Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ALK
Akademia Leona Koźmińskiego
ORCID: 0000-0003-0188-5704
e-mail: kasiachalubinska@gmail.com

CYBERBEZPIECZEŃSTWO – ZAGADNIENIA DEFINICYJNE[1]

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

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"[2]. 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

[1] Artykuł ukazał się w „Cybersecurity and Law" nr 2(2) 2019 – zaktualizowany.
[2] W. Gibson, Neuromancer, Warszawa 2009.

usług drogą elektroniczną[3]. 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[4]. 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 energie elektromagnetyczną, niezależnie od ich rodzaju"[5]. Można zatem powiedzieć, że sieć teleinformatyczna to wszelkiego rodzaju oprogramowanie, obsługiwane przez urządzenia posiadające do niego dostęp, które umożliwiają tworzenie, wymianę danych oraz informacji.

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"[6]. 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[7]. Kolejną definicję legalną pojęcia cyberprzestrzeni zawiera ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym[8]. 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[9], wraz z powiązaniami pomiędzy nimi, oraz relacjami z użytkownikami"[10]. Taką samą definicję legalną zawiera ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[11]. Ustawy te odnoszą się do zachowań w płaszczyźnie wirtualnej, w jakiej poruszają się podmioty prawa

[3] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024, poz. 1513).
[4] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2024, poz. 34), dalej pr.tel.
[5] Art. 2 pr.tel.
[6] 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.
[7] 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).
[8] Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).
[9] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).
[10] Art. 2 ust. 1a ustawy o stanie wyjątkowym.
[11] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (j.t. Dz.U. 2017, poz. 1897).

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, 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 definicja przyjętą w ustawie o informatyzacji[12], 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[13], 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 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

[12] 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.
[13] Dz.U. z 2013 r., poz. 1166.

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 zupełnie 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[14]". 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"[15]. 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[16]. 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)[17]. Analiza cech tej cybernetycznej przestrzeni prowadzi do wniosku, że jest to swoisty technosystem globalnej komunikacji społecznej, 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 platform teleinformatycznej[18]. 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

[14] M. Castells, Społeczeństwo sieci, Warszawa 2008, s. 23.
[15] J. Oleński, Ekonomika informacji, Warszawa 2003, s. 33.
[16] 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.
[17] J. Kisielnicki, MIS. Systemy informatyczne zarządzania, Warszawa 2008.
[18] P. Sienkiewicz, Terroryzm w cybernetycznej przestrzeni, [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), Cyberterroryzm – nowe wyzwania XXI wieku, Warszawa 2009.

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[19].

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[20]". 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, 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[21]. 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.

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 umożliwiającej komunikowanie, jednak nie wyczerpuje wszystkich kwestii związanych z potrzebami ochrony przed niepożądanymi działaniami w cyberprzestrzeni[22]. Należy zaznaczyć, że bezpieczeństwo w cyberprzestrzeni jest niezbędnym elementem prawidłowego postępu naukowo-technicznego i jako takie określa potrzeby ochrony tego obszaru nie tylko z punktu widzenia użyteczności, ale również ze względu na przeciwdziałanie zupełnie nieznanym dotąd zagrożeniom. W dobie globalnej informatyzacji, także sfery publicznej, w warunkach rozwoju portali społecznościowych, wszechobecnego mailingu, czyli wiadomości rozsyłanych na wiele adresów e-mail, zgromadzonych w wielkich zasobach danych, często

[19] Tamże.
[20] H. Korzeniowska, Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji, Kraków 2004, s. 9-11.
[21] J. Szmyd, Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna [w:] P. Tyrała (red.), Zarządzanie bezpieczeństwem, Kraków 2000, s. 166.
[22] Zob. pojęcie cyberbezpieczeństwa [w:] Leksykon cyberbezpieczeństwa, (red.) K. Chałubińska-Jentkiewcz, Warszawa 2024, s. 53.

dochodzi do nieuprawnionych działań, które mogą stanowić naruszenie dóbr osobistych, prawa własności czy praw konsumenckich. Jednak coraz częściej pojawiają się także innego typu cyber-zagrożenia, które dotykają struktur władzy publicznej i samego Państwa. Współcześnie, kiedy strefa prywatności człowieka wolna od ingerencji osób trzecich stopniowo się kurczy, w jednakowym, a może nawet większym stopniu proces ten dotyka każdej sfery życia także gospodarczego. Zdaniem C. Banasińskiego cyberbezpieczeństwo można sprowadzić do „sposobu wolnego od zakłóceń gromadzenia, przetwarzania i wymiany informacji utrwalonych i przetwarzanych w sposób cyfrowy”[23]. Należy zatem przyjąć, że cyberbezpieczeństwo jest zjawiskiem interdyscyplinarnym, korzystającym z dorobku wielu innych dziedzin (w tym z różnych dziedzin prawa). Aby jednak wyodrębnić je z całego systemu prawa i administracji publicznej (w tym drugim przypadku przede wszystkim organizacyjnie i podmiotowo), konieczne jest określenie zakresu działania, jakiego sfera ta dotyczy (zarówno w sensie przedmiotowym, podmiotowym, organizacyjnym, jak i funkcjonalnym). Dopiero wówczas możliwe będzie usystematyzowanie przedstawionej problematyki. W naszym przekonaniu jest to zabieg niezbędny w obliczu rozwoju TIK i cyberprzestrzeni oraz zagrożeń z nimi związanych w szczególności dla obronności Państwa i bezpieczeństwa jednostki.

