CYBERPRZESTĘPCZOŚĆ
– próba diagnozy zjawiska

nadkom. Mariusz Stefanowicz

ekspert Wydziału Rozpoznania
Biura do Walki z Cyberprzestępczością KGP

Celem artykułu jest ukazanie w przystępnej formie każdemu czytelnikowi, będącemu jednocześnie użytkownikiem komputera i Internetu, kluczowych definicji i zagadnień z zakresu cyberprzestępczości. W zamyśle jest również przedstawienie podstawowego podziału tego typu przestępczości, charakterystycznych cech pozwalających na wyróżnienie poszczególnych czynów przestępczych, a także największych problemów i trudności – zarówno prawnych, jak i organizacyjnych – z jakimi borykają się polskie organy ścigania w ich zwalczaniu.

Z uwagi na dynamiczny rozwój Internetu, usług internetowych czy coraz częstsze udostępnianie danych wrażliwych w urządzeniach mobilnych, to zagadnienie powinno być w zainteresowaniu każdego z nas.

W jak najlepiej pojętym własnym interesie każdy użytkownik Internetu, komputerów czy urządzeń telekomunikacyjnych, z uwagi na coraz to bardziej wyszukane sposoby popełniania przestępstw lub oszustw internetowych dokonywanych z wykorzystaniem socjotechniki i najnowszych technologii, powinien dobrze poznać zagadnienia, takie jak podstawy zwalczania cyberprzestępczości czy „dobre praktyki" niezbędne do bezpiecznego korzystania z Internetu.

Wstęp

Od początku swojego istnienia, tj. lat 70. i 80. dwudziestego wieku, Internet w olbrzymi sposób zmienił sposób postrzegania otaczającego nas świata. Zatarły się podziały istniejące w oparciu o granice państw czy bariery językowe. Świat stał się mniejszy i bliższy dla każdego użytkownika Internetu. W istniejącej sieci każdy miał jednakowe prawa i każdy mógł się stać zarówno odbiorcą informacji, jak i ich twórcą dla innych użytkowników.

Koniec XX i początek XXI wieku to okres, nie tylko na świecie, ale także w Polsce, gwałtownego rozwoju komputerów, samego Internetu oraz dostępu do niego z użyciem technologii mobilnych. Internet jest obecnie wykorzystywany w tak wielu ważnych aspektach naszego codziennego życia, takich jak operacje bankowe, zakupy, e-urzędy czy zwykła poczta elektroniczna, że trudno sobie wyobrazić dzień bez sprawdzenia najświeższych informacji, odwiedzin najpopularniejszych portali społecznościowych czy oglądania telewizji lub słuchania radia on-line.

W czasach, kiedy Internet raczkował i był dostępny tylko dla ograniczonego kręgu osób, kwestię bezpieczeństwa traktowano po macoszemu i pozostawiano raczej problemem marginalnym. 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 po-

licyjnych statystykach się zwiększa. Dodatkowo, z uwagi na zaangażowanie coraz większych środków finansowych poprzez bankowość internetową, rosnącą liczbę kwot przelewów elektronicznych czy zwiększające się obroty sklepów internetowych oraz portali aukcyjnych i ogłoszeniowych, stopniowo kładzie się coraz większy nacisk na zwalczanie tego typu przestępczości. Internet jest dziś powszechnie wykorzystywany jako narzędzie służące do dokonywania wszelkiego rodzaju czynów zabronionych.

Definicja cyberprzestępczości

Polskie prawodawstwo do dzisiaj nie stworzyło jednolitej definicji cyberprzestępczości. Pojęcie przestępczości komputerowej nie jest jednoznacznie zdefiniowane nawet na gruncie Kodeksu karnego. Funkcjonuje natomiast wiele tworzonych doraźnie, w zależności od potrzeb, definicji opierających się na najprostszym założeniu, iż ogólnie są to przestępstwa popełniane za pomocą komputerów oraz Internetu.
Innym źródłem definicji, z którego można korzystać, mogą być międzynarodowe podmioty, takie jak ONZ, Unia Europejska czy Interpol, które opracowały definicję cyberprzestępczości na własne potrzeby. Jednak bez względu na to, jaką definicję cyberprzestępczości przyjmiemy, zawsze to będą czyny zabronione, skierowane przeciwko systemom informatycznym, w których komputer jest celem samym w sobie, oraz czyny dokonane z użyciem komputera, w których stanowi on jedynie narzędzie.

