mgr inż. Marcin Nowak
ORCID: 0000-0002-1115-5679

https://doi.org/10.29316/9788368103205_1

CYBERPRZESTĘPCZOŚĆ JAKO WYZWANIE SYSTEMOWE

CYBERCRIME AS A SYSTEMIC CHALLENGE

Streszczenie

W rozdziale, za cel przyjęto kompleksową analizę zjawiska cyberprzestępczości w kontekście jego technologicznych uwarunkowań, różnorodnych form oraz działań podejmowanych przez państwa i organizacje międzynarodowe w celu przeciwdziałania tym zagrożeniom. Rozdział składa się z trzech zasadniczych części. W pierwszej przedstawiono ewolucję Internetu i rozwój technologii informacyjnych jako podstawę rozwoju środowiska sprzyjającego cyberprzestępczości. Druga część poświęcona została definicjom, klasyfikacjom oraz formom przestępstw popełnianych w cyberprzestrzeni, uwzględniając metody działania sprawców oraz dane statystyczne. Trzecia część omawia aktualne regulacje prawne oraz działania instytucjonalne podejmowane w Polsce i Unii Europejskiej w zakresie przeciwdziałania cyberzagrożeniom. Autor stawia pytanie badawcze: w jaki sposób rozwój Internetu oraz niedoskonałości systemów prawnych i organizacyjnych wpływają na skalę i skuteczność zwalczania

Summary

The aim of this chapter is to provide a comprehensive analysis of the phenomenon of cybercrime in the context of its technological determinants, various forms and actions taken by states and international organizations to counteract these threats. The chapter consists of three main parts. The first part presents the evolution of the Internet and the development of information technologies as the basis for the development of an environment conducive to cybercrime. The second part is devoted to definitions, classifications and forms of crimes committed in cyberspace, including the methods of action of perpetrators and statistical data. The third part discusses the current legal regulations and institutional activities undertaken in Poland and the European Union in the field of counteracting cyber threats. The author poses a research question: how do the development of the Internet and the imperfections of legal and organizational systems affect the scale and effectiveness of combating cybercrime? The hypothesis assumes that the

cyberprzestępczości? Postawiona hipoteza zakłada, że efektywność przeciwdziałania cyberprzestępczości zależy od poziomu integracji legislacyjnej, sprawności instytucji odpowiedzialnych za bezpieczeństwo cyfrowe oraz zdolności adaptacyjnych systemów ochrony wobec dynamicznie zmieniających się zagrożeń w cyberprzestrzeni. Zastosowane metody badawcze obejmują analizę literatury przedmiotu, przegląd źródeł prawa krajowego i międzynarodowego.

Słowa kluczowe: cyberprzestępczość, bezpieczeństwo cyfrowe, prawo karne, Internetu, instytucje państwowe

effectiveness of counteracting cybercrime depends on the level of legislative integration, the efficiency of institutions responsible for digital security and the ability of adaptive protection systems to dynamically changing threats in cyberspace. The research methods used include an analysis of the literature on the subject, a review of sources of national and international law.

Keywords: cybercrime, digital security, criminal law, Internet, state institutions

Wstęp

Współczesny świat, zdominowany przez technologię cyfrową i nieustanny rozwój Internetu, otwiera przed ludzkością niespotykane wcześniej możliwości komunikacji, pracy, handlu czy rozrywki. Jednocześnie jednak niesie ze sobą nowe, poważne zagrożenia. Cyberprzestępczość jako zjawisko stosunkowo nowe, lecz niezwykle dynamiczne, stała się istotnym wyzwaniem dla użytkowników indywidualnych, instytucji oraz państw.

Celem niniejszego rozdziału jest wszechstronna analiza zjawiska cyberprzestępczości: od historycznych i technologicznych uwarunkowań, przez definicyjne i klasyfikacyjne podejścia do czynów karalnych w przestrzeni cyfrowej, aż po odpowiedzi legislacyjne i instytucjonalne na poziomie krajowym i unijnym. W pierwszej części ukazano genezę i rozwój Internet jako fundament środowiska cyberprzestępczego. Druga część zawiera przegląd definicji, rodzajów cyberprzestępstw oraz metod działania sprawców, oparty o ujęcia przyjmowane przez organizacje międzynarodowe i prawo krajowe. Trzecia część koncentruje się na analizie systemu przeciwdziałania cyberprzestępczości – w tym barier prawnych, rozwiązań organizacyjnych i kierunków polityki bezpieczeństwa.

Podejście przyjęte w rozdziale ma charakter interdyscyplinarny: łączy perspektywę technologii informatycznych, prawa karnego, nauk o bezpieczeństwie i polityki publicznej. Autor opiera analizę na źródłach normatywnych, literaturze specjalistycznej oraz danych statystycznych. Całość prowadzi do wniosku, że

efektywne przeciwdziałanie cyberprzestępczości wymaga systemowej koordynacji działań międzyinstytucjonalnych, ciągłego doskonalenia przepisów prawa oraz międzynarodowej współpracy opartej na jednolitych standardach.

Geneza i rozwój Internetu jako podstawa zjawiska cyberprzestępczości

Analizując zjawisko i temat cyberprzestępczości oraz poprawne zdefiniowanie tego zjawiska, należy sięgnąć do korzeni, czyli początków powstania Internetu w Polsce i na świecie. Narodziny internatu to czas, który znacząco różni się od czasów dzisiejszych czyli współczesnego pojęcia i funkcjonowania Internetu. W tamtych czasach nie było „tradycyjnych" wyszukiwarek czy też przeglądarek internetowych, które obecnie służą nam jako niezbędne narzędzia do pozyskiwania danych czy najaktualniejszych informacji.

Ponieważ kolejne lata były ściśle powiązane z systematyczną zmianą projektową oraz nowymi koncepcjami zdalnej wymiany informacji, to z retrospektywnego punktu widzenia genezy Internetu, dość trudno i jednoznacznie wskazać jedynego twórcę tego „sieciowego wynalazku".

Początków Internetu możemy upatrywać w koncepcji połączenia ze sobą zdalnie komputerów opisanej przez Josepha Licklidera, a także w dwunastotomowej pracy napisanej przez Paula Barana dla Sił Zbrojnych Stanów Zjednoczonych w 1962 r., która zakładała stworzenie transmisji danych pomiędzy komputerami na znaczną odległość. Jednakże za faktyczny początek Internetu uznać należy powstanie pierwszych węzłów sieci nazywanych ARPANET. Ich początek datuje się na 29 października 1969 r., i rozpoczęcie eksperymentu na Uniwersytecie Kalifornijskim celem, którego było zbudowanie sieci komputerowej niemającej lokalizacji centralnej, która byłaby w stanie kierować pozostałymi podpiętymi komputerami[1]. Chodziło o taką sieć, która byłaby w stanie zachować swoje funkcjonowanie nawet w przypadku awarii lub odłączenia konkretnych elementów. Eksperyment był o tyle ważny, iż dotychczasowe sieci były sterowane za pomocą jednego komputera, co wiązało się z ryzykiem, że w przypadku jego awarii cała sieć była narażona na wyłączenie[2].

