Janusz Wasilewski

Przestępczość w cyberprzestrzeni – zagadnienia definicyjne

Choć takie wyrażenia, jak przestępczość komputerowa czy cyberprzestępczość nie należą w obowiązującym stanie prawnym do polskich wyrażeń ustawowych, nie sposób nie zgodzić się z twierdzeniem, że odnoszą się do jednego z największych zjawisk przestępnych dzisiejszych czasów. Zgodnie z aktualnymi szacunkami łączna wartość globalnych strat ponoszonych na skutek popełniania cyberprzestępstw już od kilku lat jest porównywalna do wartości całego rynku narkotykowego i plasuje się na poziomie 388 mld dolarów rocznie[1]. Jak wynika z przeprowadzonych badań, ofiarami wszelkich form nielegalnej działalności w Internecie (w tym także związanej z rozsiewaniem wirusów komputerowych oraz innych typów złośliwego oprogramowania) pada rocznie pół miliarda ludzi, co w skali światowej daje średnią około 14 ofiar tego typu bezprawnej aktywności na sekundę! W Polsce w 2010 r., według oficjalnych danych Policji[2], zgłoszono prawie osiem tysięcy przestępstw popełnionych w sieci, z czego ponad sześć tysięcy – oszustw. W 2012 r. ogólna liczba przestępstw komputerowych oscylowała już na poziomie 19 tys. (około 3/4 przypadków oszustw), aby w 2015 r. przekroczyć 20 tys. Należy zaznaczyć, że ogromna liczba przestępstw komputerowych, które potęgują zagrożenie, pozostaje ukryta w szarej strefie i wymyka się wszelkim statystykom[3]. Specyfika przestępstw popełnianych w cyberprzestrzeni powoduje bowiem, że wiele tego typu czynów pozostaje niewykrytych lub nie jest poprawnie identyfikowanych jako przestępstwo. Powodem takiego stanu rzeczy jest z jednej strony nierzadko sam użytkownik komputera lub innego urządzenia, który nie zdaje sobie sprawy z tego, że padł ofiarą przestępstwa (brak „technicznej" świadomości), z drugiej zaś zdarzenia, które są wykrywane i poprawnie kwalifikowane jako przestępne, nie zawsze zostają zgłoszone do ścigania. W przypadku dużych firm zachowanie w tajemnicy informacji o tym, że uległy one skutecznemu atakowi hackerskiemu, w którym przełamano zbyt słabe zabezpieczenia infrastruktury teleinformatycznej przedsiębiorstwa, może nie tylko być próbą ochrony swojego wizerunku, lecz także sposobem na uniknięcie ewentualnych konsekwencji odszkodowawczych (np. informacja o cyberataku na bank, w którego wyniku mogło dojść do wycieku poufnych danych jego klientów).

W świetle przytoczonych informacji suma zysków potencjalnie generowanych przez cyberprzestępczość czyni ten rodzaj działalności jedną z najbardziej lukratywnych gałęzi przestępczości w ogóle i przyciąga nie tylko drobnych złodziei czy oszustów, lecz także cybergangi specjalizujące się w nowoczesnych technologiach lub „konwencjonalne", zorganizowane grupy przestępcze, które chcą rozszerzyć swój dotychczasowy

[1] Pierwotne dane z raportu *Norton Cybercrime Report 2011*, dostępnego w wersji elektronicznej na stronie internetowej pod adresem: http://pl.norton.com/cybercrimereport/ [dostęp: 20 VI 2016].

[2] Dane pochodzą z oficjalnej strony internetowej Policji, dostępnej pod adresem: http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html oraz http://statystyka.policja.pl/st/informacje/85606,Przestepstwa-w-sieci.html [dostęp: 20 VI 2016].

[3] M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1; opracowanie dostępne również na stronie internetowej pod adresem: http://prawo.vagla.pl/node/905.

obszar aktywności. W każdym z tych przypadków cyberprzestępczość pozostaje działalnością tanią, stwarzającą przestępcom ogromne możliwości (także np. terrorystyczne), a przy tym wciąż uważaną za zapewniającą większe bezpieczeństwo niż inne, tradycyjne formy działalności przestępnej, i to zarówno przed wymiarem sprawiedliwości, jak i działaniami innych, rywalizujących przestępców[4]. Można powiedzieć, że wszelkie słabości cyberprzestrzeni stają się automatycznie siłą napędową nowoczesnych przestępców.

Mimo że określenie cyberprzestępczość[5] – oraz inne wyrażenia stosowane do opisu poruszanego tu zjawiska – wciąż nie stanowi kategorii prawnej, to z uwagi na prezentowane w literaturze przedmiotu jego zakres[6], specyfikę oraz konieczność tworzenia i poprawnego stosowania prawa należy uznać, że zapewnienie skutecznego zwalczania zagrożeń w cyberprzestrzeni uzasadnia, a wręcz wymaga, prowadzenia szerokiej analizy całej gałęzi związanej z tą dziedziną działalności przestępnej i pojęć odnoszących się do czynów wchodzących w jej skład.

Artykuł jest próbą uporządkowania stosowanych terminów oraz udzielenia odpowiedzi na podstawowe pytania o to, czym jest cyberprzestępstwo, jakie są jego rodzaje oraz co je odróżnia od innych kategorii przestępstw[7]. Tak wskazana problematyka pozostaje w ścisłym związku z określeniem, jakie (jak ujęte?) dobra prawnie chronione są przedmiotem zamachu tego rodzaju działalności przestępnej. Podobnie jak w przypadku określania cyberprzestrzeni, także i te rozważania nie mogą ograniczać się wyłącznie do płaszczyzny prawnej, która bez kontekstu technologicznego pozostaje zawieszona w próżni. Definicja cyberprzestępczości jest prezentowana oraz rekonstruowana na podstawie wielu rozwiązań przyjętych na gruncie piśmiennictwa, aktów okołoprawnych oraz powszechnie obowiązujących przepisów, zarówno krajowych, w tym także polskich, jak i powstałych w ramach inicjatyw międzynarodowych. Do rozważań wprowadzono także dodatkowe pojęcia wspomagające opis cyberprzestępczości – cyberincydent oraz cyberatak.

Analiza stosowanych pojęć

Brak jednolitych rozwiązań prawnych nakierowanych na zapobieganie oraz zwalczanie nowoczesnych form przestępczości komputerowej, wynikający w dużej mierze

[4] Zob. *Fighting Cybercrime: Technical, Juridical and Ethical Challenges*. Opracowanie dostępne na stronie internetowej pod adresem: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.

[5] Termin powstał jeszcze na początku lat 90. XX w. Oficjalnie został użyty przez tzw. Grupę z Lyon, działającą w ramach grupy G8, której zadaniem było prowadzenie prac analitycznych nad nowymi formami przestępczości, za: S. Perrin, *Cybercrime*, w: A. Ambrosi, V. Peugeot, D. Pimienta, *Word Matters: multicultural perspectives on information societies*, Caen 2005. Opracowanie dostępne także w wersji elektronicznej na stronie internetowej pod adresem: http://media.mcgill.ca/en/word_matters. A. Adamski zwraca uwagę na zastosowanie omawianego terminu w 1996 r. przez L.E. Quarantiellego, w: tenże, *Cyber Crime: How to protect yourself from computer criminals*, Wisconsin 1996; A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30 i nast.

[6] Niektórzy autorzy podają wręcz w wątpliwość, czy czyny określane pojęciami odnoszącymi się do cyberprzestępczości zachowują w rzeczywistości homogeniczność. Zob. np. U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3, s. 6, za: A. Kania, *Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni*, e-biuletyn CBKE 1/2009, Wrocław 2009, s. 8. Tekst opracowania jest dostępny również na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf.

[7] Stosowanie klasycznego dorobku prawa karnego wobec cyberprzestępczości zaznacza K. Dobrzeniecki w: tenże, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 61 i nast.

z niechęci (lub niezdolności) państw do wypracowywania wspólnych stanowisk oraz spóźnionego podjęcia odpowiednich inicjatyw legislacyjnych, spowodował wytworzenie wyjątkowo niespójnej oraz niejednorodnej siatki pojęciowej z obszaru cyberprzestępczości. Nieco ironicznie zauważa się już od dawna w piśmiennictwie, że pojęcia stosowane w tym zakresie mają często charakter bardziej publicystyczny niż naukowy[8]. Ten pogląd należy, niestety, podzielić. Tym samym wyrażeniom często są nadawane różne, krzyżujące się zakresowo znaczenia. Definicje często są tworzone ad hoc, przy okazji tworzenia nowego dokumentu lub opracowania. Na domiar złego ustawiczne zmiany spowodowane rozwojem nowoczesnych technologii, stanowiące przecież fundament cyberprzestrzeni oraz nowoczesnych usług świadczonych za pośrednictwem sieci komputerowych, również nie sprzyjają jednoznaczności oraz trwałości budowanych definicji[9]. Zasadne jest zatem, aby podjąć próbę uporządkowania istniejącego stanu rzeczy.

Pojęcie nadużycia komputerowego

W ujęciu historycznym proces formułowania nowych, specyficznych pojęć odnoszących się do przestępczości komputerowej rozpoczął się jeszcze w połowie lat 70. XX w. Był to okres pierwszych głośnych, medialnych doniesień o atakach hackerskich, które uświadomiły nie tylko szerszej opinii publicznej, lecz także przedstawicielom władz rządowych pojawienie się nowych cyberzagrożeń. Warto dodać – zagrożeń, które mogą powodować jak najbardziej realne straty finansowe. W latach 70. spopularyzowało się także określenie hacker, które negatywnie zaczęło się kojarzyć dopiero w połowie następnego dziesięciolecia[10].