Definicja Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

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 (Dz. U. z 2017 r. poz. 570, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[1].

Definicja cyberprzestępczości według Interpolu

Definicja sformułowana przez Interpol jest bardzo praktyczna i określa cyberprzestępczość w dwóch ujęciach – tzw. wertykalnym oraz horyzontalnym. Ujęcie wertykalne dotyczy przestępstw specyficznych dla cyberprzestrzeni, czyli takich, które tylko tam mogą być dokonane, np. hacking, sabotaż komputerowy. Z kolei ujęcie horyzontalne zakłada popełnianie przestępstw za pomocą technik komputerowych (np. oszustwa komputerowe, fałszowanie pieniędzy, pranie brudnych pieniędzy etc.)[2].

Definicja cyberprzestępczości według Rady Europy

W przedmiocie cyberprzestępczości Rada Europy przyjęła konwencję z dnia 23 listopada 2001 r. o cyberprzestępczości (Dz. U. z 2015 r. poz. 728). Z jej zapisów wyłania się obraz definicji cyberprzestępczości jako:

- umyślnego i bezprawnego dostępu do całości lub części systemu informatycznego;
- umyślnego i bezprawnego przechwytywania 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;
- umyślnego i bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych, poważnego zakłócania 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.

Konwencja ta wyróżnia następujące rodzaje przestępstw:

- przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów;
- przestępstwa komputerowe – fałszerstwo komputerowe oraz oszustwo komputerowe;
- przestępstwa ze względu na charakter zawartych informacji;
- przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[3].

Definicja cyberprzestępczości według Unii Europejskiej

Definicja ta została zawarta w Komunikacie Komisji Do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. „W kierunku ogólnej strategii zwalczania cyberprzestępczości".
W praktyce terminu cyberprzestępczość używa się w odniesieniu do trzech rodzajów przestępstw. Pierwszy obejmuje tradycyjne formy przestępstw, takie jak oszustwo czy fałszerstwo, jednak w kontekście cyberprzestępczości dotyczą one konkretnie przestępstw popełnionych z użyciem elektronicznych sieci informatycznych i systemów informatycznych. Drugi rodzaj stanowi publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci czy też nawoływaniem do nienawiści rasowej). Trzeci rodzaj obejmuje przestępstwa typowe dla sieci łączności elektronicznej, tj. ataki przeciwko systemom informatycznym, ataki typu DOS oraz hakerstwo[4].

Definicja cyberprzestępczości według ONZ

Definicję w przedstawionej poniżej formie przyjął X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców. Zgodnie z przyjętymi zapisami definicji zostało wyróżnione cyberprzestępstwo w ujęciu wąskim oraz w ujęciu szerokim. I tak:

- cyberprzestępstwo w wąskim sensie (przestępstwo komputerowe) – jest to wszelkie nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych;
- cyberprzestępstwo w szerokim sensie (przestępstwo dotyczące komputerów) – wszelkie nielegalne działanie popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[5].

Podstawowy podział i charakterystyka cyberprzestępczości

W najbardziej uproszczony sposób cyberprzestępczość można podzielić na dwie podstawowe kategorie:

- przestępstwa charakterystyczne dla cyberprzestępczości,
- przestępstwa popełniane z wykorzystaniem sieci Internet.

Pierwszą kategorię stanowią przestępstwa, w których przedmiotem ataku jest sam komputer oraz szeroko pojęte przetwarzanie danych w systemach informatycznych. Do tej grupy można zaliczyć takie czyny, jak:

- podawanie się za inną osobę, fałszywe profile,
- nieuprawnione uzyskanie informacji (hacking),
- podsłuch komputerowy (sniffing),
- udaremnienie uzyskania informacji,
- udaremnienie dostępu do danych informatycznych,
- sabotaż komputerowy,
- rozpowszechnianie złośliwych programów oraz cracking,
- stosowanie tzw. narzędzi hackerskich,
- oszustwo komputerowe.