Przywołane określenie podkreśla aspekt funkcjonalny bezpieczeństwa cyberprzestrzeni, czyli działania mającego na celu ochronę tego środowiska oraz jego użytkowników. Postępująca cyfryzacja i automatyzacja kolejnych dziedzin życia sprawia, że z każdym dniem coraz większa liczba procesów pozbawionych cyfrowego wsparcia stałaby się niemożliwa do przeprowadzenia. Skutkami tych zmian, które coraz bardziej są widoczne, jest uzależnienie się społeczeństwa od cyberprzestrzeni. Uzależnienie to sprawia, że wymagana jest niezawodność infrastruktury teleinformatycznej, a co za tym idzie ochrona przed potencjalnymi atakami. Do sieci przenosi się także coraz większa część ludzkiej aktywności a łatwość dostępu do informacji, a także do technologii umożliwiających jej generowanie i rozpowszechnianie wpływa jednocześnie na stały wzrost podaży danych. Skokowo rośnie też globalna sieć agregująca wiedzę, informacje oraz dostęp do rozrywki i platform komunikacyjnych. W ciągu każdej sekundy internauci dokonują setek tysięcy operacji w różnego rodzaju serwisach społecznościowych, czy transakcyjnych. Z danych tych korzystają zautomatyzowane systemy przetwarzania danych (których nawet w skali globalnej wciąż jest za mało). Jak podaje J. Surma: „Dzienna średnia liczba użyć przeglądarki Google wynosi około 3,5 miliarda. Zakładając, że każde użycie pochodzi od innej osoby, to niemal co drugi człowiek na kuli ziemskiej dokonuje jednego wyszukiwania dziennie! Liczba użytkowników Facebooka to 25% populacji całego świata. W przypadku Polski prawie 70% całej populacji używa Google i niemal 60% jest użytkownikami Facebooka”[24]. Równocześnie niezwykle intensywnie rozwija się koncepcja internetu rzeczy

[23] C Banasiński, Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni [w:] Cyberbezpieczeństwo. Zarys wykładu, C. Banasiński (red.), Warszawa 2018. s. 33.

[24] J. Surma, Cyfryzacja życia w erze Big Data, Warszawa 2017, s.74; autor wskazuje jednocześnie, że: „Tak powszechne wykorzystanie Google’a, Facebooka i innych podobnych firm globalnej gospodarki ma niebagatelne znaczenie dla bezpieczeństwa poszczególnych państw i całego świata”.

(Internet of Things – IoT), w której otaczające nas urządzenia codziennego użytku stają się częścią transgranicznego systemu wymiany informacji. Świat cyfrowy to także przestrzeń, w której aktywnie i kreatywnie korzystając z nowych narzędzi, działają zorganizowane grupy przestępcze, udoskonalając nowe metody popełniania znanych przestępstw, a także tworząc ich całkiem nowe kategorie. W wymiarze geopolitycznym i instytucjonalnym to jednocześnie dla wielu krajów atrakcyjne miejsce do realizowania celów politycznych, zadań wywiadowczych czy swoistej projekcji siły. Działania w cyberprzestrzeni mogą być także charakter operacji militarnych. Wobec zmian cywilizacyjnych i nowych wyzwań wykonywanie podstawowych zadań takich jak zapewnienie wewnętrznego i zewnętrznego bezpieczeństwa, wymaga dostosowania do sytuacji, w której nowym polem działania jest cyberprzestrzeń, a zdolność do zapewnienia cyfrowego bezpieczeństwa obywateli oraz do zabezpieczenia własnych sieci i systemów stanowi podstawowy element bezpieczeństwa narodowego. W obliczu globalizacji bezpieczeństwo w cyberprzestrzeni stało się jednym z priorytetowych zadań w sferze wewnętrznej każdego państwa wpływając jednocześnie na bezpieczeństwo w wymiarze międzynarodowym. Każde poważne zaburzenie działania cyberprzestrzeni będzie wpływać na poczucie bezpieczeństwa obywateli, bezpieczeństwo obrotu gospodarczego, sprawność funkcjonowania instytucji sektora publicznego, a w konsekwencji również na ogólnie rozumiane bezpieczeństwo. W związku z tym konieczne stało się wdrożenie rozwiązań prawnych umożliwiających zorganizowanie skutecznego i sprawnego systemu ochrony zasobów informacyjnych podmiotów publicznych, przedsiębiorców, a także obywateli. Jednym z obszarów jaki został częściowo uregulowany przez prawo, a który można wyróżnić w systemie prawa oraz w obowiązkach administracji publicznej jest cyberbezpieczeństwo.

W dziedzinie cyberbezpieczeństwa pojawiają się takie określenia jak bezpieczeństwo informacji, bezpieczeństwo sieci i systemów informatycznych, bezpieczeństwo teleinformatyczne, bezpieczeństwo cybernetyczne.