[1] J. C. R. Licklider, Man-Computer Symbiosis, https://worrydream.com/refs/Licklider_1960_-_Man-Computer_Symbiosis.pdf, [dostęp: 15.05.2025].

[2] K. Ashton, *That 'Internet of Things' Thing. In the real world, things matter more than ideas*, RFID Journal, http://www.rfid journal.com/articles/pdf?4986, [dostęp: 15.05.2025].

Pierwszym krajem, który wykorzystał koncepcję sieci rozproszonej Paula Barana, były Stany Zjednoczone. Wykorzystanie tej koncepcji było podyktowane świadomością państwa iż w przypadku ataku jako pierwszy będzie zniszczony komputer centralny. Skuteczność tej metody, okazała się na tyle progresywnym działaniem w rozwoju sieci, że stopniowo zatrudniano coraz to większą grupę naukowców do jej usprawniania.

Do końca lat 60. ubiegłego wieku funkcjonowanie sieci ARPANET było ściśle powiązane tylko z zamkniętą strukturą komputerów rządowych. Drzemiące zatem możliwości i potencjał w rozproszonej sieci dawały możliwość „wyjścia" poza potrzeby wojskowe i rządowe. Niestety pomimo wspomnianych możliwości sieci odczuwalne braki były po stronie rozbudowanych algorytmów tj. identyfikacja poszczególnych komputerów w obszarze konkretnej sieci. Było to niewątpliwym utrudnieniem w rozwoju Internetu w aspekcie globalnym[3].

Z początkiem lat 70. XX wieku, na przytoczone powyżej problemy w rozwoju sieci internetowej, przyszedł protokół TCP/IP. Był to krok milowy w rozwoju informatyzacji i sieci globalnej ogółem. TCP skupiał się na kontrolowaniu transferu danych przesyłanych za pomocą Internetu tj.: bezpośrednio z punktu A do punktu B, natomiast IP odpowiedzialne było za metodę adresowania, czyli nadanie każdemu komputerowi osobistego adresu, dzięki któremu powstała możliwość prawidłowego przesyłania danych do konkretnego komputera. Dodatkowo należy zaznaczyć, iż protokół TCP/IP, w przypadku błędu lub usterki w obszarze połączonych ze sobą komputerów w sieć, podczas przesyłania informacji taką usterkę ma możliwość ominąć i trafić do odbiorcy inną drogą. Takie zdarzenie to niezależność TCP od konkretnego ID, co tym samym zwiększa przepływ informacji oraz eliminuje opóźnienia spowodowane ewentualną awarią komputera głównego[4].

Początek lat 80. to unifikacja i stworzenie wykorzystywanego po dziś dzień systemu DNS tzn. numery IP są ściśle związane z nazwami domen internetowych.

Tuż po instytucjach wojskowych i rządowych zapotrzebowanie i „dobrodziejstwo" na ten typ i formę rozwoju technologicznego dostrzegły wyższe

[3] *Historia powstania Internetu - czyli jak narodziła się sieć?*, https://poradnikprzedsiebiorcy.pl/-historia-powstania-internetu, [dostęp: 15.05.2025].

[4] M. Mikołajewski, *Historia Internetu w pigułce Historia sieci, czyli od ARPANET-u do Internetu*, https://pclab.pl/art33917-2.html, [dostęp: 15.05.2025].

uczelnie oraz większość organizacji naukowych. Od 1989 r. Internet stał się nieodłącznym narzędziem do prac naukowych i badawczych. Siła Internetu, była na tyle mocno rozwojową stroną technologiczną, iż nie brakowało chętnych wśród społeczeństwa z segmentu prywatnego do jego wykorzystywania. Używanie Internetu do celów komercyjnych przez osoby prywatne jest możliwe po zniesieniu zakazu przez NSF (National Science Foundation) w 1991 r.

Koniec lat 90. ubiegłego wieku to powstanie pierwszej sieci dokumentów hipertekstowych o nazwie Word Wide Web, gdzie autorami był duet Tim Berners-Lee oraz Robert Cailliau, jak również stworzenie wyciąć osobiście przez Tima Bernersa-Lee pierwszego HTML-u, czyli pierwszej strony internetowej. Oczywiście strona ta nie działała tak jak obecne strony internetowe z którymi mamy do czynienia współcześnie. Ponieważ brakowało przeglądarek internetowych niektóre funkcje były bardzo mocno ograniczone.

Mosaic – to pierwsza internetowa przeglądarka, którą w 1994 r. stworzył – założyciel firmy Netscape – Marc Andressen. Firma Marca Anderessena poszła o krok dalej i stworzyła bardziej zaawansowaną przeglądarkę o nazwie Netscape Commerce S, która stała się wzorem do naśladowania dla nowych produktów internetowych. Graczami o stanowisko lidera w tym zakresie były dwie firmy, wspomniana Netscape i Microsoft. Zwycięzcą okazał się Bill Gates.Tak jak pierwsze przeglądarki, tak również pierwsze wyszukiwarki internetowe odbiegały nieco swoją konstrukcją od dzisiejszych. Pierwszą na świecie wyszukiwarkę stworzyli Alan Emtag i Peter J. Deutscha pod nazwą Archie (1990 r.). Celem Archie było bardzo szybkie wyszukiwanie plików zamieszczonych na serwerach FTP. 1993 r. to czas, kiedy pierwszy raz pojawiła się wyszukiwarka Wandex – narzędzie współpracujące bezpośrednio z odnośnikami hipertekstowymi, w następstwie czego dochodziło do odwiedzania stron internetowych za ich pośrednictwem. Twórcą tego produktu był Matthew Gray. To wydarzenie dało zielone światło do rozwoju robotów indeksujących o nazwie WWW Wanderer i rozwinięcie tej idei w przyszłości przez Google oraz Yahoo[5].

Kolejne lata to już błyskawiczny progres rozwoju sieci Internetowej. Coraz to bardziej zaawansowane narzędzia technologiczne, dawały możliwość precyzyjnego i skutecznego wyszukiwania konkretnych informacji

[5] *Historia powstania Internetu - czyli jak narodziła się sieć?*, https://poradnikprzedsiebiorcy.pl/-historia-powstania-internetu, [dostęp: 15.05.2025].

w sieci. Rozwój sieci przyniósł ze sobą większe znaczenie komunikacji a co za tym idzie różnego rodzaju komunikatorów typu: grupy dyskusyjne, blogi, fora, chaty czy serwisy społecznościowe, powodując postęp technologiczny w branży nośników informacji. Zapomniane już dzisiaj dyskietki, następnie płyty CD, DVD, Blue Ray, pendraive'y to tylko niektóre nośniki z którymi mieliśmy lub mamy do czynienia. Pokoleniu urodzonemu w latach 90. i później może się wydawać, że Internet towarzyszył ludziom od zawsze – zwłaszcza w Polsce – tymczasem to wciąż stosunkowo nowe osiągnięcie technologiczne[6].