Do drugiej kategorii należy zaliczyć przestępstwa, w których komputer jest jedynie środkiem do jego popełnienia. W tej grupie można wymienić takie działania, jak:

- obrazę uczuć religijnych (przestępstwa przeciwko wolności sumienia i wyznania),
- składanie propozycji obcowania płciowego z małoletnim,
- publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim,
- publiczne propagowanie faszystowskich lub innych totalitarnych ustrojów państwa lub nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (szeroko pojęta mowa nienawiści),
- handel fikcyjnymi kosztami,
- zbywanie własnego lub cudzego dokumentu stwierdzającego tożsamość (przestępstwa przeciwko wiarygodności dokumentów),
- oszustwa popełniane za pośrednictwem Internetu, np. na portalach aukcyjnych.

Polska przestępczość w cyberprzestrzeni charakteryzuje się tym, iż czyny te w większości można zakwalifikować do drugiej kategorii, czyli są popełniane z wykorzystaniem Internetu. Taki stan rzeczy wynika w dużej mierze z postępu technologicznego, coraz łatwiejszego i obciążonego niskimi kosztami dostępu do sieci, uruchamiania coraz większej liczby hotspotów z anonimowym, darmowym dostępem do Internetu czy coraz większej liczby komputerów i urządzeń mobilnych.
Innym czynnikiem jest „wygoda" osób, które takie czyny popełniają. Sprawca nie musi angażować tylu sił i środków jak w świecie realnym. Siedząc w domu, kilkoma kliknięciami może dokonać oszustwa, wymienić się materiałami pedofilskimi czy też dokonać wpisu szkalującego inną osobę lub obrażającego uczucia religijne.

Dodatkowym ułatwieniem dla sprawców jest głębokie przeświadczenie, że cyberprzestrzeń zapewnia im anonimowość, oraz mała świadomość ich ofiar w zakresie bezpiecznego wykorzystywania zasobów sieci Internet. Inną charakterystyczną cechą cyberprzestępczości jest sporadyczne zgłaszanie przestępstw popełnionych w Internecie, co powoduje wzrost ciemnej liczby przestępstw. W tym przypadku wynika to z wielu czynników. Jednym z nich jest niska świadomość użytkowników, którzy często nie wiedzą, że stali się ofiarą cyberprzestępstwa. Przykładem może być wirus Weelsof, który infekuje komputery użytkowników, podszywając się pod organa ścigania, i za odblokowanie zasobów komputera żąda wniesienia opłaty. Osoby, których komputery zostały zainfekowane, nie wiedzą, że takie procedury są niedozwolone i niestosowane przez organy ścigania, a także nie mają wiedzy niezbędnej do samodzielnego odblokowania komputera.

Ponadto ofiary tych działań bardzo niechętnie składają zawiadomienia o popełnieniu przestępstwa z uwagi na to, iż rzeczywiście posiadają nielegalne zasoby w komputerze w postaci materiałów chronionych prawami autorskimi w formie filmów lub muzyki czy też korzystają ze specjalistycznego oprogramowania bez wykupionych i opłaconych niezbędnych, wymaganych przepisami prawa, licencji. Kolejnym czynnikiem może być fakt, że stanie się ofiarą cyberprzestępstwa może być ukrywane w obawie przed kompromitacją i utratą reputacji.