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”[25]. Dlatego definicja cyberbezpieczeństwa wymaga uwzględnienia wielu zjawisk już zdefiniowanych albo będących w procesie definiowania. Takimi pojęciami pomocniczymi w definiowaniu cyberbezpieczeństwa są: bezpieczeństwo informacyjne, cyberprzestępczość, cyberterroryzm, cyberinwigilacja i dezinformacja.

W państwach zaangażowanych w budowę społeczeństwa informacyjnego, bezpieczeństwo cyberprzestrzeni uznawane jest za jedno z najpoważniejszych wyzwań w systemie bezpieczeństwa narodowego. Odnosi się ono zarówno do bezpieczeństwa całej instytucji państwa jak i poszczególnych obywateli. Istotne znaczenie dla zapewnienia cyberbezpieczeństwa ma prawidłowe funkcjonowanie administracji publicznej. W ostatnich latach dokonała się także ewolucja w rozumieniu

[25] T. Goban-Klas, Cywilizacja medialna, Warszawa 2005, s. 151.

pojęcia bezpieczeństwa narodowego pod względem przedmiotowym. Zauważono znaczenie nie tylko aspektów militarnych, czy politycznych, ale także m.in. ekonomicznych, kulturowych, ekologicznych i ideologicznych.

Wzrost znaczenia cyberprzestrzeni w funkcjonowaniu wielu obszarów państwa i społeczeństwa doprowadził do tworzenia narodowych i międzynarodowych strategii bezpieczeństwa cyberprzestrzeni oraz rozbudowy systemów zarządzających cyberbezpieczeństwem.

Legalna definicja wprowadzona ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[26], kluczowe znaczenie nadaje terminowi „odporność". Zgodnie z art. 2 pkt 4 ww. ustawy, cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Definicja ta została oparta na definicji „bezpieczeństwa sieci i systemów informatycznych" określoną w art. 4 pkt 2 dyrektywy 2016/1148[27], zgodnie z którą „bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne." W dyrektywie NIS 2[28] w art. 6 pkt 2 "bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Dyrektywa NIS 2 wprowadza definicję cyberbezpieczeństwa, które zgodnie z art. 6 pkt 3 oznacza cyberbezpieczeństwo zdefiniowane w art. 2 pkt 1 rozporządzenia (UE) 2019/881. Według tej definicji "cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami[29].

---

[26] Dz.U. z2018 r., poz. 1560.

[27] Dyrektywa 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 (Dz.Urz.UE.L 2016 Nr 194, s. 1); W rozumieniu przepisów dyrektywy „bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne

[28] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, s. 80).

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, s. 15).

Prowadząca w kierunku zaakcentowania działania i procesów zmierzających do zapewnienia cyberbezpieczeństwa jest definicja sformułowana w dokumentach UE. W słowniku pojęć związanych z funkcjonowaniem jednolitego rynku cyfrowego. Zgodnie z nią cyberbezpieczeństwo „odnosi się do zabezpieczeń i działań dostępnych w celu ochrony domeny cybernetycznej, zarówno w sferze cywilnej, jak i wojskowej, przed zagrożeniami, które są powiązane lub które mogą zaszkodzić jego współzależnym sieciom i infrastrukturze informacyjnej. Cyberbezpieczeństwo dąży do zachowania dostępności i integralności sieci i infrastruktury oraz poufności informacji w nich zawartych. Pojęcie cyberbezpieczeństwo obejmuje także środki zapobiegania i egzekwowania prawa w celu zwalczania cyberprzestępczości”[30].

W funkcjonalnym rozumieniu cyberbezpieczeństwa wskazuje się, iż nie chodzi tu o istniejący lub pożądany stan, lecz o „nieustający proces”, czyli działania podejmowane przy pomocy środków technicznych i nietechnicznych dla ochrony cyberprzestrzeni, w tym urządzeń, podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk, umożliwiających obywatelom lepszą ochronę ich informacji. oprogramowania oraz informacji lub danych”[31]. Takie dynamiczne ujęcie cyberbezpieczeństwa przyjęto także w przywoływanej już Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej stwierdzając, że jest to „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 8 dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni.

Funkcjonalny charakter ma także społecznościowa definicja zawarta w słowniku Cybrary określająca cyberbezpieczeństwo jako „procesy stosowane w celu ochrony i zabezpieczenia zasobów będących nośnikiem informacji o organizacji przed kradzieżą lub atakiem”[32]. Kompleksowe rozumienie terminu cyberbezpieczeństwo proponuje się w słowniku amerykańskiego Department of Homeland Security, według którego należy je definiować w sensie ścisłym jako działalność lub proces, umiejętność lub zdolność, albo stan, w którym systemy informacyjne i komunikacyjne są chronione i/lub bronione przed uszkodzeniem, nieuprawnionym użyciem, modyfikacją lub wykorzystaniem. Dostępna jest też definicja rozszerzona obejmująca strategie,

[30] Digital Single market Glossary, https://ec.europa.eu/digital-single-market/glossary, w oryginale: “Cyber security commonly refers to the safeguards and actions available to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. The term cyber security also covers prevention and law enforcement measures to fight cybercrime.”

[31] O. Wasiuta, R. Klepka, R.Kopeć, Vademecum bezpieczeństwa, Kraków 2018, s. 223.