Za pierwsze połączenie internetowe w naszym kraju, uznaje się sierpień 1991 r., kiedy to pracownik Wydziału Fizyki Uniwersytetu Warszawskiego wysłał e-mail z budynku przy ulicy Hożej. Na tamten czas należy uznać to za niezłe osiągnięcie, ponieważ dostępna prędkość Internetu niestety wynosiła tylko 9600 bit/s. Była to bardzo prosta komunikacja, nieskomplikowana, ale też pasująca do ówczesnych komputerów. Należy też wspomnieć, że Internet był narzędziem używanym tylko w niektórych miejscach np.: urzędach, firmach czy wybranych instytucjach. Zwykli obywatele nie mieli możliwości korzystania tych dobrodziejstw techniki.

Rok 1996 przyniósł ogromną rewolucję dla polskiego Internetu. W tamtym czasie Telekomunikacja Polska, największy wówczas operator telefoniczny w kraju, udostępniła numer 0-20 21 22, dzięki któremu była możliwość łączenia się z siecią przy pomocy modemu telefonicznego. Z pewnością rodzaj tego łączenia większość Polaków pamięta do dziś, gdyż przy łączeniu się z siecią towarzyszył charakterystyczny dźwięk. Największy renesans tej usługi przypada na lata 1998-2001. Mimo tego, iż szybkość połączenia wynosiła do 56 kb/s, większości użytkownikom w Polsce takie parametry nie przeszkadzały. Cieszył wówczas fakt, że sieć internetowa w ogóle działała[7].

Definicje, formy i klasyfikacje cyberprzestępczości

Od początku swojego istnienia, postępująca cyfryzacja, niemal we wszystkich dziedzinach naszego życia, przyniosła za sobą nie tylko korzyści dla codziennego egzystowania, ale również zagrożenia, wzmacniane przy tym

[6] Ł. Sarowski, *Od Internetu WEB 1.0 do Internetu WEB 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci*, Rozprawy Społeczne, 11(1), 2017, s. 34.

[7] *Historia Internetu w Polsce – Poradnik Orange*, https://www.orange.pl/poradnik/twoj-internet/historia-internetu-w-polsce/, [dostęp: 15.05.2025].

przez niezwykłą wręcz dynamikę i nieprzewidywalność rozwoju technologicznego ostatnich lat[8]. Ewolucja ta spowodowała iż przestały istnieć podziały w oparciu o bariery językowe czy granice państw, ponieważ dla każdego użytkownika Internetu światowa przestrzeń jest na wyciągnięcie ręki. Internet stał się oknem na świat, w którym każdy miał jednakowe prawa i każdy mógł się stać zarówno odbiorcą informacji, jak i ich twórcą dla innych użytkowników.

Przełom XX i XXI wieku to czas, nie tylko na świecie, ale także w Polsce, gigantycznego rozwoju zarówno komputerów, jak i sieci internetowej wraz z dostępem i użyciem technologii mobilnych.

W dzisiejszym świecie, Internet stał się nieodłącznym elementem naszego codziennego życia. Ponieważ wykorzystywany jest w wielu dziedzinach takich jak np.: banki, e-urzędy, e-zakupy czy poczta elektroniczna, z wielką trudnością przychodzi nam wyobrażenie sobie dnia bez korzystania z Internetu.

W okresie, kiedy Internet był dostępny tylko dla wąskiej grupy osób, kwestię bezpieczeństwa traktowano w sposób wybiórczy, bardziej jako problem marginalny. Dziś z uwagi na niespotykane dotychczas nasycenie wszystkich dziedzin życia nowoczesnymi technologiami, przestępczość komputerowa stanowi poważniejszy problem, a z każdym rokiem liczba przestępstw odnotowywana w policyjnych statystykach się zwiększa.[9]

W związku z coraz większym zaangażowaniem środków finansowych poprzez instytucje bankowe, a co za tym idzie wzrost kwot przelewanych elektronicznie, czy też zwiększający się obrót sklepów internetowych, portali ogłoszeniowych i aukcyjnych, tematyka zagrożeń w cyberprzestrzeni przestała być domeną wąskiej grupy specjalistów, stając się niebudzącym wątpliwości istotnym problemem współczesnego świata.[10]

Stanisław Lem, w książce pt.: „Bomba megabitowa" stwierdził, że „Zjawisko Internetu przypomina poniekąd znany nam potop, czyli nadmiar wód, w którym można ze wszystkim utonąć, jeżeli nie zdołamy dla ratunku, jak Noe, zbudować sobie Arki. Ale jakby miała wyglądać Arka Noego dla Internetu…?"[11].

---

[8] C. Banasiński (red.), *Cyberbezpieczeństwo – Zarys Wykładu*, Wolters Kluwer, Warszawa 2023, s. 15.

[9] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik Policyjny, Nr 4/2017, s. 20.

[10] C. Banasiński (red.), *Cyberbezpieczeństwo…*, op. cit., s. 15.

[11] G. Szpor, A. Gryszczyńska, *Internet – Strategie bezpieczeństwa*, Wydawnictwo C.H Beck, Warszawa 2017, s. 31.

Wyjaśnijmy zatem jaka jest definicja cyberprzestępczości. Co ona oznacza i jak ją mamy rozumieć w dzisiejszym świecie.

W latach 60. XX w., wraz z rozwojem nowych technologii i ich wykorzystywaniem w celach przestępczych pojawiła się potrzeba określenia grupy czynów polegających na posługiwaniu się komputerem do naruszania dóbr prawnych tradycyjnie chronione przez prawo karne. W literaturze przedmiotu opisując to zjawisko, zaczęto posługiwać się takimi pojęciami jak „przestępczość komputerowa" lub „przestępstwa związane z wykorzystaniem komputera". Od początku pojawienia się tych terminów wskazywano na liczne wątpliwości, co do ich zakresu znaczeniowego[12].

Z punktu widzenia cybernetyki oraz teorii informacji[13] termin ten definiowany jest jako „zbiór faktów", zdarzeń, cech itp., określonych obiektów (rzeczy, procesów systemów) zawartych w wiadomościach (komunikacie), tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne"[14]. W ujęciu tym informacja jest pojęciem ściśle związanym z człowiekiem i zdolnością jego celowego działania[15].

W myśl definicji opracowanej i zamieszczonej w „Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" przyjętej w dniu 25 czerwca 2013 r. w drodze uchwały przez Radę Ministrów, cyberprzestępstwo stanowi czyn zabroniony popełniony w obszarze cyberprzestrzeni, czyli przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[16] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[17].

---

[12] M. Siwicki, *Monografie Prawnicze – Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 10.

[13] T. Szewc, *Publicznoprawna ochrona informacji*, Wydawnictwo C. H. Beck, Warszawa 2007, s. 4.

[14] J. Petzel, *Informatyka prawnicza, Zagadnienia Teorii i praktyki*, Wydawnictwo Liber, Warszawa 1999, s. 35

[15] C. Banasiński (red.), *Cyberbezpieczeństwo…*, op. cit., s. 22.

[16] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 11 października 2024 r. w sprawie ogłoszenia jednolitego tekstu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557).

[17] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Komitet Stały Rady Ministrów, 25 czerwca 2013 r.