Trudności zwalczania cyberprzestępczości

W związku z intensywną działalnością cyberprzestępców władze wielu państw od dawna poszukują rozwiązań – prawnych i technologicznych – które umożliwiłyby skuteczną walkę z przestępczością komputerową. Polska nie jest wyjątkiem. Skuteczne ściganie cyberprzestępców z wielu stron napotyka trudności, których przezwyciężenie jest konieczne do

pozytywnego zakończenia procesu wykrywczego i w efekcie – ukarania sprawcy.
Jednym z aspektów utrudniających lub czasami wręcz uniemożliwiających skuteczne ściganie przestępstw popełnianych w cyberprzestrzeni jest fakt, iż obowiązujące przepisy prawa często nie nadążają za błyskawicznymi zmianami, jakie następują zarówno w życiu codziennym, jak i w Internecie. Inną przyczyną są wprowadzane zmiany w obowiązujących przepisach prawnych, które chroniąc wolności obywatelskie, znacząco zakłócają podjęcie niezbędnych czynności przez organy ścigania.
Przykładem takich przepisów może być ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907, z późn. zm.), w której w styczniu 2013 r. przez wprowadzoną nowelizację skrócono okres przechowywania istotnych dla organów ścigania danych retencyjnych z 24 do 12 miesięcy. Ponadto w wyniku wprowadzonych zapisów wszystkie dane starsze niż 12 miesięcy, licząc od daty wejścia w życie nowelizacji ustawy, zostały usunięte przez operatorów i dostęp do nich stał się niemożliwy.
Jedyną pozytywną zmianą w przepisach prawa telekomunikacyjnego, ułatwiającą ściganie sprawców przestępstw, jest wprowadzony w połowie 2016 r., powiązany z wejściem w życie ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904, z późn. zm.), obowiązek rejestracji u polskich operatorów wszystkich kart SIM działających w systemie pre-paid. Karty niezarejestrowane przez użytkowników do 31 stycznia br. zostały dezaktywowane przez operatora.
Należy jednak stwierdzić, że zmiany te to tylko niewielka przeszkoda dla osób zajmujących się przestępczym procederem. Mogą one bez większego problemu pozyskać przez Internet z zagranicznych portali aukcyjnych lub sklepów internetowych karty SIM zagranicznych operatorów nieobarczone obowiązkiem rejestracji lub kupić kartę SIM „z drugiego obiegu" zarejestrowaną na tzw. słupa.
Innym przykładem może być ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219, z późn. zm.), w której zabrakło precyzyjnych zapisów w zakresie okresu retencji danych. Dane, które usługodawca jest zmuszony gromadzić, są zbierane i przechowywane w zależności od możliwości finansowych i „dobrych chęci" przez dowolny okres – może to być pół roku, miesiąc czy tydzień.
Skutkiem takich nieprecyzyjnych zapisów są bezpowrotnie tracone dane mające olbrzymie znaczenie dla prowadzonych postępowań i niejednokrotnie stanowiące jedyną podstawę prowadzenia dalszych czynności wykrywczych.

Dużym ułatwieniem i pomocą w realizacji działań przestępczych było też wprowadzenie do obiegu przez banki kart płatniczych w systemie „pre-paid" (przedpłaconych). Można je było uzyskać z banku bez potwierdzenia i przypisania do nich tożsamości użytkownika, a umożliwiały one dokonywanie całkowicie anonimowych płatności internetowych, przelewów na inne konta bankowe czy wypłat środków pieniężnych w całej sieci bankomatów.

Jednak w wyniku przeprowadzonej przez Urząd Komisji Nadzoru Finansowego (UKNF) analizy, Komisja Nadzoru Finansowego (KNF) w dniu 10 lipca 2015 r. wystosowała do zarządów banków krajowych pismo, w którym zajęła stanowisko, że prowadzona przez banki działalność w zakresie kart pre-paid nie jest wydawaniem pieniądza elektronicznego w rozumieniu obowiązujących przepisów prawa i nie powinna być kontynuowana bez przyjęcia istotnych zmian[6].
W wyniku podjętych przez KNF działań instytucje bankowe zaprzestały wydawania kart na okaziciela w pierwotnie przyjętej formie.

Aspektem utrudniającym zwalczanie cyberprzestępczości jest także dynamiczny rozwój narzędzi, które wykorzystane przez nawet niezaawansowanego użytkownika zapewniają mu ukrycie jego tożsamości i prawdziwej lokalizacji. Służą do tego narzędzia anonimizujące sieć – TOR lub usługa serwera Anonymous Proxy – używane przez sprawców przestępstw.