Jednym z pierwszych, szeroko rozpoznawanych opracowań poświęconych zwalczaniu nowoczesnych form przestępczości stała się książka autorstwa Donna Parkera zatytułowana *Crime by Computer* (*Przestępstwo z wykorzystaniem komputera*) wydana w 1976 r.[11] Wbrew tytułowi autor skupił się w niej wokół pojęcia nadużycie komputerowe[12], które rozumiał jako (…) *każdy incydent polegający na zamierzonym zachowaniu, którego ofiara poniosła lub mogła ponieść szkodę, zaś sprawca odniósł lub mógł odnieść zysk, wiążący się z komputerami*[13]. Wskazał także cztery rodzaje przeznaczenia komputera lub zgromadzonych w nim danych w tak określonym nadużyciu:

1) jako przedmiot ataku,
2) jako narzędzie wytwarzające specyficzne środowisko lub nowe formy dóbr prawnych podlegających ochronie,
3) jako środek lub narzędzie służące do popełnienia nadużycia,
4) jako symbol użyty w celu zastraszenia lub dokonania oszustwa[14].

---

[8] Zob. np. A. Adamski, *Prawo karne komputerowe*…, s. 30.

[9] Trudnościom w budowaniu odnośnych definicji była poświęcona nawet odrębna część *Zalecenia Nr R(89)9 Komitetu Ministrów Rady Europy z 1989 r. w sprawie przestępczości komputerowej*.

[10] Słowo „*hacker*" oznaczało pierwotnie (znaczenie pozytywne) osobę o wysokich kwalifikacjach komputerowych, potrafiącą w szerokim zakresie wykorzystywać możliwości nowych technologii informatycznych.

[11] D.B. Parker, *Crime by Computer*, Nowy Jork 1976 (tłumaczenie tytułu – własne).

[12] W oryginale: *computer abuse.*

[13] W oryginale: *any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain and is associated with computers*. Cyt. za: A. Reyes, *Cyber Crime Investigations*, bmw, [USA] 2007, s. 25 (tłumaczenie własne).

[14] Tamże, s. 25.

Choć wymienione rodzaje przeznaczenia komputera i zgromadzonych w nim danych częściowo przeplatały się zakresowo, każdy z nich odnosił się do różnych form dokonywania nadużyć. Pierwszy nawiązywał do ochrony samych systemów teleinformatycznych oraz przechowywanych w nich danych w postaci elektronicznej, które mogą stać się celem działania przestępnego. Drugi, zdecydowanie wyprzedzający swoje czasy, nawiązywał do nowego sposobu postrzegania dóbr prawnie chronionych, które wraz z rozwojem cyberprzestrzeni mogą wyrażać się w zupełnie nowych, nieznanych dotychczas formach, wykraczając poza postać typowych praw, ruchomości, nieruchomości oraz dóbr osobistych. Trzeci rodzaj przeznaczenia można odnieść do kategorii nadużyć komputerowych sensu stricto, w których komputer staje się niezbędnym narzędziem do popełnienia przestępstwa (które może być skierowane także przeciwko dobrom prawnym mającym wyłącznie swój cyfrowy wymiar), czwarty zaś odwoływał się do tych czynów, dla których komputer staje się wyłącznie środkiem komunikacyjnym, samo zaś zachowanie można kwalifikować jako przejaw klasycznych form czynów bezprawnych (jak np. oszustwo czy zniesławienie). Pomimo tak szerokiego ujęcia, żaden z wymienionych rodzajów przeznaczenia nie odnosił się jednak bezpośrednio do wykorzystywania komputerów jako samodzielnych źródeł dowodowych, które mogą dostarczać dowodów także w sprawach niezaliczających się ściśle do kategorii nadużyć komputerowych. Z uwagi na czasy, w których definicja była budowana (przed powstaniem Internetu), żadne z ujęć nie odwoływało się także do wykorzystania komputera w celu przeprowadzania ataków za pośrednictwem sieci.

W przytoczonej definicji proponuje się, aby dwiema głównymi cechami nadużycia komputerowego były jego umyślność oraz jednoczesna strata bądź korzyść majątkowa, powstające na skutek przestępstwa. Innymi słowy – nadużyciem komputerowym nie mógł stać się ani czyn niezamierzony, jak np. nieumyślne uszkodzenie zasobów chronionych, ani taki, który w ogóle nie zakładał możliwości odniesienia korzyści przez jego sprawcę, jak akt wandalizmu polegający na skasowaniu lub podmianie plików strony internetowej. Oba wskazane wymogi, stanowiące przejaw utożsamiania nadużyć komputerowych z przestępczością nastawioną na określone korzyści majątkowe, należy wiązać z dawnym rozumieniem przestępczości komputerowej jako przestępczości wysokospecjalistycznej, wymagającej świadomego podejmowania skomplikowanych operacji.

Pojęcie nadużycie komputerowe znalazło się w wydanym w 1986 r. raporcie Organizacji Współpracy Gospodarczej i Rozwoju (OECD) zatytułowanym *Computer -related Crime: Analysis of Legal Policy* (*Przestępstwa związane z komputerem: analiza polityki legislacyjnej*)[15]. Czyn nadużycia komputerowego został roboczo określony w raporcie jako *Każde zachowanie niezgodne z prawem, nieetyczne lub nieuprawnione, odnoszące się do automatycznego przetwarzania oraz przekazywania danych*[16].

Oprócz przytoczonej wyżej definicji nadużycia komputerowego w raporcie OECD wymieniono także enumeratywnie i określono pięć kategorii nadużyć komputerowych, które powinny być penalizowane we wszystkich porządkach prawnych. Zaliczono do nich: oszustwo komputerowe (nastawione na uzyskiwanie korzyści majątkowych), fałszerstwo komputerowe, zakłócenie poprawnego funkcjonowania systemu (sabotaż), nielegalne kopiowanie programów komputerowych oraz nielegalny dostęp do systemu

[15] *Computer-related Crime: Analysis of Legal Policy*, OECD, Paris 1986 (tłumaczenie tytułu – własne).

[16] Tłumaczenie własne. W oryginale: *Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data*.

komputerowego uzyskany przez naruszenie zabezpieczeń lub w celu wyrządzenia szkody[17]. Wykaz typowych nadużyć komputerowych został zatem przedstawiony wyłącznie w kontekście czynów, które powinny podlegać kwalifikacji karnej, w odróżnieniu od podejścia, które zaprezentowano w ramach budowy definicji nadużycia komputerowego. Jednocześnie łączył kategorie ściśle karnistyczne (fałszerstwo, włamanie) z ochroną praw autorskich, nazywając nadużyciem komputerowym także kopiowanie programów (dziś zwane potocznie piractwem komputerowym), które może być dokonywane z całkowitym pominięciem komputerów. Na marginesie warto zaznaczyć, że oprócz omawianego tu pojęcia w raporcie OECD posługiwano się również kategorią przestępstwa związanego z komputerem, które, choć odgrywało drugorzędną rolę, pojawiało się z niewyjaśnionych przyczyn w samym tytule dokumentu.

Równolegle do pojawienia się pojęcia nadużycie komputerowe w raporcie OECD w 1986 r. to pojęcie pojawiło się w obszernej amerykańskiej kodyfikacji prawa nastawionej na kompleksowe zwalczanie zagrożeń komputerowych. Przybrała ona formę ustawy zatytułowanej *Computer Fraud and Abuse Act*[18], której przepisy stały się podstawowym narzędziem amerykańskiego wymiaru sprawiedliwości w walce z przestępstwami popełnianymi z wykorzystaniem komputera. Co istotne, pomimo historycznej już daty wprowadzenia tej ustawy, pozostaje ona aktem wciąż obowiązującym, co nadaje prowadzonym rozważaniom waloru aktualności. Od chwili wejścia w życie ustawa była wielokrotnie nowelizowana, m.in. w latach 1989, 1994, 1996, 2001 (ustawą *PATRIOT Act*[19] wydaną po zamachu na WTC) oraz 2008 (ustawą *Identity Theft Enforcement and Restitution Act*[20])[21]. Przepisy wprowadzone ustawą z 1986 r. uzupełniły także sekcję 1030 (stworzoną w 1984 r.) 47. rozdziału 18. tytułu amerykańskiego *United States Code*[22]. W tej sekcji pierwotnie była uregulowana penalizacja szczególnych przypadków uzyskania bezprawnego dostępu do informacji rządowych, przede wszystkim informacji niejawnych oraz informacji finansowych, w sytuacji gdy te informacje były przetwarzane w komputerach należących do agend rządowych[23]. Sama sekcja 1030 została zatytułowana *Oszustwo oraz podobna działalność w powiązaniu z komputerami*[24].

Ustawą *Computer Fraud and Abuse Act* wprowadzono penalizację wielu czynów stypizowanych, które, zgodnie z samą nazwą aktu normatywnego, zostały określone jako „nadużycia oraz oszustwa komputerowe". W odniesieniu do zastosowanej

[17] A. Adamski, *Prawo karne komputerowe*…, s. 6.

[18] W tłumaczeniu własnym: *Ustawa o komputerowym oszustwie oraz nadużyciu*. Tekst ustawy dostępny na stronie internetowej pod adresem: http://www.law.cornell.edu/uscode/text/18/1030.

[19] Nazwa ustawy „*PATRIOT Act*" pisana wielkimi literami stanowi skrót od wyrazów: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. W tłumaczeniu własnym: *Jednocząc oraz wzmacniając Amerykę poprzez dostarczenie stosownych narzędzi wymaganych do wykrywania oraz zapobiegania terroryzmowi*.

[20] W tłumaczeniu własnym: *Ustawa o ściganiu przestępstwa kradzieży tożsamości oraz jej restytucji*.

[21] C. Doyle, *Cybercrime*: *An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, Congressional Research Service, s. 1. Tekst pełnego opracowania dostępny na stronie internetowej pod adresem: http://www.fas.org/sgp/crs/misc/97-1025.pdf.

[22] *United States Code* (U.S.C.) jest swoistym odpowiednikiem Dziennika Ustaw, który obejmuje skodyfikowane prawo federalne USA. Więcej na temat U.S.C. na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/United_States_Code.