Interpol definiuje i określa cyberprzestępczość w dwóch ujęciach. Pierwsze z nich to wertykalnym a drugie horyzontalne. Ujęciem wertykalnym można nazwać przestępstwa specyficzne dla cyberprzestrzeni, czyli takie, które tylko tam mogą być dokonane, np. hacking czy sabotaż komputerowy. Z kolei w ujęciu horyzontalnym zakłada się popełnianie przestępstw za pomocą technik komputerowych (np. oszustwa komputerowe, fałszowanie pieniędzy, pranie brudnych pieniędzy itp.)[18].

Z przyjętej konwencji Rady Europy dotyczącej przedmiotu cyberprzestępczości[19] zjawisko to można określić jako, umyślny i bezprawny dostęp do całości lub części systemu informatycznego, umyślne i bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne, umyślne i bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych, poważne zakłócenia funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych, produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw lub hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw[20].

Przyjęta konwencja wyróżnia rodzaje przestępstw m.in.: przeciwko poufności, integralności oraz dostępności danych informatycznych. Do przestępstw komputerowych zalicza się fałszerstwo i oszustwo komputerowe jak również mamy do czynienia z przestępstwami ze względu na charakter zawartych informacji i naruszeniem praw autorskich.

---

[18] *Przestępstwa komputerowe – Prawo karne - kodeks karny, oskarżony przed sądem, świadek, ofiara przestępstwa*, http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe, [dostęp: 15.05.2025].

[19] Dz. U. z 2015 r. poz. 728.

[20] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik Policyjny, Nr 4/2017, s. 20.

Wg Unii Europejskiej definicję cyberprzestępczości – Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. „W kierunku ogólnej strategii zwalczania cyberprzestępczości" – należy interpretować jako odniesienie do trzech rodzajów przestępstw. Pierwsze odniesienie ukierunkowane jest na tradycyjne formy przestępstw np.: oszustwo czy fałszerstwo, jednak w aspekcie cyberprzestępczości dotyczą one konkretnych przestępstw popełnionych przy użyciu elektronicznych sieci informatycznych oraz systemów informatycznych. Drugi rodzaj przestępstw dotyczy nielegalnych publikacji treści w mediach elektronicznych. Za przykład możemy tu podać materiały związane z pornografią dziecięcą czy też nawoływaniem do ksenofobi. Trzeci rodzaj przestępstw można uznać za przestępstwa natury technicznej, ponieważ dotyczą typowo sieci łączności elektronicznej. To tej grupy przestępstw można zaliczyć ataki przeciwko systemom informatycznym, hakerstwo lub ataki typu DOS. Tego typu ataki są bardzo dobrze zorganizowane, a ich celem jest wymuszenie[21].

Definicję cyberprzestępczości w ujęciu wąskim i szerokim przyjął X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców. Zgodnie z przyjętymi zapisami wg ONZ, pojęcie cyberprzestępstwa w wąskim ujęciu to wszelkie nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzonych przeciw bezpieczeństwu systemów komputerowych lub też procesowanych przez te systemy danych.

Cyberprzestępstwo w szerokim sensie, czyli przestępstwo dotyczące komputerów, to takie, które dotyczy wszelkich nielegalnych działań popełnionych za pomocą lub dotyczących systemów lub sieci komputerowych, włączając w to między innymi bezprawne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[22].

Istotny jest jednak nie tyle spór definicyjny o istotę pojęcia cyberprzestępstwa, ile fakt, że rozwój technologii informacyjnych i komunikacyjnych oraz ich współczesna powszechność spowodował wyjątkową łatwość i swobodę dystrybucji, dostępu i wymiany informacji[23].

---

[21] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów „W kierunku ogólnej strategii zwalczania cyberprzestępczości" 22 maja 2007 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267, [dostęp: 15.05.2025].

[22] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010, s. 55.

[23] C. Banasiński (red.), *Cyberbezpieczeństwo…,* op. cit., s. 22.

Cyberprzestępczość przybrała wiele form i rodzajów działania. Pierwsza kategoria to przestępstwa typowe dla cyberprzestępczości, czyli takie, których celem jest bezpośredni atak na komputer lub też globalne przetwarzanie danych w systemach informatycznych. Do tej grupy można zaliczyć: fałszywe profile, hakowanie (hacking), czyli bezprawne uzyskanie informacji, podawanie się za inną osobę, sniffing, czyli podsłuch komputerowy, udaremnienie uzyskania informacji, sabotaż komputerowy, rozpowszechnianie złośliwych programów, oszustwa komputerowe czy też stosowanie narzędzi hackerskich[24].

Do drugiej kategorii cyberprzestępstw należy zaliczyć przestępstwa dotyczące wykorzystania typowo sieci internetowej a komputer jest jedynie środkiem do jego popełnienia. Typowe działania tej grupy cyberprzestępstw to m.in.: obraza uczuć religijnych, publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim, faszystowskim lub innym totalitarnym ustroju danego państwa oraz nawoływanie do nienawiści, na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, czyli szeroko rozumiana mowa nienawiści. Handel fikcyjnymi kosztami, zbywanie własnego lub cudzego dokumentu stwierdzającego tożsamość tzw.: przestępstwa przeciwko wiarygodności dokumentów, oszustwa popełniane za pośrednictwem portali aukcyjnych[25].

Jak podaje w Monogramie Prawniczym Maciej Siwicki, cyberprzestępczość można podzielić na trzy generacje. Pierwsza z nich obejmowała głównie naruszenia integralności systemów komputerowych i modyfikację znajdujących się tam danych na skutek wprowadzenia programów określanych jako „wirus" lub „robak". Druga generacja cyberprzestępstwa była ściśle związana z rozwojem sieci teleinformatycznych i atakami przez hakerów na bezpieczeństwo elektroniczne przetwarzanych tam informacji. Trzecia generacja cyberprzestępczości jest związana z zauważalnym procesem „automatyzacji" cyberprzestępczości, będącej m.in. efektem wykorzystania złośliwego oprogramowania i bitnetów. Generację tą charakteryzuje niskie prawdopodobieństwo wykrycia sprawcy oraz zorganizowane struktury przestępcze, skupione wokół tzw.: „podziemia komputerowego"[26].

Nowa generacja cyberprzestępstw to zautomatyzowane, rozproszone ataki przeprowadzone z wykorzystaniem napisanego w tym celu

[24] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 21.

[25] Ibidem.

[26] M. Siwicki, *Monografie Prawnicze – Cyberprzestępczość…*, op. cit., s. 1.

oprogramowania, które mają również charakter transgraniczny, co jest szczególnym utrudnieniem w ściganiu sprawców i zabezpieczaniu dowodów, jak również wymusza międzynarodową współpracę i koordynację podejmowanych działań[27].

Rosnący zakres działań cyberprzestępców to nie tylko ataki na globalne spółki, systemy bankowe, włamania do instytucji finansowych i podmiotów publicznych na całym świecie – w tym również w Polsce, ale ataki te mogą być również ukierunkowane na pozyskanie informacji, wpływanie na decyzje o charakterze strategicznym lub nastroje społeczne oraz powodowanie destabilizacji zarówno politycznej, jak i gospodarczej. Przykładem takiego ataku może być - ostatnio bardzo popularne narzędzie polityczne: fake news. Kampanie dezinformacyjne oraz ataki na infrastrukturę informacyjną są bardzo ważnym elementem wojny hybrydowej. Okazuje się zatem, że polityka w dzisiejszych czasach do „dziedzina, w której Internet może się przyczynić do zła o wiele szybciej, łatwiej, pewniej, aniżeli do dobra"[28].