[32] Cyber Security are the processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. It requires extensive knowledge of the possible threats such as Virus or such other malicious objects. Identity management, risk management and incident management form the crux of cyber security strategies of an organization, https://www.cybrary.it/glossary/c-the-glossary/cyber-security/ dostęp 11.10.2023 r.

polityki i standardy dotyczące bezpieczeństwa cyberprzestrzeni i działania w cyberprzestrzeni obejmujące pełny zakres redukcji zagrożeń, zmniejszania podatności na zagrożenia, odstraszania, zaangażowania międzynarodowego, reagowania na incydenty, odporności oraz polityk i działań związanych z odzyskiwaniem sprawności, w tym operacje w sieciach komputerowych, zapewnienie informacji, egzekwowanie prawa, dyplomacja, misje wojskowe i wywiadowcze, dotyczące bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej[33]. Jeśli chodzi o zakres cyberbezpieczeństwa należy podkreślić, iż w odniesieniu do warstwy społecznej cyberprzestrzeni, państwo może regulować działania cybernetyczne podejmowane przez podmioty znajdujące się na jego terytorium, w tym zarówno osoby fizyczne jak i prawne. Na przykład, państwo może kryminalizować zamieszczanie w Internecie takich materiałów, jak pornografia dziecięca czy treści wzywające do przemocy. Należy pamiętać, że państwowa cenzura lub ograniczenia komunikacji i działalności w Internecie podlegają obowiązującemu międzynarodowemu prawu praw człowieka[34].

Wśród licznych typologii na uwagę zasługuje zwłaszcza ta zaproponowana przez M.Lakomego, który z punktu widzenia bezpieczeństwa państwa podzielił zagrożenia na ustrukturalizowane i nieustrukturalizowane. Pierwsze charakteryzują się wysokim stopniem organizacji ich źródeł, zaawansowaniem technicznym oraz z punktu widzenia atakującego, dominacją motywacji politycznych, wojskowych, religijnych oraz gospodarczych, a zaliczyć do nich można: cyberterroryzm, cyberszpiegostwo i operacje zbrojne w cyberprzestrzeni. Zagrożenia nieustrukturalizowane odznaczają się zaś niskim poziomem organizacji, stanowiąc z reguły mniejsze zagrożenie dla bezpieczeństwa państwa, cechując się dominacją motywacji politycznych, społecznych oraz indywidualnych. Autor zalicza do nich: haking, haktywizm, „haktywizm patriotyczny" i cyberprzestępczość sensu stricto[35]. Zagrożenia dla cyberbezpieczeństwa można także podzielić ze względu na: podmiot: przestępcy, terroryści, podmioty państwowe, motywację: chęć zysku, chęć wywarcia nacisku politycznego, chęć uzyskania informacji, chęć osiągnięcia przewagi militarnej, forma żartu, chęć zaistnienia w określonym środowisku, zdobycia popularności czy rozgłosu. Cyberzagrożenie to wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich

[33] W oryginale: „Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure." https://niccs.us-cert.gov/about-niccs/glossary#C (dostęp r.)

[34] Manual Talliński tłumaczenie na zlecenie ACPC.

[35] M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015, s. 137.

systemów oraz innych osób[36]; *modus operandi*: działanie doraźne lub długofalowe, działanie z rozgłosem lub ukryte"[37]. Należy oddać, iż agresja jako działanie określone w rezolucji ZO NZ nr 3314 z 1974 roku, czyli użycie siły zbrojnej przez państwo przeciwko integralności terytorialnej lub niezawisłości politycznej drugiego państwa, albo w jakikolwiek inny sposób niezgodny z Kartą Narodów Zjednoczonych może mieć miejsce także w cyberprzestrzeni[38]. Wówczas mówimy o akcie agresji w cyberprzestrzeni.

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"[39]. Dlatego definicja cyberbezpieczeństwa wymaga uwzględnienia wielu zjawisk już zdefiniowanych. Takimi pojęciami pomocniczymi w definiowaniu cyberbezpieczeństwa są: bezpieczeństwo informacyjne, cyberiwigilacja, cyberterroryzm, cyberprzestępczość a także dezinformacja.

Podsumowując należy stwierdzić, że cyberbezpieczeństwo, zważywszy na definicję legalną cyberprzestrzeni (systemy teleinformatyczne i ich użytkownicy), która dotyczy ochrony systemów teleinformacyjnych, nie obejmuje samych relacji między użytkownikami. Dlatego w budowaniu systemu cyberbepieczeństwa RP, także w kontekście prawnym, regulacyjnym brać pod uwagę także te zagadnienia, uwzględniając poufność, integralność, legalność przetwarzanych treści oraz usług e-commerce.

---

[36]Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, s. 15).

[37]O. Wasiuta O., R. Klepka, R. Kopeć, Vademecum…, op.cit., s. 223.

[38] Zob. Rezolucja Zgromadzenia Ogólnego ONZ nr 3314 (XXIX) w sprawie definicji agresji, Nowy Jork, 14 grudnia 1974 r. [w:] M. Flemming, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Zbiór dokumentów, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Zbiór dokumentów, uzupełnienie i red. M. Gąska, E. Mikos-Skuza, Warszawa 2003, s. 90.