[23] H.M. Jarrett, M.W. Bailie, E. Hagen, S. Eltringham, *Prosecuting Computer Crimes*, Washington DC 2010, s. 1. Opracowanie dostępne na stronie internetowej pod adresem: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

[24] Tłumaczenie własne. W oryginale: *Fraud and related activity in connection with computers*.

tu nazwy zbiorczej uwagę zwraca wyraźne wydzielenie oszustwa komputerowego z pozostałych nadużyć komputerowych, co z jednej strony może podkreślać szczególny charakter tego czynu (obejmujący połączenie działań komputerowych z elementami socjotechniki oraz nastawienie na uzyskanie korzyści majątkowej), z drugiej zaś czyni zasadnym pytanie, czy w tej sytuacji oszustwo komputerowe należy, na gruncie omawianego aktu, zaliczać do ogólnej kategorii nadużyć komputerowych. Wyraźne usytuowanie „oszustw" obok „nadużyć" mogłoby sugerować intencjonalne oddzielenie obu kategorii, przesądzające, że „oszustwo" nie należy do zbioru nadużyć komputerowych, choć brakuje możliwości potwierdzenia takiej tezy na gruncie samych przepisów. Z uwagi na pozostawienie w treści ustawy omawianych wyrażeń bez jakichkolwiek definicji, także określenie ich znaczenia jest możliwe wyłącznie przez prezentację typologii przestępstw ujętych w przepisach aktu. Z uwagi na normatywny charakter omawianego dokumentu forma, w jakiej zostały określone kolejne przestępstwa, jest typowo kodeksowa (np.: *Kto uzyskuje bezprawny dostęp*...). W rezultacie w przepisach zostały pominięte jakiekolwiek dodatkowe określenia, które miałyby się stać nazwami dla poszczególnych przestępstw. Nazwy rodzajowe stosowane w dalszej części artykułu nie pochodzą zatem z samej ustawy, a z oficjalnego opracowania Kongresu USA i tym samym przynależą do sfery języka prawniczego, to jest języka II stopnia.

Amerykańska ustawa o nadużyciach oraz oszustwach komputerowych określiła siedem kategorii czynów zabronionych:

1) świadome uzyskanie dostępu do komputera bez uprawnienia lub z przekroczeniem posiadanych uprawnień oraz zdobycie w ten sposób informacji prawnie chronionych, w tym informacji obronnych lub dotyczących stosunków międzynarodowych, w sytuacji gdy z okoliczności wynika, że te informacje mogłyby zostać użyte na szkodę USA, a także nastąpiłoby przekazywanie takich informacji na korzyść jakiegokolwiek obcego państwa,
2) umyślne uzyskanie nieuprawnionego dostępu do komputera bez uprawnienia lub z przekroczeniem posiadanych uprawnień oraz zdobycie informacji bankowych lub finansowych, informacji przetwarzanych przez organy administracji publicznej lub informacji pochodzących z chronionych komputerów,
3) umyślne uzyskanie nieuprawnionego dostępu do niedostępnego publicznie komputera administracji, który jest przeznaczony do użytku wyłącznie na rzecz rządu USA lub jest używany przez rząd USA, działanie sprawcy zaś wpływa na ten użytek,
4) świadome oraz z zamiarem dokonania oszustwa uzyskanie dostępu do chronionego komputera bez uprawnienia lub z przekroczeniem uprawnień oraz osiągnięcie w ten sposób jakiejkolwiek korzyści majątkowej, chyba że przedmiotem oszustwa oraz jedyną korzyścią jest samo użycie komputera, a wartość tego użycia nie przekracza 5 tys. dolarów w ciągu roku,
5) umyślne spowodowanie szkód w chronionym komputerze przez świadome spowodowanie transmisji programu, informacji, kodu lub polecenia, a także uzyskanie dostępu bez uprawnienia,
6) świadoma oraz z zamiarem dokonania oszustwa nielegalna sprzedaż haseł lub podobnych informacji mogących służyć uzyskaniu dostępu do komputera bez uprawnień, pod warunkiem, że takie działanie może wpłynąć na obrót międzystanowy lub zagraniczny albo że dany komputer jest wykorzystywany przez rząd USA lub na jego rzecz,

7) transmitowanie, w ramach obrotu międzystanowego lub zagranicznego, jakichkolwiek komunikatów zawierających groźby spowodowania uszkodzeń chronionego komputera, groźby nieuprawnionego zdobycia informacji pochodzących z chronionego komputera lub ich uszkodzenia, a także żądania pieniędzy lub innych korzyści majątkowych w związku z uszkodzeniem chronionego komputera – w celu bezprawnego osiągnięcia korzyści majątkowych od jakiejkolwiek osoby[25].

Pojęcie przestępstwa związanego z komputerem

Trzy lata po napisaniu przez D. Parkera pierwszego, obszernego opracowania naukowego traktującego o fenomenie przestępczości komputerowej, a więc jeszcze pod koniec lat 70. XX w., problematyka zwalczania cyberzagrożeń została wprowadzona na grunt dokumentów rządowych. Pierwszym na świecie quasi-normatywnym aktem dotyczącym zwalczania tego typu działalności przestępnej stał się wydany w 1979 r. podręcznik dla pracowników amerykańskiego wymiaru sprawiedliwości zatytułowany *Computer Crime: Criminal Justice Resource Manual*[26]. Rządowy podręcznik, mający stać się ogólną instrukcją postępowania śledczych w sprawach przestępczości dotyczącej nowoczesnych technologii, został przygotowany na zamówienie Ministerstwa Sprawiedliwości USA (Department of Justice) we współpracy z Instytutem Naukowym Stanforda (Stanford Reserch Institute – SRI). Z uwagi na zaangażowanie w tę tematykę udział w pracach brał także sam D. Parker.

Pomimo wcześniejszego dorobku doktryny amerykańskiej, wyrażeniem stosowanym jako podstawowe na gruncie omawianego podręcznika stało się pojęcie przestępstwa związanego z komputerem[27] (w oryginale: *computer-related crime*). Warto zaznaczyć, że w samym tytule dokumentu zupełnie niekonsekwentnie posłużono się innym – niezdefiniowanym w podręczniku i stosowanym wówczas głównie w kontekście publicystycznym – wyrażeniem przestępczość komputerowa (w oryginale: *computer crime*[28]), w tekście opracowania zaś pojawiały się także inne, również niezdefiniowane w nim, pojęcia, m.in. nadużycie komputerowe[29]. Podstawowym określeniem omawianego opracowania pozostawało jednak przestępstwo związane z komputerem, które zostało wyjaśnione w treści tego dokumentu jako *Każde nielegalne działanie, które dla skutecznego ścigania wymaga wiedzy w zakresie technologii komputerowej*[30].

Na gruncie przytoczonej definicji przestępstwem związanym z komputerem mógł tym samym stać się każdy czyn zabroniony – niezależnie od dobra prawnie chronionego będącego przedmiotem ataku, modus operandi sprawcy czy jakichkolwiek innych cech przestępstwa – jeśli tylko jego ściganie wymagało od śledczych określonych umiejętności.

---

[25] Ustawa federalna *Computer fraud and abuse act* (18 U.S.C. 1030), lit. a, pkt 1–7. Tłumaczenie własne.

[26] *Computer Crime*: *Criminal Justice Resource Manual* [online], SRI International, National Criminal Justice Information and Statistics Service, California, 1979; Washington DC 1989, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf.

[27] S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*. Opracowanie jest dostępne w postaci elektronicznej na stronie internetowej pod adresem: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

[28] Zob. przypis nr 14.

[29] W oryginale: *computer abuse*.

[30] Tłumaczenie własne. W oryginale: *Any illegal act for which knowledge of computer technology is essential for a successful prosecution*, za: *Computer Crime: Criminal Justice Resource Manual*…, s. XXVI.

W rezultacie zastosowania wskazanej konstrukcji zakres semantyczny definicji stał się jednak zbyt szeroki i objął także takie kategorie czynów niedozwolonych, które w żadnym razie nie dotyczyły nowoczesnych technologii teleinformatycznych. Dla zaktualizowania wymagań „wiedzy komputerowej" od śledczych wystarczające było, aby w trakcie ścigania dowolnego czynu posłużyli się oni nowoczesnymi bazami danych, w których są przechowywane elektroniczne wersje kartotek. Obecnie takie działanie jest standardowym elementem pracy dochodzeniowo-śledczej.

Przestępstwem związanym z komputerem mógł być także każdy czyn, dla którego źródłem materiału dowodowego były dane zapisane na komputerze, na którym np. prowadzono listę nielegalnych transakcji, niekoniecznie wykonywanych za pośrednictwem sieci. Można także stwierdzić nieco ironicznie, że tak zdefiniowanym przestępstwem komputerowym mogła być nawet kradzież sprzętu komputerowego ze sklepu.

Przytoczona definicja pomijała jednak nowe, specyficzne formy przestępstw, które pojawiły się dopiero z chwilą rozwinięcia sieci oraz świadczonych za ich pośrednictwem usług, jak choćby ataki typu *dos*, *ddos*, *man-in-the-middle*, *cache poisoning* czy *pharming*, stanowiące różne formy zakłócania pracy systemów, podszywania się pod użytkowników lub dokonywania włamań komputerowych. Tak sformułowany zakres semantyczny definicji (pojęć) stanowił zatem rozwiązanie zupełnie nieefektywne, które nie tylko obejmowało zbyt wiele czynów, lecz także nie pozwalało na wyróżnienie jakichkolwiek cech szczególnych przestępczości związanej z komputerem. Pomimo przedstawionych wad przyjętej konstrukcji, analogiczne rozwiązanie zostało wprowadzone także do kolejnego, wydanego w 1989 r., opracowania Ministerstwa Sprawiedliwości USA[31].

Powtórna implementacja oryginalnego zapisu stworzonego jeszcze w połowie lat 70. XX w. spotkała się jednak z gruntowną krytyką[32]. Ostatecznie należy zauważyć, że w dobie postępującej informatyzacji coraz mniej czynności wykonuje się z wykluczeniem udziału systemów teleinformatycznych, co jednak nie powinno oznaczać logicznego przeniesienia całej przestępczości do sfery cyberprzestrzeni. Definicja odwołująca się do „obszaru przestępczości komputerowej" powinna przy tym umożliwiać precyzyjne wydzielenie tego typu działalności z innych form przestępczości. W innym przypadku tworzenie nowych, szczególnych regulacji prawnych, zarówno materialnych, jak i procesowych, nastawionych na walkę z nowoczesnymi zagrożeniami, stałoby się niemożliwe.