Wg aktualnych szacunków, ogólna wartość globalnych strat poniesionych na skutek występowania cyberprzestępstw obecnie, porównywalna jest do wartości całego rynku narkotykowego, plasując się na poziomie około 388 miliardów dolarów rocznie[29].

Z danych policyjnych wynika, że rocznie ilość osób, które padły ofiarą różnej formy cyberprzestępstwa jest niemal pół miliarda ludzi na świecie, co za tym idzie średnio prawie 14 ofiar bezprawnej aktywności na sekundę. Polska niestety nie jest wyjątkiem. Według danych Policji, w Polsce w 2010 r. zgłoszono prawie 8 tys. cyberprzestępstw, z czego ponad 6 tys. przypadków to oszustwa[30]. Na rok 2012 przypada 19 tys. zgłoszonych przestępstw komputerowych w Polsce, z czego blisko 75% to przypadki oszustw. W 2015 r. liczba odnotowanych w naszym kraju cyberprzestępstw przekroczyła gigantyczny poziom, bo aż dwadzieścia tysięcy. Należy tu zaznaczyć, iż ogromna

[27] G. Szpor, A. Gryszczyńska, *Internet – Strategie bezpieczeństwa*, Wydawnictwo C.H Beck, Warszawa 2017, s. 31-32.

[28] S. Lem, *Bomba megabitowa*, Kraków 1999, s. 13-14.

[29] *Norton Cybercrime Report 2011*, http://pl.norton.com/cybercrimereport, [dostęp: 15.05.2025].

[30] Statystyka Policyjna, http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html, [dostęp: 15.05.2025].

liczba cyberprzestępstw pozostaje zamaskowana w szarej strefie, wymykając się obliczeniom statystycznym[31].

Polska cyberprzestępczość charakteryzuje się głównie tym, iż czyny przestępcze popełniane są w większości z wykorzystaniem Internetu. Wynika to z faktu, iż w dużej mierze ma na to wpływ duży progres postępu technologicznego, coraz łatwiejszy i obciążony niskimi kosztami dostęp do Internetu, uruchamianie coraz większej ilości hot spotów z anonimowym i darmowym dostępem do sieci czy też zwiększająca się z roku na rok liczba komputerów i urządzeń mobilnych. Inny czynnik, który ma na ten proceder wpływ to „komfort przestępcy". Przestępca nie musi angażować całej armii ludzi i sił, jak również środków finansowych, tak jak to się odbywa w rzeczywistości. Będąc aktywnym użytkownikiem komputera w domu, za pomocą kilku kliknięć jest w stanie dokonać oszustwa, wymienić się materiałami o naturze pedofilskiej lub też dokonać wpisu typu fake news szkalującego i obrażającego inną osobę[32].

Intensywna działalność cyberprzestępców – szczególnie w XXI w., to dla władz wielu państw bardzo poważny problem. Od dawna kraje te poszukują konkretnych rozwiązań – prawnych i technologicznych – które w sposób skuteczny pomogłyby w walce z przestępczością komputerową. Nasz kraj nie jest wyjątkiem. Efektywne ściganie przestępców komputerowych napotyka na co dzień wiele trudności. Pokonanie tych trudności jest konieczne do prawidłowego i pozytywnego zakończenia całego procesu wykrywczego, a co za tym idzie, ostatecznie ukarania sprawcy[33]. Jedną z przyczyn, która ma bezpośredni wpływ na utrudnienie, czasami wręcz uniemożliwiające skuteczne ściganie cyberprzestępstw jest fakt, że obowiązujące prawo w dużej mierze nie nadąża za bardzo szybkimi zmianami. Błyskawiczny progres zmian następuje zarówno w codziennej egzystencji, jak również w sieci Internetowej. Kolejną przyczyną, o której informują służby prawne i policyjne kraju, to – można powiedzieć- „konflikt" między wprowadzanymi zmianami w obowiązujących przepisach prawnych, które z założenia chronią wolność obywatelską, ale

[31] M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, Czasopismo Prawa Karnego i Nauk Penalnych, z. 1, 2000.

[32] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 23.

[33] *Prezydent RP: Cyfrowe zagrożenia na liście kluczowych problemów*, https://www.bbn.gov.pl/pl/wydarzenia/8326,Prezydent-RP-Cyfrowe-zagrozenia-na-liscie-kluczowych-problemow.html?search=51534879342831, [dostęp: 15.05.2025].

niestety mają znaczący wpływ na „zakłócenia" w podjęciu niezbędnych czynności przez organy ścigania[34].

Jako przykład wspomnianego „konfliktu" może być podana ustawa z dnia 16 lipca 2004 r.: Prawo telekomunikacyjne[35], w której wprowadzona nowelizacja w styczniu 2013 roku skróciła okres przechowywania istotnych dla organów ścigania danych tzw.: retencyjnych z 24 miesięcy do 12. Dodatkowo, skutkiem wprowadzonych zmian w tej ustawie, wszystkie bazy z danymi starsze niż 12 miesięcy, zaczynając liczenie od daty wejścia w życie nowych zapisów, zostały usunięte przez operatorów, a dostęp do nich stał się zupełnie niemożliwy.

Pozytywną i jak na razie jedyną zmianą w przedmiotowej ustawie, która ułatwia ściganie cyberprzestępców, jest wprowadzony w połowie 2016 r., nawiązujący do ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[36], obowiązek rejestracji u polskich operatorów wszystkich kart SIM, które działają w systemie prepaid.

Niestety dla osób zajmujących się „fachową" cyberprzestępczością, to tylko niewielka przeszkoda techniczno-prawna. Bez większego wysiłku, cyberprzestępcy mogą pozyskać przez sieć – najczęściej z portali aukcyjnych lub też sklepów internetowych – kartę SIM od zagranicznych operatorów, na których nie spoczywa obowiązek takiej rejestracji, lub też mają możliwość kupienia karty SIM z tzw.: „drugiego obiegu", którą rejestrują na tzw.: „słupa".

Kolejną nieprecyzyjną pozycją prawną jest ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[37], w której brakuje doprecyzowania zapisów dotyczących okresu retencji danych. Dane, które usługodawca jest zobligowany do gromadzenia, zbierania i przechowywania uzależnione jest od potencjału finansowego firmy i „dobrych chęci" przez dowolny okres – może to być rok, pół lub miesiąc czy tylko tydzień.

Efektem takich nieprecyzyjnych zapisów prawnych są bezpowrotnie utracone dane, które w całym procesie wykrywania cyberprzestępczości mają

[34] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 23.

[35] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800).

[36] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2016 r. poz. 904).

[37] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204).

olbrzymie znaczenie dla prowadzonych postępowań i niejednokrotnie stanowią jedyną podstawę i kierunek prowadzenia dalszych czynności operacyjnych[38].