[39] 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[40]". 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[41]. 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[42]". 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[43]. 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 zasobów informacyjnych, zmierzające do ich ochrony przed niepożądanym, nieuprawnionym ujawnieniem, zmianą lub zniszczeniem[44]. Jednak, wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji a nie odnosi się 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,

[40] L. Ciborowski, Walka informacyjna, Toruń 1999, s. 186.
[41] M. Jabłoński, M. Mielus, Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej, [w:] M. Kwieciński (red.), Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane, Kraków 2010, s. 25.
[42] 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.
[43] Tamże, s. 71.
[44] P. Potejko, Bezpieczeństwo informacyjne [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Bezpieczeństwo państwa, Warszawa 2009, s. 194.

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[45]. 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 cyberprzestrzeń. Cyberatak jest to celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzenie, 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[46]. 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 nauk prawnych, jak i wśród ekspertów zajmujących się bezpieczeństwem teleinformatycznym[47]. 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[48]: 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

[45] K. Chałubińska-Jentkiewicz, M. Karpiuk, Prawo nowych technologii. Wybrane zagadnienia, Warszawa 2015, s. 351.
[46] Słownik Terminów i Definicji NATO, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf, s. 105.
[47] M. Czyżak, Spamming i jego karalność w polskim systemie prawnym, „Pomiary. Automatyka. Kontrola" 2009, nr 7.
[48] W. Filipkowski, Internet – przestępcza gałąź gospodarki, „Prokurator" 2007, nr 1.

odpowiednio zaadaptowane do warunków jakie oferuje sieć teleinformatyczna[49]. 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[50]. 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.

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[51]. 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 zwalczanie. Współczesny terroryzm odznacza się trzema charakterystycznymi cechami[52]. Po pierwsze, akty terrorystyczne są przeprowadzane w sposób umożliwiający uzyskanie przez

[49] K. Chałubińska-Jentkiewicz, M. Karpiuk, Prawo..., s. 351-352.
[50] S. Dworecki, Zagrożenia bezpieczeństwa państwa, Warszawa 1994, s. 16.
[51] K. Sławik, Terroryzm. Aspekty prawno-międzynarodowe, kryminalistyczne i policyjne, Poznań 1993, s. 114-130.
[52] Tamże.

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 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[53].” 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)[54]. 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 prawno-karną zarówno na gruncie prawa międzynarodowego i jaki i ustawodawstwa krajowego. Zgodnie z art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[55] 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[56], lub zagrożenie zaistnienia takiego przestępstwa. Zgodnie z § 20 przestępstwem 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

[53] J. Kisielnicki, MIS. Systemy informatyczne zarządzania, Warszawa 2008.
[54] J. Szafrański, Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?, [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), Cyberterroryzm – nowe wyzwania XXI wieku, Warszawa 2009.
[55] Dz.U. z 209 r., poz. 796
[56] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tj. Dz.U. z 2019 r., poz. 1950 ze zm.).

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 szczególność 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 podlegającego 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 cyfrowe lub analogowej[57]. W przypadku sabotażu komputerowego, przedmiotem ochrony prawno karnej 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 również fizycznymi zamachami na infrastrukturę teleinformatyczną oraz aktywnością ideologiczną w internecie[58]. W konsekwencji zapewnieniem cyberbezpieczeństwa będzie ochrona cyberprzestrzeni, czyli zespół przedsięwzięć organizacyjno-prawnych, mający na celu zwalczanie cyberterroryzmu.

DEZINFORMACJA

Dezinformacja to zjawisko znane od zarania dziejów, jednak w powiązaniu z nowymi technologiami cyfrowymi, stanowi ogromne zagrożenie dla bezpieczeństwa jednostek i państw. Dezinformacja jest zjawiskiem, które godzi w samo serce demokracji, ponieważ wykorzystuje jej niezbędny element – wolność słowa[59]. Z tego powodu tak trudnym procesem będzie regulacja międzynarodowa. Proponowane rozwiązanie pozwala na zwalczanie

[57] M. Czyżak, Wybrane aspekty zjawiska cyberterroryzmu, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1-2, s. 45.
[58] P. Sienkiewicz, Terroryzm w cybernetycznej przestrzeni, [w:] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), Cyberterroryzm – nowe wyzwania XXI wieku, Warszawa 2009.
[59] Zob. pojęcie dezinformacji [w:] Leksykon cyberbezpieczeństwa, (red.) K. Chałubińska-Jentkiewicz, Warszawa 2024, s. 98.

dezinformacji, przy zastosowaniu jej największego atutu – powszechności, którą gwarantuje środowisko internetowe[60].