Wyrażenie przestępstwo związane z komputerem było wykorzystywane w kolejnych latach także w licznych aktach międzynarodowych, które proponowały swoje definicje tego pojęcia. Przykładowo: na potrzeby zalecenia Nr R (89) 9[33] w sprawie przestępczości związanej z komputerami wydanego przez Komitet Ministrów Rady Europy w 1989 r. grupa ekspertów, która przygotowywała dokument, postanowiła określić znaczenie analizowanego pojęcia przez stworzenie jego typologii, a zatem przez zbudowanie wykazu czynów, a nie określenie ich cech rodzajowych. Jako uzasadnienie odstąpienia od budowy klasycznej definicji pojęcia wskazano

[31] *Computer Crime: Criminal Justice Resource Manual*, b.m.w. 1989, U.S. Department of Justice, National Institute of Justice.

[32] Np. M. Goodman, *Making Computer Crime Count*, „FBI Law Enforcement Biulettin", 2001, t. 70, s. 12. Biuletyn dostępny na stronie internetowej pod adresem: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2001-pdfs/aug01leb.pdf. Także: R.W. Aldrich, *Cyberterrorism and Computer Crimes*: *Issues Surrounding the Establishment of an International Legal Regime*. Materiał dostępny na stronie internetowej pod adresem: http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf.

[33] Council of Europe, *Computer-Related Crime: Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems*, Strasbourg 1989.

trudności w wypracowaniu wspólnego, jednolitego sposobu postrzegania tego typu przestępczości. Spowodowało to wymienienie we wspomnianym zaleceniu tych kategorii czynów, które powinny być penalizowane właśnie jako przestępstwa związane z komputerem. Do czynów obligatoryjnie kwalifikowanych w ten sposób (znajdujących się na tzw. liście minimalnej – obligatoryjnej) zaliczono wówczas: oszustwo związane z komputerem, fałszerstwo komputerowe, uszkodzenie danych lub programów, sabotaż komputerowy, nieuprawniony dostęp do zasobów, nieuprawniony podsłuch, bezprawne powielanie chronionych programów komputerowych oraz bezprawne powielanie topografii półprzewodników. Dodatkowo wskazano cztery kolejne kategorie przestępstw, co do których nie osiągnięto pełnego konsensusu w ich zakwalifikowaniu przy tworzeniu tzw. listy opcjonalnej do grupy przestępstw związanych z komputerem. Znalazły się na niej: nieuprawniona modyfikacja danych lub oprogramowania, szpiegostwo komputerowe, wykorzystywanie komputera bez zezwolenia oraz nieuprawione używanie programu komputerowego[34]. Z wyjątkiem bezprawnego kopiowania topografii półprzewodników wszystkie wymienione kategorie działań odnosiły się bezpośrednio do szeroko rozumianego przetwarzania danych i łączyły, w sposób charakterystyczny dla dawniejszych dokumentów, sferę stricte karną z ochroną praw autorskich. W typologii nie wyodrębniono także specjalistycznych ataków komputerowych jako osobnej kategorii, starając się uzyskać bardziej definicyjny, ogólny charakter. Warto zaznaczyć, że pomimo oparcia przywołanego dokumentu Rady Europy na ustaleniach wcześniejszego, pochodzącego z połowy lat 80. XX w., raportu OECD zatytułowanego *Przestępstwa związane z komputerem: analiza polityki legislacyjnej*[35], wcześniejsze opracowanie międzynarodowe – co zostało już zaznaczone – zawierało określenie nadużycie komputerowe, a nie przestępstwo związane z komputerem.

Pojęcie przestępstwa związanego z komputerem było wymieniane także w regulacjach ONZ, m.in. w *Rezolucji VIII Kongresu ONZ w sprawie zapobiegania przestępczości i postępowania z przestępcami* (1990), w której tytule się pojawiło (*computer-related crime*)[36]. Ta rezolucja jednak nie tylko nie oferowała żadnej definicji tego pojęcia, lecz także wprowadzała inne, nieznane dotychczas, również niezdefiniowane wyrażenia: nadużycia komputerów[37] (w przeciwieństwie do nadużycia komputerowego) oraz nadużycia związanego z komputerem[38].

Jednocześnie te pojęcia były traktowane synonimicznie. Pomimo niespójności oraz nieokreśloności przyjętej siatki pojęciowej, rezolucja jest często wskazywana jako wyraz zaangażowania ONZ w problematykę przeciwdziałania nowoczesnym formom przestępczości. Podkreśla się jej ponadeuropejski zasięg stawiający poruszany temat na arenie światowej oraz kierunki działań proponowane w treści rezolucji, m.in. koniecz-

[34] Tamże, s. 36 i nast.

[35] *Computer-related crime: Analysis*…

[36] Rezolucja opublikowana w: *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Havana, 27 August – 7 September 1990: report prepared by the Secretariat, United Nations publication, Sales No. E.91.IV.2), sekcja C, rezolucja nr 9, s. 140 i nast. Pełny tekst raportu dostępny na stronie internetowej pod adresem: http://www.asc41.com/UN_Congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/026%20ACONF.144.28.Rev.1%20Eighth%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf.

[37] Tłumaczenie własne. W oryginale *abuse of computers*.

[38] Tłumaczenie własne. W oryginale *computer-related abuse*.

ność uzupełnienia prawodawstwa o nowe rodzaje czynów bezprawnych[39]. Chaotyczność terminologii zastosowanej na gruncie rezolucji należy uznać za istotną wadę opracowania, które, stawiając sobie za jeden z głównych celów identyfikację niedostatków obowiązującego prawa, nie określało jednoznacznie samego przedmiotu prowadzonej analizy. Wyrażenie przestępstwo związane z komputerem zostało wykorzystane przez ONZ także w wydanym w 1994 r. podręczniku, który był kolejnym opracowaniem tej organizacji.

Pojęcie bezprawnego użycia komputera

Pojęcie bezprawnego użycia komputera pochodzi z wydanej w 1990 r. brytyjskiej ustawy *Computer Misuse Act*[40], będącej pierwszą na Wyspach i nadal obowiązującą kodyfikacją prawa nakierowaną na zwalczanie przestępstw popełnianych z użyciem komputera. Ta ustawa wprowadziła do zasobu słownictwa prawniczego języka angielskiego nowe, nieznane dotychczas w doktrynie określenie: bezprawne użycie komputera (w oryginale: *computer misuse*), które znaczeniowo miało zastępować inne, rozpoznawane już na arenie międzynarodowej wyrażenia: nadużycie komputerowe i przestępczość związana z komputerem. Z uwagi na niuanse językowe, niezbędne staje się poczynienie uwagi o charakterze technicznym: anglojęzyczne wyrazy *misuse* oraz *abuse* (wykorzystywane odpowiednio w dwóch różnych wyrażeniach: *computer misuse* oraz *computer abuse*) można tłumaczyć synonimicznie jako „nadużycie”[41]. Tym samym, na gruncie językowym, polskojęzyczna kategoria „nadużycie komputerowe” mogłaby obejmować łącznie pojęcia: *computer abuse* (omówione wcześniej) oraz *computer misuse*, choć z punktu widzenia prawnego błędnie stawiałoby to znak równości między zwrotami zachowującymi w oryginale różne brzmienia. Aby uniknąć takiej sytuacji, zwrot *computer misuse* należy tłumaczyć jako „bezprawne użycie komputera”, mając na uwadze brytyjskie rozumienie prawniczego zwrotu *misuse* oraz przypadki jego występowania na gruncie angielskiego ustawodawstwa[42].

Z uwagi na brak ustawowej definicji omawianego pojęcia znaczenie „bezprawnego użycia komputera” musi być rekonstruowane na podstawie typologii czynów zabronionych charakteryzowanych w ustawie. Podobnie jak w przypadku amerykańskiej ustawy karnej z 1986 r., także ustawa brytyjska została skonstruowana w sposób typowo kodeksowy (np. *kto uzyskuje*...), a typizowane w niej czyny nie zostały nazwane żadnymi określeniami rodzajowymi (np. *hacking*). Tak samo kodeks karny nie posługuje się terminami zabójstwo i morderstwo. W brytyjskiej ustawie można zatem znaleźć wyłącznie opisy poszczególnych typów przestępstw zawarte w hipotezach przepisów. W oryginalnym kształcie ta ustawa przewidywała penalizację trzech następujących kategorii czynów:

[39] Na te cechy wskazuje m.in. A. Adamski w: tenże, *Prawo karne komputerowe*…, s. 9–10.

[40] *Computer Misuse Act 1990*. W tłumaczeniu własnym: *Ustawa o bezprawnym użyciu komputera z 1990 r.* Pełny oryginalny tekst aktu dostępny na stronie internetowej parlamentu brytyjskiego pod adresem: http://www.legislation.gov.uk/ukpga/1990/18/enacted.

[41] Zob. np. internetowy słownik Mirriam-Webster dostępny na stronie internetowej pod adresem: http://www.merriam-webster.com/dictionary/misuse.

[42] Wyraz *misuse* jest wykorzystywany m.in. przez brytyjską ustawę antynarkotykową *Drugs Misuse Act 1986*. Ta ustawa porusza problem nie tylko samego używania środków odurzających, lecz także ich produkcji czy sprzedaży, wykraczając tym samym poza zakres rozumienia polskiego wyrażenia nadużywanie narkotyków.

1) nieuprawnionego, umyślnego dostępu do zasobów komputera polegającego na użyciu jakiejkolwiek funkcji komputera z zamiarem zapewnienia dostępu do jakiegokolwiek programu lub danych przechowywanych na jakimkolwiek komputerze,
2) nieuprawnionego dostępu, o którym mowa w pkt 1, z zamiarem popełnienia dalszych przestępstw lub ułatwienia ich popełnienia dowolnej osobie, w dowolnym czasie,
3) nieuprawnionej modyfikacji zasobu komputerowego dokonywanej w celu zakłócenia poprawnego funkcjonowania jakiegokolwiek komputera, uniemożliwienia lub utrudnienia dostępu do programu, a także zakłócenia działania programu lub naruszenia wiarygodności danych[43].