Regulacje prawne i instytucjonalna odpowiedź na cyberzagrożenia

Kolejnym „zielonym światłem" dla cyberprzestępców jest możliwość korzystania z anonimowego dostępu do Internetu, który realizowany jest poprzez wykorzystanie punktów darmowego dostępu do Internetu tzw.: hotspot.

Znaczącą trudnością w zwalczaniu cyberprzestępczości są również różnice legislacyjne pomiędzy krajami. Wydłuża to lub uniemożliwia błyskawiczne ustalenie sprawcy. Dzieje się tak dlatego, iż składane wnioski o ściganie przestępców, które trafiły do tamtejszych sądów, rozpatrywane są według litery prawa, obowiązującej w danym kraju. W sytuacji, gdy w danym państwie czyn nie stanowi przestępstwa, zamknięta jest droga prawna do wydania takich danych. Najczęściej wnioski te są rozpatrzone negatywnie. Zjawisko takie ma destrukcyjny wpływ na szybkie wykrycie sprawcy, gdyż jak wiadomo w tego typu procederze czas jest kluczem do sukcesu. Transgraniczność sieci internetowej, to kolejne istotne utrudnienie dla organów ścigania[39]. Polega to na bardzo łatwym dostępie do usług świadczonych przez firmy zarejestrowane poza granicami kraju. Taka sytuacja wymusza prowadzenie innych- dodatkowych czynności operacyjnych, angażując przy tym organy ścigania innych państw[40].

Pierwszym krajem na świecie, który wprowadził do swojego systemu prawnego karalność przestępczości komputerowej były Stany Zjednoczone. Pierwszymi przepisami stanowymi w USA, których celem było przeciwdziałanie przestępczości komputerowej były przepisy karne stanu Floryda, które datuje się na 1 sierpnia 1978 r. Na wzór Florydy podobne rozwiązanie przepisów prawnych zostało wprowadzone w stanie Arkansas, West Virginia i rok 1989 oraz Maine i rok 1990 to stany, które jako ostanie przyjęły podobne rozwiązania prawne. Zderzając ze sobą przepisy stanowych kodeksów karnych,

[38] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 23.

[39] *Raport Cyberbezpieczeństwo A.D. 2018*, NASK – Państwowy Instytut Badawczy, Warszawa 2019, https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpieczeństwo-A.D.-2018.pdf, [dostęp: 15.05.2025].

[40] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s.24.

których przedmiotem jest przestępczość komputerowa, można łatwo stwierdzić, że różnią się one nie tylko ilością zamieszczonych artykułów, i ich treścią, lecz również zakresem dyspozycji i sankcji, które są przewidziane za ten sam czyn przestępny. Przykładem tego rozwiązania są przepisy Texas Penal Code – teksańskiego kodeksu karnego. O rodzaju przestępstwa drugiego czy trzeciego stopnia albo czy czyn taki jest występkiem, decyduje wartość powstałej szkody[41].

Przenosząc temat na obszar europejski, nie bez znaczenia – iż pomimo pozytywnej działalności przez pierwszy rok Europejskiego Centrum ds. Walki z Cyberprzestępczością, którego głównym zadaniem jest wspieranie, a w przypadku potrzeby również koordynowanie operacji dochodzeniowych prowadzonych przez państwa członkowskie[42], jest raport przygotowany przez Business Software Alliance (BSA) pt.: „European CyberSecurity Dashboard", opublikowany w marcu 2015 r.[43], w którym zwrócono szczególną uwagę na braki w cyberbezpieczeństwie UE. Braki te wynikały głównie z różnic politycznych, zapisów prawnych, jak również potencjału państw członkowskich.

Choć początki aktywności Unii Europejskiej w obszarze cyberbezpieczeństwa przypadają na rok 1997, „kiedy to Parlament wraz z Radą UE wydały dyrektywę w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym"[44], możliwości UE w obszarze prawa karnego były bardzo mocno ograniczone, natomiast wydawane dyrektywy bardzo rzadko nawiązywały do prawnokarnych środków ochrony. Wraz z wejściem w życie Traktatu z Lizbony[45], sytuacja ulegała zmianie. Przepisy prawa karnego stały się osobnym zakresem współpracy międzynarodowej. Artykuły od 82 do 86 Traktatu o Funkcjonowaniu Unii Europejskiej upoważniają Unię do ujednolicenia przepisów prawa karnego. Na szczególną uwagę zasługuje

[41] C. Banasiński (red.), *Cyberbezpieczeństwo…,* op. cit., s. 45.

[42] Komisja Europejska - Komunikat Prasowy: Europejskie Centrum ds. Walki z Cyberprzestępczością - pierwszy rok działalności.

[43] European CyberSecurity Dashboard and 28 Country Reports Launched - 3 March 2015.

[44] Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (97/66/WE).

[45] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r. (Dz. U. z 2009 r. Nr 203, poz. 1569).

potrzeba przeciwdziałania przestępczości ukierunkowanej na transgraniczność jak również współpraca w zakresie ich zwalczania[46].

Obecnie podstawy prawne cyberbezpieczeństwa w Unii Europejskiej są silnie zintegrowane z dokumentami programowymi, które stanowią „przedwiośnie" określonych regulacji prawnych na poziomie europejskim, albo też stanowią ich uzupełnienie o działania je wspomagające. Wyrazem tego podejścia jest Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa UE,[47] zastępująca Europejską Strategię Bezpieczeństwa z 2003 r. Strategia ta o tyle jest istotna, że określa priorytety działań zewnętrznych UE, którymi są: bezpieczeństwo, odporność państwa i społeczeństwa, zintegrowane podejście do konfliktów i kryzysów, wspieranie współpracy regionalnej oraz zarządzanie globalne w XXI wieku.[48] W przedmiotowej strategii wskazano konieczność wzmocnienia cyberbezpieczeństwa w drodze zwiększenia odporności infrastruktury krytycznej i sieci przesyłowych, walki z cyberprzestępczością, a przede wszystkim poprzez włączenie kwestii związanych z tym obszarem w inne polityki unijne oraz zacieśnienie współpracy między państwami członkowskimi, a także USA i NATO[49].

Punktem zwrotnym na rzecz zintegrowanego podejścia do problematyki cyberbezpieczeństwa była Europejska agenda cyfrowa, która była elementem przyjętej przez Komisję Strategii „Europa 2020" i zakłada, że technologie informacyjno-komunikacyjne powinny pełnić podstawową funkcję rozwojową – jeśli Europa za cel obrała realizację swoich ambitnych założeń do 2020 r. W strategii „Europa 2020" wyraźnie zwrócono bowiem uwagę na znaczenie upowszechnienia szeroko pasmowego Internetu, co ma sprzyjać włączeniu społecznemu i konkurencyjności gospodarki UE[50].

W Polsce, pierwsze próby dostosowania obowiązujących norm prawnych do zwalczania cyberprzestępczości, zostały podjęte w połowie lat 90

---

[46] Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE z 2012 r. C 326/47).