Zwalczanie dezinformacji w mediach społecznościowych staje się jednym z podstawowych celów działań na rzecz cyberbezpieczeństwa. To kolejny nowy obszar tworzący nowe środowisko zagrożeń ze strony mediów. Chociaż prowadzone przez państwo kampanie dezinformacyjne w mediach społecznościowych to stosunkowo nowe zjawisko, a ich oddziaływanie poprzez zastraszanie i dyskredytowanie może stanowić zagrożenie dla jednostki, określonych grup społecznych czy państw, wciąż istnieją ograniczone dowody na to, że mogą wpływać na poglądy czy systemy wartości. Jednak już same kampanie dezinformacyjne w mediach społecznościowych wyraźnie odnoszą sukces operacyjny. Było to szczególnie widoczne w przypadku wyborów prezydenckich w Stanach Zjednoczonych, które odbyły 8 listopada 2016 roku. Podczas poprzedzającej je kampanii wyborczej publikowano fałszywe informacje, które zdobywały w Internecie znacznie większą popularność niż prawdziwe wiadomości. Przykładem „fake newsa" z tego okresu może być komunikat informujący o Papieżu Franciszku[61]. Technika dezinformacyjna, jaka jest fake news stała się jedną z najbardziej popularnych metod walki w informacyjnej wojnie między Ukrainą i Rosją. W zasadzie, nieprawdziwe fakty są używane wśród serwisów społecznościowych Rosji dla rozpalenia nienawiści u Rosjan w stosunku do ludności Ukrainy i prowadzonej polityki nienawiści. Podobne techniki stosuje się wobec sojuszników Ukrainy. Studenci jednego z najpopularniejszych uniwersytetów na Ukrainie stworzyli stronę internetową, na której walczą z rosyjską propagandą – „StopFake"[62] Strona do weryfikacji informacji została uruchomiona 2 marca 2014 roku. Na pomysł jej uruchomienia wpadli wykładowcy, absolwenci oraz studenci Mohylańskiej Szkoły Dziennikarstwa i kursu dla dziennikarzy i redaktorów Digital Future of Journalism. Do projektu dołączyli dziennikarze, redaktorzy, programiści, tłumacze i wszyscy, którym nie był obojętny los Ukrainy i jej narodu w czasie okupacji Krymu i wojny w Donbasie. Projekt stał się serwisem informacyjnym, w którym wszelkie formy kremlowskiej propagandy poddawane są wnikliwej analizie.

Sam przekaz dezinformacyjny to informacja tworzona z intencją generalnej szkody bądź także bezmyślne powtarzanie niesprawdzonych informacji. Przekazy te można podzielić, korzystając z dwóch kryteriów łącznie: stosunku do prawdy oraz intencji tworzenia i rozpowszechniania. Wyróżniamy kilka podstawowych gatunków, które mają swoje własne, odróżniające cechy. Mylne informacje (misinformation) to fałszywe wiadomości, które są rozpowszechniane bez złej intencji. Ta kategoria obejmuje fałszywe łączenie faktów (false connection), jeśli przykładowo tytuł, czy ilustracje nie są zgodne z treścią tekstu; wprowadzającą w błąd treść (misleading content) lub wprowadzające w błąd użycie informacji.

[60] Na podstawie K. Chałubińska-Jentkiewicz, Prawne granice dezinformacji w środkach społecznego przekazu, Toruń 2023.
[61] Papież Franciszek popierał kandydaturę Donalda Trampa pod czas wyborów Stanach Zjednoczonych w 2016 roku.
[62] https://www.stopfake.org/uk/golovna/(dostęp: 27.01.2025.)

Z drugiej strony, możliwe jest niegodziwe użycie informacji (malinformation), czyli udostępnianie prawdziwych informacji w celu dokonania szkody. W tej kategorii mieszczą się cyberataki, czy mowa nienawiści.

Jednak dezinformacja to przede wszystkim akt, w ramach którego fałszywe informacje są tworzone i udostępniane w złej wierze lub prawdziwe informacje przekazywane są w taki sposób by wywołać fałszywe opinie. Sama dezinformacja także może mieć różny charakter. Możemy wymienić sfabrykowaną treść (fabricated content) – gdy nowa treść jest zupełnie fałszywa i stworzona, żeby oszukać odbiorcę i wyrządzić szkodę; zmanipulowaną treść (manipulated content) – kiedy prawdziwa informacja lub obraz są zniekształcone, żeby oszukać odbiorcę; fałszywą treść (imposter content) – jeśli fałszywie powołuje się na prawdziwe źródła oraz fałszywy kontekst (false context) – kiedy prawdziwa treść jest ulokowana w fałszywym kontekście. Jeszcze innym obliczem dezinformacji jest prowadzenie polityki informacyjnej mającej na celu podważanie atrybutów danego państwa, autorytetu jego władzy publicznej. W tym sensie dezinformacja, bardzo często jednocześnie jako akt agresji w cyberprzestrzeni, staje się elementem wojny informacyjnej.

Oficjalną unijną definicję dezinformacji opracował zespół ekspertów z krajów członkowskich Unii Europejskiej. Zgodnie z tą definicją, dezinformacja to „fałszywa, niedokładna lub wprowadzająca w błąd informacja, stworzona, zaprezentowana i rozpowszechniana dla zysku lub rozmyślnego spowodowania szkody publicznej”[63]. Zgodnie z powyższą definicją, dezinformacja jest działaniem celowym, zmierzającym do wywołania określanej reakcji społecznej, politycznej czy też gospodarczej. Dezinformacja podważa zaufanie do instytucji publicznych oraz szkodzi demokracjom przez utrudnianie obywatelom podejmowania świadomych decyzji. Szkoda publiczna obejmuje zagrożenia dla demokratycznych procesów politycznych i kształtowania polityki oraz dla dóbr publicznych, takich jak ochrona zdrowia obywateli UE, środowisko naturalne lub bezpieczeństwo. Dezinformacja nie obejmuje błędów sprawozdawczych, satyry i parodii ani wyraźnie oznaczonych stronniczych wiadomości i komentarzy.