Kolejnym ułatwieniem, z którego cyberprzestępcy chętnie korzystają, jest anonimowy dostęp do Internetu realizowany z wykorzystaniem punktów darmowego dostępu do Internetu – hotspot.
Inną trudnością w zwalczaniu cyberprzestępczości są różnice legislacyjne pomiędzy krajami, co wydłuża lub wręcz uniemożliwia szybkie ustalenie sprawcy. Wnioski o ściganie sprawców lub dane udostępniane przez firmy prowadzące działalność poza granicami Polski trafiają do tamtejszych sądów i są rozpatrywane według przepisów prawa, które obowiązują w danym państwie. W przypadku, gdy w określonym kraju czyn nie stanowi przestępstwa lub nie ma podstaw do wydania danych, takie wnioski pozostają rozpatrzone odmownie. Te procedury w znaczący sposób wydłużają czas realizacji czynności niezbędnych do wykrycia sprawcy czynności, a szybkość działania przy tego typu przestępczości jest niejednokrotnie kluczem do sukcesu. Co więcej, w niektórych przypadkach to firmy zagraniczne, same, bez udziału sądu czy prokuratury, interpretują przesłanki przemawiające za udostępnieniem danych i ich zakresu. Przykładowo, administratorzy portali, takich jak np. google.com, facebook.com czy youtube.com, we własnym zakresie analizują żądania policji i podejmują decyzje, czy udostępnić dane.
Kolejnym istotnym utrudnieniem dla organów ścigania jest transgraniczność Internetu polegająca na bardzo łatwym dostępie do usług świadczonych przez firmy zagraniczne (konta e-mail, komunikatory itp.). Nie obowiązują ich przepisy polskiego prawodawstwa w zakresie udostępniania danych niezbędnych dla prowadzonych postępowań, co wymusza prowadzenie dodatkowych czynności z zaangażowaniem organów ścigania innych państw. Obecnie stosowany system międzynarodowej wymiany informacji, w którym jest brak jednolitego, elektronicznego i bezpośredniego systemu międzynarodowej wymiany informacji pomiędzy komórkami zajmującymi się cyberprzestępczością, powoduje liczne trudności. Należy również zauważyć, że o ile wymiana informacji z organami ścigania z Europy Zachodniej, z mniejszymi lub większymi proble-

mami, ale jest w sposób ciągły prowadzona, o tyle uzyskanie informacji z krajów egzotycznych, takich jak Chiny, Indie czy Ameryka Południowa, jest praktycznie niemożliwe.
Wszystkie te elementy powodują co najmniej wydłużenie czasu uzyskiwania informacji lub w ogóle uniemożliwiają jej otrzymanie, co ma istotny wpływ na skuteczne i efektywne zwalczanie przestępczości internetowej.

Tendencje i ewentualne nowe trendy w zagrożeniach bezpieczeństwa cyberprzestrzeni