[47] *List Prezydenta na IV Europejskie Forum Cyberbezpieczeństwa* Cybersec, https://www.prezydent.pl/aktualnosci/wypowiedzi-prezydenta-rp/inne/art,826,list-prezydenta-na-iv-europejskie-forum-cyberbezpieczenstwa-cybersec-.html, [dostęp: 15.05.2025].

[48] *Notatka BBN nt. Europejskiej Agendy Bezpieczeństwa na lata 2015-2020***,** https://www.bbn.gov.pl/pl/wydarzenia/6721, NOTATKA-BBN-Europejska-Agenda-Bezpieczenstwa-na-lata-2015-2020.html?search=43892397, [dostęp: 15.05.2025].

[49] M. Wróblewska-Łysik, *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Bezpieczeństwo Narodowe, 1-4, 2016, s. 67.

[50] C. Banasiński (red.), *Cyberbezpieczeństwo…*, op. cit., s. 45-46.

XX wieku. Do chwili obecnej zapisy prawa karnego wciąż poddawane są nowelizacjom[51].

Zgodnie z obowiązującym stanem prawnym, w Polsce to Minister Cyfryzacji odpowiada za zapewnienie minimalnych wymagań w zakresie bezpieczeństwa teleinformatycznego w administracji publicznej. Wynika to wprost z ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[52] oraz mówi o tym rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[53].

2015 r. to zatwierdzenie przez Ministra Cyfryzacji *Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych.* Celem zatwierdzonego dokumentu jest gwarancja wsparcia przeprowadzenia kontroli działania systemów teleinformatycznych, które używane są do realizacji zadań publicznych – w tym również wymagań w obszarze bezpieczeństwa informacji.

Podjęcie prac kompleksowego uregulowania krajowego systemu cyberbezpieczeństwa w Polsce,[54] wynikało z potrzeby zapewnienia podejścia systemowego do krajowego systemu cyberbezpieczeństwa, jak również potrzeby systematycznego wdrażania do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady 2016/1148/UE[55].

Analizując temat cyberprzestępczości, należy tu zaakcentować fakt powstania w Polsce pewnego rodzaju instytucji z wyznaczonymi konkretnymi zadaniami, jakim jest Biuro do Walki z Cyberprzestępczością. Powstało ono 1 grudnia 2016 r. Głównymi zadaniami nowo powstałej jednostki są

---

[51] M. Siwicki, *Cyberprzestępczość*, wyd. C.H. Beck, Warszawa 2013, s. 25.

[52] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565).

[53] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526).

[54] Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL 2017, https://www.bbn.gov.pl/pl/wydarzenia/7865,Polskie-Forum-Cyberbezpieczenstwa-CYBERSEC-PL-2017.html?search=51534879342831, [15.05.2025].

[55] Uzasadnienie do Uchwały Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

„zadania związane z tworzeniem warunków do efektywnego wykrywania sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych”[56].

Do zadań Biura do Walki z Cyberprzestępczością należą w szczególności takie zadania jak: „… nadzorowanie, koordynowanie i wspieranie ukierunkowanych na zwalczanie cyberprzestępczości działań prowadzonych przez komendy wojewódzkie (Stołeczną) Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałanie z Centralnym Biurem Śledczym Policji w tym zakresie, prowadzenie czynności operacyjno-rozpoznawczych pozostających we właściwości biura, inicjowanie i prowadzenie współpracy z organami administracji rządowej, sądami, prokuraturami, instytucjami państwowymi, a także podmiotami prywatnymi w zakresie zadań pozostających we właściwości biura, prowadzenie współpracy międzynarodowej oraz współdziałanie z Biurem Międzynarodowej Współpracy Policji w zakresie zadań pozostających we właściwości biura, prowadzenie całodobowej służby mającej na celu koordynowanie działań Policji w zakresie zagrożeń przestępstwami w sieci Internet, ich zwalczania oraz współdziałania jednostek organizacyjnych Policji z krajowymi i zagranicznymi organami i podmiotami pozapolicyjnymi, prowadzenie konsultacji technicznych, inicjowanie i wspieranie badań oraz projektów, a także współpraca z podmiotami krajowymi i zagranicznymi zmierzająca do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z cyberprzestępczością…”[57].

W 2017 r. w kwietniu, uchwałą nr 52/2017 Rady Ministrów przyjęty został dokument strategiczny dotyczący bezpieczeństwa cyberprzestrzeni w postaci Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.[58] Dokument ten to efekt prac zespołu międzyresortowego pod kierunkiem Ministerstwa Cyfryzacji. Jednym z głównych zadań wskazanych w KRPC jest osiągnięcie jak najwyższego poziomu odporności krajowych systemów teleinformatycznych[59]. Dotyczy to świadczenia usług kluczowych, usług cyfrowych oraz usług administracji publicznej. Koncepcją jest

[56] http://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html

[57] http://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html

[58] Notatka BBN nt. Europejskiej Agendy Bezpieczeństwa na lata 2015-2020.

[59] „*Pięć żywiołów. Wolność – informacja – bezpieczeństwo” – wystąpienie Szefa BBN*, https://www.bbn.gov.pl/pl/wydarzenia/5631,Piec-zywiolow-Wolnosc-informacja-bezpieczenstwo-wystapienie-Szefa-BBN.html?search=43892397, [dostęp: 15.05.2025].

rozbudowa krajowego systemu cyberbezpieczeństwa w takiej formie, aby mógł być on „ukierunkowany na zbudowanie zdolności w zakresie bieżącego monitorowania zagrożeń oraz zarządzania cyberbezpieczeństwem w skali kraju”[60].

Przedstawione działania, podjęte przez Ministerstwo Cyfryzacji we współpracy z innymi resortami podyktowane były zmianą ustawy o działach administracji rządowej w grudniu 2015 r.[61], jak również zaleceniami pokontrolnymi skierowanymi do byłego Ministerstwa Administracji i Cyfryzacji, w związku z przeprowadzoną kontrolą przez NIK w 2014 r., która dotyczyła instytucji publicznych odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.

Na obecną chwilę polski system prawny nie posiada przepisów, które regulują szczegółowo zagadnienia dotyczące cyberbezpieczeństwa w dziedzinach objętych zakresem dyrektywy PE 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 UE. Niektóre elementy o charakterze bezsankcyjnym, które wprost odnoszą się do regulacji wymagań bezpieczeństwa teleinformatycznego infrastruktury krytycznej, zostały zawarte w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK).

Wizja cyberbezpieczeństwa Polski, o której można przeczytać w załączniku do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. dot. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, „Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni. Dzięki synergii działań wewnętrznych i międzynarodowych cyberprzestrzeń RP stanowić będzie bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli”[62].

Z założeń przedmiotowej ustawy wynika, że Polska będzie krajem dążącym do kontynuacji dyskursu dotyczącego sprawnie funkcjonujących systemów międzynarodowych zarządzanych przez globalną sieć oraz zagadnień

[60] Uzasadnienie do Uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

[61] Ustawa z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. z 2015 r. poz. 2281).

[62] Załącznik do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. dot. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, s. 8, 25.

związanych z prawną oceną cyberataków. Dyskusja ta będzie miała na celu wypracowanie spójnych rozwiązań, które gwarantują pewność międzynarodowej wymiany informacji w Internecie. Ustawa zakłada iż Polska będzie angażować się we wzmacnianie środków budowy bezpieczeństwa i zaufania „w ramach istniejących forów międzynarodowych, w tym OBWE. Rząd będzie włączał się również w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym".