Nieprawdziwe informacje sieją niepewność oraz przyczyniają się do napięć społecznych, co może mieć poważne konsekwencje szczególne dla bezpieczeństwa obywateli. Rozwój nowoczesnych technologii sprawił, że takie nieprawdziwe informacje z łatwością rozprzestrzeniają się na skalę globalną[64]. Wraz z rozwojem nowoczesnych technologii, powstały również nowe formy rozpowszechniania nieprawdziwych informacji. Obecnie, przy pomocy sztucznej inteligencji można wykreować również sztuczne wideo, tzw. „deepfake”. Wideo to polega na podmienieniu twarzy albo ciała konkretnej osoby na dowolną inną postać. Dzięki temu, można zmienić wypowiedź osoby, a także jej ruchy ciała. Po raz pierwszy sformułowaniem „deepfake”, pojawiło się w 2017 roku. Był to pseudonim użytkownika, który przy pomocy sztucznej inteligencji, tworzył i publikował filmy pornograficzne z wykorzystaniem

[63]https://www.cyberdefence24.pl/ue-unijna-definicja-dezinformacji-i-nowy-kodeks-postepowania-dla-mediow (dostęp: 27.01.2025.).

[64] Krajowa Rada Radiofonii i Telewizji, Fake news – dezinformacja online. Próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski, Warszawa 2020, s. 7.

wizerunków znanych gwiazd. Deepfake polega nie tylko na podmianie obrazu, może być również podłożony dźwięk, naśladujący głos konkretnej osoby[65]. Technologia deepfake niesie za sobą wiele zagrożeń, gdyż może być ona wykorzystywana do manipulowania opinią publiczną. Wraz z rozwojem tej technologii, takie fałszywe filmy stają się coraz trudniejsze do wykrycia[66]. Nie istnieją również uregulowania prawne, które ograniczałyby korzystanie z tej technologii. W związku z tym istnieje niepewność co do legalności publikowania oraz ewentualnych sankcji za udostępnianie nieprawdziwych informacji i sztucznie spreparowanych przekazów audio wideo.

W polskim systemie prawnym nie ma obecnie jednorodnej regulacji dotyczącej definiowania terminu dezinformacji. Zagadnienia związane z rozpowszechnianiem takich informacji w przestrzeni publicznej, są uregulowane w różnych aktach prawnych, przede wszystkim w ustawie z dnia 26 stycznia 1984 r. Prawo prasowe, w której zostały uregulowane zagadnienia związane z prasową działalnością wydawniczą i dziennikarską. W tym kontekście oczywiście te unormowania odnoszą się do wąskiej strefy prasy internetowej. Art. 6 ust. 1 wyżej wymienionej ustawy, stanowi o tym, że prasa zobowiązana jest do prawdziwego przedstawiania omawianych zjawisk. Dziennikarz natomiast jest zobowiązany do starannego i rzetelnego zbierania oraz wykorzystywania materiałów prasowych, w szczególności powinien sprawdzać czy uzyskane wiadomości są zgodne z prawdą lub podać ich źródło (art. 12 ust. 1). Publikowanie w prasie nieprawdziwych informacji nie podlega, co do zasady, karze. Redaktor, autor albo inna osoba, która opublikowała materiał prasowy, ponosi natomiast odpowiedzialność cywilną za naruszenie praw wynikające z opublikowania materiału prasowego. Publikacja materiału prasowego, nawet wtedy gdy jest prawdziwa, może naruszać dobra osobiste osoby fizycznej lub prawnej. W momencie, gdy okaże się, że opublikowane informacje są nieprawdziwe, to odpowiedzialność dziennikarza będzie zależała od ustalenia, czy przy zbieraniu materiału, zachował należytą staranność oraz rzetelność i czy mógł powziąć wątpliwość co do wiarygodności swoich źródeł informacji[67]. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, reguluje natomiast kwestie związane z odpowiedzialnością usługodawców, świadczących usługi na odległość.

Naturalnym środowiskiem działań dezinformacyjnych (czy też dezinformujących) jest chaos informacyjny oraz nacechowanie emocjonalne przekazów medialnych, w ramach których często ścierają się różne grupy interesu. Jeżeli do tego mamy do czynienia z dynamicznym rozwojem sytuacji, nieprzewidywalnością procesów społecznych, to w praktyce bardzo trudne lub wręcz niemożliwe jest odróżnienie aktywności zwykłych aktorów sceny publicznej, w tym ekspertów, doradców, duchownych czy naukowców komentujących daną sytuację zagrożenia, od celowych działań inspirowanych przez obce służby specjalne lub innych aktorów państwowych.