Całe zjawisko cyberprzestępczości jest napędzane bardzo prostą zależnością. Rosnąca liczba użytkowników Internetu i – co za tym idzie – coraz większa ilość ulokowanych tam środków finansowych powoduje wzrost liczby przestępstw popełnianych za pomocą komputera. Na podstawie analizy bieżących tendencji przewiduje się szybki wzrost przestępczości w zakresie wykorzystania zaawansowanych technologii informatycznych, które mogą objąć nowe dziedziny życia społecznego i gospodarczego. Telefony komórkowe, smartfony, tablety czy komputery oraz sieć Internet – poprzez możliwości jakie dają – odgrywają coraz większą rolę w nielegalnej działalności lub też w znaczny sposób ułatwiają jej prowadzenie. Handel przedmiotami uzyskanymi w wyniku przestępstwa, oszustwa internetowe, pirackie oprogramowanie, naruszenia praw autorskich czy coraz częściej spotykana przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych to tylko niewielka część czynów, jakie można popełnić, nie wychodząc z domu, nie narażając się na bezpośredni kontakt ze swoją ofiarą, przypadkowym świadkiem, służbami porządkowymi, takimi jak straż miejska lub pracownicy ochrony czy przedstawicielami organów ścigania.
Sprawcy przestępstw, którzy z premedytacją dążą do zapewnienia sobie „sukcesu przestępczego", coraz częściej wykorzystują specjalne oprogramowanie umożliwiające kamuflowanie miejsca, z którego działają. Również zjawiska takiego typu jak np. sieć TOR czy wirtualne systemy dokonywania płatności w Internecie BitCoin, pozostające poza jakąkolwiek kontrolą instytucji finansowych, sprzyjają realizacji przestępczych celów.
Jest przewidywany dalszy wzrost przestępczości w zakresie wykorzystania zaawansowanych technologii informatycznych, które mogą dotyczyć nowych aspektów, jak np. upowszechniający się podpis elektroniczny. Internet będzie używany także do szantażu i wyłudzeń, np. poprzez groźbę wykorzystania luk w zabezpieczeniach systemów komputerowych lub „eksploatację" skradzionych informacji. Będzie ujawniana coraz większa liczba przestępstw komputerowych o wysokiej jednostkowo wartości strat, a także nastąpi dalszy wzrost liczby oszustw na aukcyjnych portalach internetowych. Największym zagrożeniem najprawdopodobniej będzie – ze względu na mało skomplikowany charakter przestępstwa – oszustwo dokonywane z wykorzystaniem platform handlowych i portali aukcyjnych. W najbliższych latach, jak można przypuszczać, wzrośnie obrót na aukcjach internetowych i serwisach darmowych ogłoszeń, gdyż coraz więcej osób będzie poszukiwać tzw. „zakupowych okazji", z kolei inni będą sprzedawać przedmioty codziennego użytku, które są im już zbędne lub w celu poprawy stanu budżetu domowego, co bezpośrednio może się przełożyć na wzrost przestępstw internetowych. Nieograniczony dostęp do szerokich zasobów Internetu na całym świecie spowoduje, iż należy się spodziewać dynamicznego rozwoju nowych form cyberprzestępczości i nasilenia już istniejących, takich jak akty terroru, oszustwa, przestępstwa związane z phishingiem, handlem ludźmi, rozpowszechnianiem pornografii dziecięcej czy oferowaniem do sprzedaży przedmiotów pochodzących z przestępstwa, przestępstwa związane z naruszeniem praw własności intelektualnej, a także szpiegostwo elektroniczne, nieuprawniony dostęp do informacji czy kradzieże tożsamości i szantaż.

[1] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Komitet Stały Rady Ministrów, 25 czerwca 2013 r., https://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp: 13.12.2017 r.].

[2] http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html [dostęp: 13.12.2017 r.].

[3] Konwencja Rady Europy o cyberprzestępczości („Konwencja o cyberprzestępczości") podpisana w dniu 23 listopada 2001 r.

[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 [dostęp: 13.12.2017 r.].

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

[6] Stanowisko KNF w sprawie wydawania przez banki tzw. kart przedpłaconych. 10 lipca 2015 r., https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 13.12.2017 r.].

Summary

Cybercrime – an attempt to diagnose the phenomenon

The purpose of the article is to present to an every reader, being simultaneously a user of a computer and the Internet, crucial definitions and issues in cybercrime in an accessible form. It is also intended to present the basic division of this type of crime, characteristic features allowing for distinguishing individual criminal acts, as well as the biggest problems and difficulties – both legal and organizational – which the Polish law enforcement agencies deal with in fighting them.
Due to the rapid development of the Internet, internet services or making available sensitive data in mobile devices more and more often, this issue should be of great interest for each of us.
In the best comprehended self-interest every Internet, computers or telecommunications devices user, due to more and more sophisticated ways of committing offences or Internet frauds committed with the application of the social engineering and new technologies, should familiarize well with the problems such as bases of fighting cybercrime or "best practices" essential for the safe use of the Internet.

Tłumaczenie: Renata Cedro