Pojęcie przestępstwa komputerowego

Już od drugiej połowy lat 70. XX w. w piśmiennictwie oprócz wyrażenia nadużycie komputerowe było popularyzowane także inne określenie nowego zjawiska przestępnego – przestępczość komputerowa. Tym pojęciem posłużyli się m.in. Ulrich Sieber, uważany za jednego z ojców „prawa informatycznego", oraz August Bequai, którzy wprowadzili je do tytułów swoich opracowań wydanych odpowiednio: w 1977[44] oraz 1978[45] r. Ogólne rozumienie pojęcia prezentowane w tych opracowaniach nie odbiegało jednak od sposobu charakteryzowania wcześniej zdefiniowanego wyrażenia nadużycie komputerowe. W następnych latach wyrażenie przestępstwo komputerowe pojawiało się wielokrotnie także w opracowaniach amerykańskich (m.in. w amerykańskiej prasie), jednak bez stworzenia definicji tego pojęcia, która stałaby się szeroko rozpoznawana w literaturze przedmiotu.

Cztery lata po uchwaleniu przez VIII Kongres ONZ rezolucji w sprawie przestępstw związanych z komputerem (opisanej już przy omawianiu tego pojęcia) Organizacja Narodów Zjednoczonych podjęła kolejną inicjatywę odnoszącą się do problematyki zwalczania nowoczesnych form przestępczości. Wyrazem tego stało się wydanie w 1994 r. *Podręcznika w sprawie zapobiegania oraz kontroli przestępstw związanych z komputerem*[46]. Dostrzegając dotychczasowe trudności w ustaleniu spójnej siatki pojęciowej (odczuwalne już globalnie), a także chcąc nadać podręcznikowi możliwie uniwersalny charakter, ponownie odstąpiono od budowy ogólnej definicji na rzecz ujęcia funkcjonalnego (zastosowano zatem rozwiązanie analogiczne do rozwiązania zawartego w opracowaniu wydanym w 1989 r. przez Komitet Ministrów Rady Europy). Zamiast klasycznej definicji zaproponowano wykaz zdarzeń, które miały być określane – co wymaga zaznaczenia – zamiennie, mianem przestępstwa związanego z komputerem lub przestępstwa komputerowego[47]. Na gruncie omawianego podręcznika ONZ oba wyrażenia stały się więc tak naprawdę synonimami i nie tylko postawiły pod znakiem zapytania jakąkolwiek zasadność ich różnicowania, lecz także uczyniły to wbrew przyjętym zasadom tworzenia oraz interpretacji przepisów, które jednoznacznie nakazują, aby dwóm różnym pojęciom nadawać zawsze dwa różne znaczenia, jednemu zaś – zawsze jedno i to samo.

[43] *Computer Misuse Act 1990*, art. 1–3.
[44] U. Sieber, *Computercriminalität und Strafrecht*, Köln 1977.
[45] A. Bequai, *Computer Crime*, Heath (Massachusetts) 1978.
[46] *United Nations Manual on the prevention and control of computer-related crime*. Tekst dostępny na stronie internetowej pod adresem: http://www.uncjin.org/Documents/EighthCongress.html.
[47] Tłumaczenie własne. W oryginale odpowiednio: *computer-related crime* oraz *computer crime*.

Pomimo deklarowanej równości pojęć, w dokumencie wyraźnie częściej posługiwano się określeniem przestępstwa komputerowego, które zostało użyte także przy próbie nazwania zjawiska. W celu przybliżenia zakresu semantycznego tak określonej kategorii czynów, w punkcie 22 opracowania została wprowadzona quasi-definicja, zgodnie z którą *Przestępstwo komputerowe może polegać na podejmowaniu tradycyjnych w swojej naturze działań przestępnych, takich jak kradzież, oszustwo, fałszerstwo oraz wyrządzanie szkód, które zasadniczo wszędzie podlegają sankcji karnej. Komputery wytworzyły jednak także wiele nowych, potencjalnych działań bezprawnych lub możliwości nadużyć, które mogą lub powinny być uważane za przestępstwa*[48].

W przytoczonym zapisie w sposób czytelny zwrócono uwagę na rozróżnienie dwóch głównych kategorii czynów, które mogą być określone jako przestępczość komputerowa. Z jednej strony są to „tradycyjne z natury" działania przestępne, dla których komputer staje się nowym narzędziem przestępstwa (w tym tworzy nowe, specyficzne środowisko do ich popełniania), z drugiej zaś – zupełnie nowe typy czynów bezprawnych, niepoddające się subsumpcji. W podręczniku podkreślano też, że komputer może stać się nie tylko narzędziem, lecz także przedmiotem, czyli innymi słowy – celem tak określonego czynu. Zaprezentowane rozróżnienie na kategorie typowych oraz nowych form przestępstw stało się w kolejnych latach cechą charakterystyczną omawianego tu pojęcia przestępstwa komputerowego.

Poza przytoczoną definicją w podręczniku ONZ prezentowano także wykaz typowych przestępstw komputerowych, w którym zostały zawarte następujące kategorie czynów: oszustwo przez komputerową manipulację (odnoszące się do zaburzenia poprawnego funkcjonowania urządzenia), fałszerstwo komputerowe, uszkodzenie lub modyfikacja przetwarzanych danych lub oprogramowania, nieuprawniony dostęp do systemu komputerowego lub usługi oraz nieuprawnione powielanie chronionego prawem programu komputerowego. Pomimo przyjęcia nieco innego nazewnictwa, przedstawiony wykaz pozostawał w istocie zbieżny z listą przestępstw stworzoną osiem lat wcześniej przez ekspertów OECD na potrzeby wydanej przez tę organizację analizy polityki legislacyjnej. Zważywszy na niezwykle szybkie tempo rozwoju technologicznego oraz podążający za nim rozwój form i metod nowoczesnej przestępczości, brak nowych, precyzyjnych zapisów spełniających standardy prawa karnego należy uznać za przejaw nienadążania regulacji prawnych za wymaganiami, jakie stawia otaczająca nas rzeczywistość. Korzystanie z już przyjętych rozwiązań świadczy o tym, jak trudnym zadaniem jest wypracowywanie na arenie międzynarodowej kompromisów w odniesieniu do tworzenia nowych, wspólnych regulacji karnych.

Pojęciem przestępstwa komputerowego w Polsce posłużył się także Andrzej Adamski, zawierając je w swoim opracowaniu zatytułowanym *Prawo karne komputerowe*[49]. Książka, wydana w 2000 r., jest uznawana za kanon polskich rozważań prawniczych dotyczących charakteryzowania zjawiska przestępczości komputerowej. A. Adamski zwrócił uwagę na istotne wady siatki pojęciowej stosowanej w prawie karnym komputerowym i zaprezentował własną, poszerzoną charakterystykę przestępstwa komputerowego, wprowadzając podział definicyjny przestępczości komputerowej na

[48] Tłumaczenie własne. W oryginale: *Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well*.

[49] A. Adamski, *Prawo karne komputerowe*…, s. 30 i nast.

dwa odrębne ujęcia: materialno-prawne oraz procesowe. W ramach ujęcia materialno-prawnego, stosując kryterium roli, w jakiej mogą występować komputery w działaniu przestępnym, wyróżnił dwie subkategorie przestępczości komputerowej – w rozumieniu wąskim (tzw. przestępstwa stricte komputerowe) oraz szerokim:

1) przestępstwami stricte komputerowymi A. Adamski nazwał te czyny bezprawne, które są skierowane przeciwko systemom, danym lub programom, czyli czyny, w których nowoczesne technologie informatyczne stanowią bądź to sam przedmiot zamachu, bądź też środowisko do jego przeprowadzenia. Jak zauważa autor, w tym przypadku następuje swoiste genetyczne powiązanie nowoczesnych form przestępczości z technologią komputerową. Przestępstwa należące do tej kategorii trzeba odnieść do czynów naruszających tzw. atrybuty bezpieczeństwa danych, szczególnie ich poufność, integralność oraz dostępność. Te cechy oznaczają odpowiednio, że dane przetwarzane w systemach teleinformatycznych nie zostały ujawnione osobom nieuprawnionym (zdarzenie nazywane także kompromitacją danych); nie zostały one w sposób nieuprawniony zmodyfikowane ani uszkodzone oraz są dostępne dla uprawnionych użytkowników, zgodnie z zasadami panującymi w danym systemie (np. nie dokonano przeciążenia łączy, co uniemożliwiałoby odwołanie się do danego zasobu),
2) przestępstwami komputerowymi w ujęciu szerokim zostały nazwane wszystkie czyny, których ustawowa regulacja wprowadza expressis verbis wykorzystanie komputera do ich popełnienia, np. przestępstwa z art. 130 § 3, art. 267–269, art. 278 § 2, art. 285 i art. 287 *Kodeksu karnego*[50]. Jak zauważa A. Adamski są to przestępstwa komputerowe (…) *nie ze względu na przedmiot zamachu, lecz ustawowo określony sposób działania sprawcy*[51]. Dobrem prawnie chronionym nie jest tutaj samo funkcjonowanie systemu, lecz różne inne dobra. Przestępstwa należące do tej grupy A. Adamski sugeruje nazywać „przestępstwami komputerowymi" z dodaniem określenia przedmiotu ochrony, np. „przestępstwo komputerowe przeciwko wiarygodności dokumentów".