V. Volkoff podkreśla, że dezinformacja może być rozumiana na dwa sposoby – węższy oraz szerszy. W ujęciu wąskim dezinformacja to zjawisko w połowie drogi między wprowadzaniem w błąd a wpływaniem. Autor ten wskazuje, że o ile wprowadzanie w błąd jest czynnością jednorazową, związaną

[65] https://miroslawmamczur.pl/deepfake-co-to-takiego-i-jak-go-zrobic/ (dostęp:27.01.2025)
[66] https://miroslawmamczur.pl/deepfake-co-to-takiego-i-jak-go-zrobic/ (dostęp:27.01.2025)
[67] Ibidem, s. 30-31.

z konkretnym zadaniem, gdzie dopuszcza się pewną *amatorszczyznę* w związku z wykorzystywaniem najróżniejszych środków zmierzających do wmówienia pewnych określonych treści konkretnym osobom, to już sama dezinformacja prowadzona jest w sposób systematyczny, fachowy, zawsze za pośrednictwem mass mediów i jest adresowana do opinii publicznej, a nie sztabów krajów-obiektów działań[68]. Z kolei podczas gdy wpływanie ma charakter pozornie niezorganizowany, oportunistyczny i głównie ilościowy, dezinformacja ma za zadanie realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości społecznej będących przedmiotem tych działań, poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie. Wtedy też dezinformacja zostaje *wchłonięta* w przez kontekst bezpieczeństwa i nie ma większego znaczenia, że dany decydent zdementuje konkretną informację lub tezę. Siłą rzeczy staję ona wówczas elementem oficjalnego dyskursu bezpieczeństwa.

W szerszym znaczeniu dezinformacja obejmuje także techniki wpływania, jak podkreśla V.Volkoff, z dwóch zasadniczych powodów. Z jednej strony ci sami ludzie, w ramach tej samej organizacji prowadzą działania w obu tych dziedzinach – wprowadzania w błąd oraz wpływania. Z drugiej natomiast posługują się analogiczną charakterystyką celu. Zarówno w dezinformacji jak i we wpływaniu „cel widzi się jako wspólnika”[69]. Zdaniem autora wystarczy wprowadzić do opinii publicznej minimalny nawet, ale odpowiedni katalizator, a nastąpi reakcja społeczna zgodna z oczekiwaniami dezinformatorów, a posiadająca przy tym pozory spontaniczności. Podkreśla się, że wprowadzanie w błąd jest techniką, natomiast dezinformacja doktryną[70].

Dezinformacja to akt, w ramach którego fałszywe informacje są tworzone i udostępniane w złej wierze lub prawdziwe informacje przekazywane są w taki sposób by wywołać fałszywe opinie. informacja tworzona z intencją generalnej szkody bądź także bezmyślne powtarzanie niesprawdzonych informacji. Przekazy te można podzielić, korzystając z dwóch kryteriów łącznie: stosunku do prawdy oraz intencji tworzenia i rozpowszechniania.

Zatem dezinformację należy rozumieć jako możliwe do zweryfikowania nieprawdziwe, wprowadzające w błąd lub także prawdziwe informacje, (mające na celu wywołanie fałszywej opinii na dany temat) tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną.

ZAKOŃCZENIE

Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[71] cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność

[68] V. Volkoff, Psychosocjotechnika, dezinformacja – oręż wojny, Wydawnictwo Antyk, Komorów 1999 r., s. 8.
[69] Ibidem, s. 9.
[70] Ibidem, s. 11.
[71] Dz.U. z 2018 r., poz. 1560.

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 której następuje przekaz takich usług[72]. 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 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[73]. Wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji a nie odnosi się 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

[72] K. Chałubińska-Jentkiewicz, M. Karpiuk, Prawo bezpieczeństwa informacyjnego, Warszawa 2015, s. 5.
[73] P. Potejko, Bezpieczeństwo..., s. 194.

obejmującego generalnie swoim zakresem zagrożenia, jakie pojawiają się w cyberprzestrzeni[74].

Bibliografia

Literatura

Banasiński C., Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni [w:] Cyberbezpieczeństwo. Zarys wykładu, C. Banasiński (red.), Warszawa 2018.
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.
Chałubińska-Jentkiewicz K., Prawne granice dezinformacji w środkach społecznego przekazu, Toruń 2023.
Chałubińska-Jentkiewicz K. (red.), Leksykon cyberbezpieczeństwa, Warszawa 2024.
Ciborowski L., Walka informacyjna, Toruń 1999.
Czyżak M., Spamming i jego karalność w polskim systemie prawnym, „Pomiary. Automatyka. Kontrola" 2009, nr 7.
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.
Lakomy M., Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015.
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.

[74] 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.

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.
Surma J., Cyfryzacja życia w erze Big Data, Warszawa 2017.
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.
Volkoff V., Psychosocjotechnika, dezinformacja – oręż wojny, Komorów 1999.
Wasielewski J., Zarys definicyjny cyberprzestrzeni, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.
Wasiuta O., Klepka R., Kopeć R., Vademecum bezpieczeństwa, Kraków 2018.

Akty prawne

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2024 r., poz. 34).
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 (j.t. Dz.U. 2017, poz. 1897).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (j.t. Dz. U. z 2024, poz. 1513).
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 (tj. Dz.U. z 2019 r., poz. 1950 ze zm.).
Dyrektywa 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 (Dz.Urz.UE.L 2016 Nr 194, s. 1).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, s. 80).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, s. 15).

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.