Podsumowanie

Cyberprzestępczość jest jednym z największych wyzwań współczesnego świata cyfrowego. Jej dynamiczny rozwój idzie w parze z postępem technologicznym, co sprawia, że coraz trudniej jest skutecznie się przed nią bronić. Jednocześnie jednak istnieją coraz bardziej zaawansowane metody przeciwdziałania zagrożeniom płynącym z sieci – od nowoczesnych systemów bezpieczeństwa, przez odpowiednie regulacje prawne, po rosnącą świadomość użytkowników. Skuteczna walka z cyberprzestępczością wymaga współpracy międzynarodowej, inwestycji w edukację oraz ciągłego dostosowywania środków ochronnych do zmieniających się realiów cyfrowych. Tylko w ten sposób możliwe będzie bezpieczne korzystanie z dobrodziejstw nowoczesnych technologii bez obaw o utratę danych, prywatności czy reputacji.

Z przeprowadzonych rozważań wynika, że kluczowym problemem w skutecznym przeciwdziałaniu cyberprzestępczości pozostaje niedostosowanie obowiązujących systemów prawnych do szybko ewoluujących form działalności przestępczej w sieci. Istotnym utrudnieniem jest także ograniczona skuteczność działań instytucji państwowych, wynikająca z braku jednoznacznych procedur, zbyt krótkiego okresu przechowywania danych oraz transgranicznego charakteru przestępstw, który wymaga ścisłej współpracy międzynarodowej.

Wnioskiem zasadniczym jest potrzeba przyjęcia podejścia systemowego, opartego na trzech filarach: harmonizacji prawa na poziomie krajowym i unijnym, wzmacnianiu kompetencji instytucji zajmujących się cyberbezpieczeństwem oraz ciągłej edukacji i uświadamianiu użytkowników sieci co do skali i form zagrożeń. Tylko przy zaangażowaniu wszystkich tych elementów możliwe jest ograniczenie skali cyberprzestępczości oraz zwiększenie

poziomu ochrony informacji, prywatności i interesów państwa w środowisku cyfrowym.

Literatura

1. Banasiński C. (red.), *Cyberbezpieczeństwo – Zarys Wykładu*, Wolters Kluwer, Warszawa 2023.
2. Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (97/66/WE).
3. European CyberSecurity Dashboard and 28 Country Reports Launched – 3 March 2015.
4. Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe*, Czasopismo Prawa Karnego i Nauk Penalnych, z. 1, 2000.
5. Komisja Europejska – Komunikat Prasowy: Europejskie Centrum ds. Walki z Cyberprzestępczością – pierwszy rok działalności.
6. Lem S., *Bomba megabitowa*, Kraków 1999.
7. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 24 lutego 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz. U. z 2017 r. poz. 570, z późn. zm.
8. Petzel J., *Informatyka prawnicza. Zagadnienia Teorii i praktyki*, Wyd. Liber, Warszawa 1999.
9. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Komitet Stały Rady Ministrów, 25 czerwca 2013 r.
10. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz.U. 2012 poz. 526.
11. Sarowski Ł., *Od internetu WEB 1.0 do internetu WEB 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci*, Rozprawy Społeczne, 11(1), 2017.
12. Siwicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013.
13. Siwicki M., *Monografie Prawnicze – Cyberprzestępczość*, wyd. C.H. Beck, Warszawa 2013.
14. Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik Policyjny Nr 4/2017.
15. Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010.
16. Szewc T., *Publicznoprawna ochrona informacji*, wyd. C. H. Beck, Warszawa 2007.
17. Szpor G., Gryszczyńska A., *Internet – Strategie bezpieczeństwa*, wyd. C.H Beck, Warszawa 2017.
18. Traktat o funkcjonowaniu Unii Europejskiej, Dz.Urz. UE 2012, C 326/47.

19. Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r., Dz.U. 2009 nr 203, poz. 1569.
20. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Dz.U. 2004 nr 171 poz. 1800.
21. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Dz.U. 2016 poz. 904.
22. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002 nr 144 poz. 1204.
23. Ustawa z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw. Dz.U. 2015 poz. 2281.
24. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005 nr 64 poz. 565.
25. Uzasadnienie do Uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.
26. Wróblewska-Łysik M., *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Bezpieczeństwo Narodowe, 1-4, 2016.
27. Załącznik do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. dot. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

Netografia

1. Ashton K., *That 'Internet of Things' Thing. In the real world, things matter more than ideas*, „RFID Journal", http://www.rfid journal.com/articles/pdf?4986.
2. *Historia powstania Internetu – czyli jak narodziła się sieć?*, https://poradnikprzedsiebiorcy.pl/-historia-powstania-internetu.
3. *Historia Internetu w Polsce – Poradnik Orange*, https://www.orange.pl/poradnik/twoj-internet/historia-internetu-w-polsce/.
4. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów „W kierunku ogólnej strategii zwalczania cyberprzestępczości" 22 maja 2007 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267.
5. Licklider J. C. R., *Man-Computer Symbiosis*, https://worrydream.com/refs/Licklider_1960_-_Man-Computer_Symbiosis.pdf.
6. List Prezydenta na IV Europejskie Forum Cyberbezpieczeństwa Cybersec, https://www.prezydent.pl/aktualnosci/wypowiedzi-prezydenta-rp/inne/art,826,list-prezydenta-na-iv-europejskie-forum-cyberbezpieczenstwa-cybersec-.html.
7. *Norton Cybercrime Report 2011*, http://pl.norton.com/cybercrimereport.
8. Notatka BBN nt. Europejskiej Agendy Bezpieczeństwa na lata 2015-2020, *Pięć żywiołów. Wolność – informacja – bezpieczeństwo* – wystąpienie Szefa BBN, https://www.bbn.gov.pl/pl/wydarzenia/5631,Piec-zywiolow-Wolnosc-informacja-bezpieczenstwo-wystapienie-Szefa-BBN.html?search=43892397.

9. Mikołajewski M., *Historia Internetu w pigułce Historia sieci, czyli od ARPA-NET-u do Internetu*, https://pclab.pl/art33917-2.html.
10. Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL 2017, https://www.bbn.gov.pl/pl/wydarzenia/7865,Polskie-Forum-Cyberbezpieczenstwa-CYBERSEC--PL-2017.html?search=51534879342831.
11. *Przestępstwa komputerowe – Prawo karne – kodeks karny, oskarżony przed sądem, świadek, ofiara przestępstwa*, http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe.
12. *Prezydent RP: Cyfrowe zagrożenia na liście kluczowych problemów*, https://www.bbn.gov.pl/pl/wydarzenia/8326,Prezydent-RP-Cyfrowe-zagrozenia-na-liscie--kluczowych-problemow.html?search=51534879342831 .
13. *Raport Cyberbezpieczeństwo A.D. 2018*, NASK – Państwowy Instytut Badawczy, Warszawa 2019, https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf.
14. Statystyka Policyjna, http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html.