Istotnym uzupełnieniem zaprezentowanego podziału jest także sposób uwzględnienia pozostałych czynów (nienależących do żadnej z kategorii przestępstw komputerowych), w których komputer może jednak wystąpić w roli narzędzia do popełnienia „klasycznego" przestępstwa, np. przestępstwa zniewagi, zniesławienia, groźby karalnej, propagacji treści prawnie zabronionych lub oszustwa. Dla tej kategorii zdarzeń A. Adamski przyjmuje nazwę „przestępstwa popełniane z użyciem (wykorzystaniem) komputera". Tym mianem są określane te czyny, których ustawowa regulacja nie zakłada użycia komputera jako przesłanki konstytuującej czyn, lecz możliwe jest ich popełnienie także z zastosowaniem systemów teleinformatycznych (szczególny, lecz niewymagany przepisem rodzaj modus operandi sprawcy).

W ujęciu procesowym przestępstwami komputerowymi, na gruncie opracowania A. Adamskiego, określono (…) *wszelkie czyny zabronione przez prawo karne, których ściganie wymaga od organów wymiaru sprawiedliwości uzyskania dostępu do informacji przetwarzanej w systemach komputerowych lub teleinformatycznych. Pojęcie przestępstw komputerowych w aspekcie procesowym obejmuje zatem zarówno przypadki, w których system komputerowy stanowi przedmiot, jak i narzędzie zamachu*[52].

[50] *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 5 lipca 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137) – przyp. red.

[51] A. Adamski, *Prawo karne komputerowe*…, s. 31–32.

[52] Tamże, s. 34.

Pojęcie przestępstwa powiązanego z technologią informacyjną

Pojęcie przestępstwa powiązanego z technologią informacyjną, przyjmujące w oryginale brzmienie: *Offence Connected with Information Technology*[53], zostało zdefiniowane w związku z pracami prowadzonymi nad *Zaleceniem Komitetu Ministrów Rady Europy Nr R (95)13 z dnia 11 września 1995 r. w sprawie „Problemów karnoprocesowych związanych z technologią przetwarzania informacji"*[54].

Powyższy dokument stał się pierwszym istotnym wyrazem międzynarodowego zainteresowania problematyką podejmowania czynności procesowych ze szczególnym uwzględnieniem ich roli dowodowej w zwalczaniu nowoczesnych form przestępczości[55]. Analiza definicji zawartej w dokumencie pozwoli zaprezentować podejście, które zostało stworzone specjalnie z myślą o zagadnieniach karnoprocesowych. Zgodnie z memorandum wyjaśniającym (*explanatory memorandum*), stanowiącym funkcjonalne uzupełnienie treści samego *Zalecenia...*, przestępstwem powiązanym z technologią informacyjną jest *Każde przestępstwo, w którego procesie śledczym właściwe organy wymiaru sprawiedliwości muszą uzyskać dostęp do informacji przetwarzanych lub przekazywanych w systemach komputerowych lub* (...) *systemach przetwarzania danych występujących w postaci elektronicznej*[56].

Na potrzeby *Zalecenia...* pojęcia systemy komputerowe oraz systemy przetwarzania danych zostały ujęte możliwie szeroko i objęły w zasadzie wszelkie przykłady technologii informacyjnych, w tym zarówno pojedyncze (odseparowane od środowiska cyfrowego) komputery, jak i całe sieci. Jak można przeczytać we wprowadzeniu do definicji, systemy w tak określonym przestępstwie mogą być wykorzystane jako:

1) narzędzia do popełnienia przestępstwa,
2) przedmiot (cel) przestępstwa,
3) środowisko popełnienia przestępstwa,
4) środowisko, w którym mogą się pojawić dowody przestępstwa; w tym przypadku sam system nie musi stanowić żadnego elementu w procesie popełniania przestępstwa.

Pojęcie cyberprzestępstwa

Pojęcie cyberprzestępstwo (w oryginale: *cybercrime*) jest obecnie jednym z najszerzej rozpoznawanych pojęć używanych do określenia nowoczesnych form przestępczości komputerowej. Swoją rangę zawdzięcza wprowadzeniu go do konwencji Rady Europy o cyberprzestępczości[57] (dalej: konwencji), zwanej też czasami konwen-

[53] W skrócie też *IT offence* – 'przestępstwo dotyczące IT'.

[54] *Problems of Criminal Procedural Law Connected with Information Technology. Recommendation No. R(95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995 and explanatory memorandum*, Council of Europe Publishing, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 [dostęp: 20 VI 2016].

[55] A. Adamski, *Prawo karne komputerowe*…, s. XVII.

[56] Tłumaczenie własne. W oryginale: *Any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or, as they are referred to above, electronic data processing systems*.

[57] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.* (Dz.U. z 2015 r. poz. 728) – przyp. red. Tytuł oryginalny: *Convention on Cybercrime*, CETS Nr: 185. Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.

cją z Budapesztu lub konwencją budapesztańską[58], będącej wynikiem jednej z najistotniejszych inicjatyw na arenie międzynarodowej odnoszących się do regulacji zwalczania przestępczości komputerowej. Konwencja została otwarta do podpisu 23 listopada 2001 r., w życie zaś weszła 1 lipca 2004 r., po uzyskaniu ratyfikacji pięciu państw (wymogiem było, aby przynajmniej trzy z nich należały do Rady Europy). Łącznie podpisało ją 47 państw, w tym Polska, która stała się sygnatariuszem dokumentu już w dniu jego otwarcia do podpisu[59]. Wśród ważnych sygnatariuszy należy wskazać Wielką Brytanię, Niemcy, Francję, Szwecję, Rosję, a także Stany Zjednoczone i Japonię[60]. W dniu 28 stycznia 2003 r. w Strasburgu został otwarty do podpisu także *Protokół dodatkowy do Konwencji w sprawie kryminalizacji aktów natury rasistowskiej oraz ksenofobicznej popełnianych za pośrednictwem systemów komputerowych*[61]. Protokół wszedł w życie 1 marca 2006 r. (po uzyskaniu pięciu ratyfikacji). Polska podpisała go 21 lipca 2003 r.[62]

Choć nasz kraj oficjalnie nie ratyfikował konwencji, o której mowa, aż do 2015 r. (ustawa ratyfikacyjna – 27 maja 2015 r.[63]), to krajowe ustawodawstwo karne zostało dostosowane do jej zapisów znacznie wcześniej, szczególnie na mocy *Ustawy z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń*[64].

Omawiając szczegółowe zapisy konwencji z Budapesztu, należy zauważyć, że nie wprowadzono w niej definicji pojęcia cyberprzestępstwo. Nakazano tym samym rekonstrukcję jego znaczenia na podstawie opisanych w akcie rodzajów czynów zabronionych. Podobnie jak w przypadku wielu innych dokumentów, także i tu zastosowano tzw. ujęcie funkcjonalne, skupiające się na opisach hipotez czynów, które powinny być penalizowane w systemach prawnych państw stron umowy, oraz tworzeniu katalogów takich czynów. Sam termin cyberprzestępstwo lub cyberprzestępczość (w oryginale: *cybercrime*), stosowane wymiennie, jest użyte w konwencji dziewięciokrotnie, przy czym tylko raz w samej treści postanowień aktu (w odniesieniu do współpracy międzynarodowej), a pozostałe osiem razy w preambule niestanowiącej materiału normatywnego. Uwzględniając kryterium „dobra prawnie chronionego" będącego przedmiotem ataku, czyny stypizowane w konwencji zostały podzielone na cztery kategorie (wskazane w tytułach 1–4 rozdziału II konwencji): przestępstwa przeciwko poufności, integralności i dostępności danych informatycz-

int/Treaty/EN/Treaties/Html/185.htm.

[58] Zob. np. na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Convention_on_Cybercrime.

[59] Aktualne informacje dotyczące sygnatariuszy można znaleźć na oficjalnej stronie internetowej konwencji, dostępnej pod adresem: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

[60] Konwencję podpisały cztery państwa niebędące członkami Rady Europy, choć z tej grupy ratyfikowało ją wyłącznie USA (29 września 2006 r.); w USA konwencja weszła w życie 1 stycznia 2007 r.

[61] Tytuł oryginalny: *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, CETS Nr: 189. Pełny tekst protokołu jest dostępny na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm. Polska wersja: *Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28 stycznia 2003 r*. (Dz.U. z 2015 r. poz. 730).

[62] Aktualne informacje dotyczące sygnatariuszy protokołu można znaleźć na oficjalnej stronie internetowej konwencji, dostępnej pod adresem: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG.

[63] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r*. (Dz.U. z 2001 r. poz. 728) – przyp. red.

[64] Dz.U. z 2004 r. Nr 69 poz. 626.

nych i systemów[65]; przestępstwa komputerowe[66]; przestępstwa ze względu na charakter zawartych informacji[67] oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[68]. Klasyfikację poszczególnych czynów zaprezentowano poniżej:

I. Przestępstwa przeciwko poufności, integralności oraz dostępności danych oraz systemów komputerowych:
   - nielegalny dostęp – rozumiany jako dostęp do całości lub części systemu bez posiadania uprawnień do takiego działania,
   - nielegalne przechwytywanie danych – rozumiane jako przechwytywanie wszelkich transmisji danych komputerowych nieposiadających charakteru publicznego, w tym przechwytywanie ulotu elektromagnetycznego,
   - naruszenie integralności danych – rozumiane jako niszczenie, wykasowywanie, uszkadzanie i usuwanie danych informatycznych oraz dokonywanie ich zmian,
   - naruszenie integralności systemu – rozumiane jako poważne zakłócenie funkcjonowania systemu komputerowego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie i dokonywanie zmian lub usuwanie danych informatycznych,
   - niewłaściwe wykorzystanie urządzeń – rozumiane jako posiadanie, wytwarzanie lub inne formy udostępniania urządzeń lub programów zaprojektowanych albo przystosowanych do popełniania wymienionych wyżej czynów albo kodów dostępowych lub innych danych pozwalających na uzyskanie dostępu do całości lub części systemu komputerowego oraz handel nimi.

II. Przestępstwa komputerowe:
   - fałszerstwo komputerowe – rozumiane jako bezprawne wprowadzenie, dokonywanie zmian, wykasowywanie lub ukrywanie danych informatycznych, skutkujące ich nieautentycznością, z zamiarem wykorzystania tak przekształconych danych jako autentyczne,
   - oszustwo komputerowe – rozumiane jako powodowanie strat majątkowych z zamiarem bezprawnego uzyskania dla siebie lub osoby trzeciej korzyści majątkowych przez wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych lub też ingerencję w funkcjonowanie systemu komputerowego.

