić, że istotnym elementem tego procesu wciąż pozostaje działanie człowieka. Prawo bezpieczeństwa informacyjnego dotyka zagadnień związanych z prawną ochroną systemu telekomunikacyjnego, który zawiera określone dane umożliwiające świadczenie usług, ochroną samych usług świadczonych drogą elektroniczną i związanych z nimi treści oraz baz danych, a także samych sieci, za pomocą których następuje przekaz takich usług[42]. Jednak elementem wspólnym podlegającym ochronie jest wartość o szczególnym charakterze – informacja. W przepisach prawnych ustawodawca podjął próbę zdefiniowania czynów przestępczych, gdzie dochodzi do naruszeń związanych z informacją i systemami, które te informacje przetwarzają, a także ustalenia zakresu odpowiedzialności za działania nielegalne. Jednak obok pojęcia bezpieczeństwa informacyjnego wykształciło się pojęcie cyberbezpieczeństwa, które można

40 P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
41 Dz.U. z 2018 r., poz. 1560.
42 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, s. 5.

zdefiniować jako wszelkie działania – metody, procedury, rozwiązania prawne – podejmowane przez właściwe w tym względzie podmioty, które zmierzają do integralności zgromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, zmierzające do ich ochrony przed niepożądanym, nieuprawnionym ujawnieniem, zmianą lub zniszczeniem[43]. Wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji a nie odnosi się do wielu innych zagrożeń, które nie muszą być związane bezpośrednio z jakimkolwiek nielegalnym wykorzystaniem cyberprzestrzeni a mogą dotyczyć działań przestępczych wykorzystujących narzędzia informatyczne – oprogramowania, komputery lub samą informację. Podobnie jak wskazana powyżej definicja cyberbezpieczeństwa przyjmująca je za odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy, która odnosi się do bezpieczeństwa sieci teleinformatycznej i usług świadczonych za ich pomocą (art. 2 pkt 4 ustawy o krajowym systemie). Cyberbezpieczeństwo jest pojęciem odnoszącym się do stanu zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają samej cyberprzestrzeni, jak i funkcjonowania w cyberprzestrzeni, a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji. Natomiast na rzecz tego stanowiska przemawia charakterystyka pojęcia samej cyberprzestępczości, cyberinwigilacji i cyberterroryzmu jako pojęcia obejmującego generalnie swoim zakresem zagrożenia, jakie pojawiają się w cyberprzestrzeni[44].

Bibliografia

Literatura

Castells M., *Społeczeństwo sieci*, Warszawa 2008.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Ciborowski L., *Walka informacyjna*, Toruń 1999.

Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary. Automatyka. Kontrola" 2009, nr 7.

43 P. Potejko, *Bezpieczeństwo*..., s. 194.

44 Zaznaczyć także trzeba, że jednym z wciąż podstawowych problemów dotyczących odpowiedzialności w sieci jest zagadnienie jurysdykcji terytorialnej, która znalazła zastosowanie w przepisach Konwencji o cyberprzestępczości. Problemy z ustaleniem osoby przestępcy a jak wiadomo większość przestępstw popełnianych jest w innych państwach niż faktyczne miejsce przebywania przestępcy utrudnia działania związane z efektywnością ścigania cyberprzestępczości.

Czyżak M., *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1–2.
Dworecki S., *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994.
Filipkowski W., *Internet – przestępcza gałąź gospodarki*, „Prokurator" 2007, nr 1.
Gibson W., *Neuromancer*, Warszawa 2009.
Goban-Klas T., *Cywilizacja medialna*, Warszawa 2005.
Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej* [w:] M. Kwieciński (red.), *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, Kraków 2010.
Kaliski M., Kierkowska A., Tomaszewski G., *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] J. Kaczmarek, M. Kwieciński (red.), *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010.
Kisielnicki J., *MIS. Systemy informatyczne zarządzania*, Warszawa 2008.
Korzeniowska H., *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Kraków 2004.
Oleński J., *Ekonomika informacji*, Warszawa 2003.
Potejko P., *Bezpieczeństwo informacyjne* [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009.
Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
Sławik K., *Terroryzm. Aspekty prawno-międzynarodowe, kryminalistyczne i policyjne*, Poznań 1993.
Sobczak J., *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007.
Sobczak J., *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek (red.), *Demokracja w dobie globalizacji*, t. 2, *Aspekty teoretyczne*, Katowice 2008.
Szafrański J., *Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?* [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009.
Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] P. Tyrała (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000.
Wasielewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Akty prawne

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2014 r., poz. 243 ze zm.).
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).
Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz. 1204 ze zm.).
Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).
Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2019 r., poz. 1950 ze zm.).

Cyber security – definition issues

Abstract

In the current legal conditions, the regulators' approach to the issue of cybersecurity results from the identification of this type of phenomenon with the need to counteract attacks primarily targeted at IT networks. This position, however, seems unfounded, especially in the context of analyzing the concept of cyberspace and the threats associated with it. Cybersecurity is a term referring to ensuring protection and counteracting threats that affect cyberspace, as well as functioning in cyberspace, and this applies to both the public and private sectors and their mutual relations. This position is also supported by the characteristics of the concept of cybercrime, which generally covers in its scope threats that appear in cyberspace. However, it is widely accepted that the digital world should be regulated just like the real world. The article attempts to justify the position indicated above.

Key words: cybersecurity, cyberspace, information, surveillance, terrorism