III. Przestępstwa ze względu na charakter informacji:
   - przestępstwa związane z pornografią dziecięcą – polegające na wytwarzaniu, udostępnianiu, posiadaniu lub pozyskiwaniu materiałów pornograficznych z udziałem małoletniego (domyślnie konwencja ustala granicę 18 lat, zezwalając jednak państwom na obniżenie cezury wieku do lat 16).

IV. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych – rozumiane jako działania kierowane przeciwko prawom autorskim lub prawom pokrewnym na skalę komercyjną, przy zastosowaniu systemu komputerowego.

---

[65] W oryginale: *Offences against the confidentiality, integrity and availability of computer data and systems*.

[66] W oryginale: *Computer-related offences*. Wydaje się, że poprawne tłumaczenie powinno brzmieć: *przestępstwa związane z komputerami*.

[67] W oryginale: *Content-related offences*.

[68] W oryginale: *Offences related to infringements of copyright and related rights.*

Zgodnie z definicjami przyjętymi na gruncie konwencji:

- system informatyczny to każde urządzenie lub grupa połączonych lub wiązanych urządzeń, z których przynajmniej jedno przetwarza dane w zautomatyzowany, zaprogramowany sposób,
- dane informatyczne to wszelkie przedstawienie faktów, informacji lub pojęć w formie odpowiedniej do przetwarzania w systemie, w tym także oprogramowanie zdolne do wykonywania określonych funkcji.

Przytoczony wykaz czynów zabronionych uzupełniają zapisy wspomnianego *Protokołu dodatkowego do Konwencji...* (art. 3–7). Ten dokument wprowadza szczególną penalizację czynów dokonywanych za pośrednictwem systemów komputerowych, które polegają na:

- publicznym udostępnianiu rasistowskich oraz ksenofobicznych materiałów w systemach komputerowych,
- kierowaniu gróźb karalnych o podłożu rasowym lub ksenofobicznym, przekazywanych przez systemy komputerowe,
- publicznym znieważaniu osób na tle rasistowskim lub ksenofobicznym, dokonywanym przy użyciu systemów komputerowych,
- publicznym udostępnianiu przez systemy komputerowe materiałów odmawiających ludziom praw lub im umniejszających na tle rasistowskim lub ksenofobicznym, a także pochwalających lub usprawiedliwiających zbrodnie ludobójstwa lub inne zbrodnie przeciwko ludzkości, zdefiniowane na mocy odpowiednich przepisów międzynarodowych,
- udzielaniu pomocy w popełnieniu lub ułatwianiu popełnienia któregokolwiek z powyższych czynów zabronionych.

Przy omawianiu powyższego wykazu czynów bezprawnych, określanych łącznie – zgodnie z tytułem konwencji – mianem „cyberprzestępstw", należy podkreślić jego szeroki zakres przedmiotowy oraz złożoność. Obejmuje on wiele zróżnicowanych czynów, które są kierowane przeciw różnym dobrom prawnie chronionym. Z uwagi na szeroki zakres opisów poszczególnych czynów, ich szczegółowy modus operandi może przybierać rozliczne formy i treści. Ponadto zawiera on zarówno te czyny, których popełnienie jest możliwe wyłącznie w cyberprzestrzeni, jak i te, w których systemy teleinformatyczne są wyłącznie narzędziami, to jest czyny, których popełnienie nie narusza samej pracy systemów czy bezpieczeństwa przetwarzanych w nich danych. Przestępstwa związane z propagowaniem pornografii dziecięcej, nielegalnym kopiowaniem materiałów chronionych prawem autorskim czy udostępnianiem materiałów rasistowskich także stają się cyberprzestępstwami, jeśli są popełnione z wykorzystaniem komputera.

Jako ciekawostkę warto także zauważyć, że w *Raporcie wyjaśniającym*[69] do konwencji o cyberprzestępczości pojęcie *cybercrime* pojawia się tylko raz w tytule samej konwencji. Raport wprowadza natomiast inne, nieznane na gruncie konwencji budapesztańskiej, pojęcia: czyny bezprawne cyberprzestrzeni oraz przestępstwa cyberprzestrzeni[70], odwołujące się zarówno do czynów skierowanych przeciw integralności, dostępności i poufności systemów komputerowych oraz sieci telekomunikacyjnych, jak i czynów zawierających element wykorzystania takich sieci oraz oferowanych przez nie usług do popełnienia tradycyjnych przestępstw[71].

[69] *Explanatory Report* [online], http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm [dostęp: 20 VI 2016].
[70] Tłumaczenie własne. W oryginale: *cyber-space offences*.
[71] *Explanatory Report*…, cz. 2, pkt 8.

W dokumentach krajowych pojęcie cyberprzestępstwo było wykorzystywane po przyjęciu konwencji o cyberprzestępczości w wielu rządowych programach ochrony cyberprzestrzeni. Zostało wprowadzone w pierwszej kolejności do programu USA (2003 r.), a następnie programów Polski (2009 r.), Anglii (2009 r. i 2011 r.), Niemiec (2011 r.), Francji (2011 r.) oraz Holandii (2011 r.). Pojawia się także w *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[72], nazywanej na wcześniejszych etapach prac legislacyjnych *Rządowym Programem Ochrony Cyberprzestrzeni na lata 2011–2016*. Ten dokument to kontynuacja wcześniejszego *Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011*. Pomimo występowania omawianego pojęcia na szeroką skalę, jedynie dwa ze wskazanych wyżej rządowych programów wprowadzają jego definicję – są nimi strategia francuska oraz *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*.

Pochodzący z 2011 r. rządowy program Francji, zatytułowany *Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji*[73], definiuje cyberprzestępstwo jako *Czyny naruszające postanowienia umów międzynarodowych lub regulacji krajowych, wykorzystujące sieci lub systemy informacyjne jako narzędzia do popełnienia deliktu lub przestępstwa, lub jako cel bezprawnego zamachu*[74]. Wymieniony system informacyjny to zorganizowany zbiór zasobów sprzętowych, programowych, osobowych oraz organizacyjnych (proceduralnych), służący do przetwarzania oraz przesyłania informacji[75].

Inaczej niż w przypadku zapisów zawartych w konwencji o cyberprzestępczości, przytoczona definicja nie buduje zamkniętego wykazu czynów bezprawnych, wskazując w zastępstwie dwie przesłanki, których łączne spełnienie jest niezbędne, aby dany czyn uznać za cyberprzestępstwo:

1) czyn musi być penalizowany na mocy przepisów odrębnych – krajowych bądź międzynarodowych,
2) sieci lub systemy teleinformatyczne muszą występować w takim czynie przynajmniej w jednej z dwóch ról – jako narzędzie popełnienia przestępstwa lub jako przedmiot zamachu.

Z punktu widzenia analizy pojęciowej ciekawe określenie cyberprzestępstwa prezentuje *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* przyjęta 25 czerwca 2013 r. uchwałą Rady Ministrów RP, wprowadzająca jedną z najkrótszych, choć jednocześnie najnowocześniejszych charakterystyk omawianego pojęcia. Cyberprzestępstwo jest tu określane jako *Czyn zabroniony popełniony w obszarze cyberprzestrzeni*. Charakterystyczną cechą przytoczonego określenia jest jego wyraźne odwoływanie się do pojęcia cyberprzestrzeń. Inaczej niż w przypadku omawianych wcześniej definicji zagranicznych, definicja krajowa nie określa ani wykazów czynów zabronionych, które powinny być penalizowane jako cyberprzestępstwa, ani szczegóło-

[72] Pełny tekst dokumentu jest dostępny na stronie internetowej pod adresem: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html. Należy zaznaczyć, że dokument jest kontynuacją wydanego w 2009 r. *Rządowego programu ochrony cyberprzestrzeni RP na lata 2009–2011. Założenia*.

[73] Tłumaczenie własne. W oryginale: *Défense et sécurité des systèmes d'information. Stratégie de la France*. Dokument dostępny na stronie internetowej pod adresem: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011 [dostęp: 20 VI 2016].

[74] Tłumaczenie własne. W oryginale: *Cybercriminalité Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible*; cyt. za: tamże, s. 21 [dostęp: 20 VI 2016].

[75] Tłumaczenie własne. W oryginale: *Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information*, tamże, s. 22.

wych metod działania cyberprzestępców, zastępując wskazane elementy odwołaniem do obszaru cyberprzestrzeni stanowiącej cyfrową domenę przetwarzania danych. Pomimo pozornego uproszczenia semantycznego, zastosowane w niej odwołanie nie tylko zapewnia szeroki kontekst znaczeniowy charakteryzowanego pojęcia, lecz także pozwala na wprowadzenie nieco mniej konwencjonalnego spojrzenia na opis zjawiska nowoczesnej przestępczości komputerowej oraz jego form.

Stosując wcześniej zaproponowany sposób analizy przywoływanych definicji, należy wskazać, że na gruncie *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* cyberprzestępstwem jest każdy czyn spełniający łącznie dwie następujące przesłanki:

1) jest czynem zabronionym w rozumieniu dowolnego przepisu prawnego,
2) szczególnym miejscem popełnienia czynu musi być cyberprzestrzeń rozumiana nie jako kategoria geograficzna, ale nowa, logiczna domena ludzkiej działalności, podbudowywana przez szeroko rozumianą infrastrukturę teleinformatyczną, lecz z nią nieutożsamiana (cyberprzestrzeń jako środowisko wirtualne, oderwane od substratu fizycznego).

Po przeanalizowaniu wymienionych przesłanek jako główne kryterium zaliczania poszczególnych czynów do kategorii cyberprzestępstw przyjęto ocenę możliwości wystąpienia danego czynu w cyberprzestrzeni. Pojawiające się w innych definicjach oceny charakteru dóbr prawnie chronionych będących przedmiotem zamachu, roli systemów teleinformatycznych w przestępstwie czy też opisu szczególnego rodzaju modus operandi sprawcy, w omawianym przypadku straciły w rezultacie swoje znaczenie na rzecz ujednoliconego odwołania do pojęcia cyberprzestrzeń. Na jego tle uzasadnione staje się zadanie następującego pytania: Czy do stwierdzenia zaistnienia tak charakteryzowanego cyberprzestępstwa konieczne jest, aby dany czyn w całości „zamykał się" w cyberprzestrzeni (w tym także ze swoimi skutkami), czy też jest wystarczające, aby w cyberprzestrzeni wystąpiły jedynie niektóre z elementów opisujących dane przestępstwo[76]? Czy wprowadzenie kogoś w błąd w rozmowie telefonicznej przez fałszywe podanie się za osobę pracującą np. w dziale obsługi technicznej banku, skutkujące wykonaniem przez osobę oszukaną niekorzystnej operacji za pośrednictwem sieci Internet (m.in. przesłanie hasła, autoryzowanie przelewu online) powinno być oceniane jako cyberprzestępstwo czy też jako przestępstwo „klasyczne"? Podczas analizy przedstawionego problemu niezbędne wydaje się odwołanie do przepisu art. 6 § 2 kodeksu karnego, zgodnie z którym miejscem popełnienia czynu jest miejsce działania lub zaniechania sprawcy, a także miejsce, w którym nastąpił lub jedynie miał nastąpić skutek stanowiący znamię przestępstwa. Tym samym należy stwierdzić, że na gruncie omawianej definicji, w celu ukonstytuowania cyberprzestępstwa jako przestępstwa popełnianego w cyberprzestrzeni, wystarczające jest stwierdzenie wystąpienia w obszarze domeny cyfrowej choćby jednego ze wskazanych elementów, tj. przestępnego działania, zaniechania lub skutku. W rezultacie przyjętej konstrukcji zakres pojęciowy omawianego wyrażenia ulega wydatnemu rozszerzeniu i obejmuje nie tylko typowe, bezsporne przykłady cyberprzestępstw, jak *hacking*, podmiana treści stron czy zakłócanie poprawnego funkcjonowania systemów, lecz także przypadki działań występujących tak naprawdę w całości poza cyberprzestrzenią. Przykładem może być zaniechanie sprawdzenia poprawnego funkcjonowania systemów teleinformatycznych, które może sprowadzić niebezpieczeństwo dla ludzi, np. kierowanie ruchem pojazdów. Ten czyn, choć intuicyjnie nie zalicza

[76] Zob. B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, s. 25 i nast.

się do zjawiska cyberprzestępczości z powodu braku działania w systemach teleinformatycznych, w świetle postanowień definicji będzie właśnie cyberprzestępstwem.

Odwołanie do cyberprzestrzeni przyjęte w omawianej definicji z uwagi na brak wprowadzenia jakichkolwiek ograniczeń powoduje także swoistą konkurencyjność kwalifikacji miejsca popełnienia czynu zabronionego między przestrzenią fizyczną a cyberprzestrzenią, umożliwiając przyjmowanie podwójnej kwalifikacji dla jednego czynu (np. gdy działanie przestępne następuje w świecie fizycznym, skutek zaś pojawia się w cyberprzestrzeni). Takie rozwiązanie, choć nie ułatwia kwalifikowania przestępczości w cyberprzestrzeni, wydatnie zwraca uwagę na ścisłą zależność współczesnych społeczeństw od nowoczesnych technologii, w tym technologii cyberprzestrzeni.

Przy ocenie definicji cyberprzestępstwa proponowanej w krajowej *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, należy stwierdzić, że pomimo jej szerokiego zakresu przedmiotowego, wyznacza ona nowoczesny kierunek utożsamiania cyberprzestępczości z przestępczością popełnianą w cyberprzestrzeni, niezależnie od jej form oraz szczegółowych metod działania sprawcy. Przyjęte założenie pozwala uniknąć tworzenia specyficznych katalogów cyberprzestępstw i stawia swoisty znak równości między przestępczością „klasyczną" a cyberprzestępczością, z jednoczesnym wprowadzeniem kryterium miejsca popełnienia przestępstwa jako determinującym istotę cyberprzestępczości.

Po przeanalizowaniu literatury prawniczej można zauważyć, że pojęcie c y b e r p r z e s t ę p s t w a coraz częściej występuje w nowych opracowaniach przedmiotu, szczególnie w opracowaniach amerykańskich[77]. Posługuje się nim także Federalne Biuro Śledcze USA – używa go w swoich biuletynach informacyjnych publikowanych na oficjalnej stronie internetowej agencji. W kontekście konwencji o cyberprzestępczości jest ono wykorzystywane także w piśmiennictwie europejskim i zdobywa coraz większą popularność wśród autorów, w tym też autorów polskich. W opracowaniach krajowych tym pojęciem posłużył się przede wszystkim A. Adamski w swoim artykule zatytułowanym *Cyberprzestępczość – aspekty prawne i kryminologiczne* (tekst ukazał się w 2005 r.[78]). Zachowując przekrojowy charakter artykułu, A. Adamski zaprezentował w nim systematykę cyberprzestępczości będącą swoistym rozwinięciem koncepcji przedstawionych wcześniej w innej jego książce pt. *Prawo karne komputerowe* (2000 r.). Na potrzeby analizy omawianego zjawiska A. Adamski podzielił roboczo cyberprzestępczość na cztery kategorie:

1) przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych (np. nieuprawniony dostęp do systemu, podsłuchiwanie transmisji danych lub zakłócanie funkcjonowania systemów),
2) przestępstwa przeciwko dostępowi warunkowemu do usług informacyjnych (np. nieuprawniony dostęp do płatnej, kodowanej telewizji),
3) przestępstwa związane z wykorzystywaniem komputerów (np. oszustwo komputerowe, fałszerstwo komputerowe),
4) przestępstwa związane z rozpowszechnianiem lub przesyłaniem określonych rodzajów informacji (np. propagowanie treści rasistowskich, pornografii dziecięcej czy choćby rozsyłanie niezamówionych informacji handlowych, tzw. spamów).

Przy odwoływaniu się do systematyki przyjętej w *Prawie karnym kompute-*

[77] Na przykład M. Cross, D.L. Shinder, *Scene of the Cybercrime*, b.m.w. [USA] 2008 oraz A. Reyes, *Cyber Crime*… to jedne z najczęściej cytowanych pozycji.

[78] A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 51 i nast.

rowym, pierwszą kategorię przestępstw można przyrównać do przestępstw stricte komputerowych, podczas gdy kategorie trzecia i czwarta obejmują swoim zakresem zarówno przestępstwa z wykorzystaniem komputera (przestępstwa klasyczne), jak i przestępstwa komputerowe w ujęciu szerokim (przestępstwa, co do których przepis karny przewiduje szczególny modus operandi sprawcy zakładający obligatoryjne wykorzystanie komputera lub sieci). Kategoria druga zawęża analizę wyłącznie do obszaru cyberprzestrzeni i wydaje się być szczególną podgrupą przestępstw kierowanych przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych (zawartych w pierwszej kategorii), i w ten sposób zalicza się ponownie do przestępstw stricte komputerowych.

Wnioski

Poniżej przedstawiono w postaci tabelarycznej wykaz omawianych dokumentów wraz ze wskazaniem, które z definiowanych pojęć było stosowane na gruncie danego dokumentu.

Tabela. Występowanie pojęć związanych z przestępczością w cyberprzestrzeni w dokumentach i literaturze przedmiotu (w ujęciu chronologicznym).

Lp.	Rok wydania	Rodzaj oraz oryginalny tytuł dokumentu źródłowego	Pojęcie stosowane jako centralne	
			w oryginale	w tłumaczeniu
1.	1976	**Opracowanie naukowe**: D.B. Parker, *Crime by Computer*	***computer abuse***	**nadużycie komputerowe**
2.	1979	**Rządowy podręcznik USA**: *Computer Crime: Criminal Justice Resource Manual*	***computer-related crime***	**przestępstwo związane z komputerem**
3.	1986	**Raport OECD**: *Computer-related crime: Analysis of legal policy*	***computer abuse***	**nadużycie komputerowe**
4.	1986	**Ustawa USA:** *Computer Fraud and Abuse Act*	***computer abuse***	**nadużycie komputerowe**
5.	1989	**Zalecenie Komitetu Ministrów Rady Europy**: *Recommendation No. R (89) 9 of the Committee Of Ministers to Member States on Computer-Related Crime*	***computer-related crime***	**przestępstwo związane z komputerem**
6.	1990	**Ustawa Wielkiej Brytanii**: *Computer Misuse Act 1990*	***computer misuse***	**bezprawne użycie komputera**

7.	1990	**Rezolucja ONZ:** *Prevention of Crime and the Treatment of Offenders*	***computer-related crime***	**przestępstwo związane z komputerem**
8.	1994	**Podręcznik ONZ**: *United Nations Manual on the prevention and control of computer-related crime*	***computer crime*** = ***computer-related crime***	**przestępstwo komputerowe** = **przestępstwo związane z komputerem**
9.	1995	**Zalecenie Komitetu Ministrów Rady Europy:** *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with information technology*	***offence connected with Information Technology***	**przestępstwo powiązane z technologią informacyjną**
10.	2000	**Opracowanie naukowe:** A. Adamski, *Prawo karne komputerowe*	**przestępstwo komputerowe**	–
11.	2001	**Konwencja Rady Europy**: *Convention on Cybercrime*	***cybercrime***	**cyberprzestępstwo**
12.	2003	**Rządowy program USA:** *The National Strategy to Secure Cyberspace*	***cybercrime***	**cyberprzestępstwo**
13.	2009	**Rządowy program Polski:** *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011*	**cyberprzestępstwo**	–
14.	2009	**Rządowy program Wielkiej Brytanii:** *Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space*	***cyber crime***	**cyberprzestępstwo**
15.	2011	**Rządowy program Wielkiej Brytanii:** *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*	***cyber crime***	**cyberprzestępstwo**

16.	2011	**Rządowy program Niemiec:** *Cyber Security Strategy for Germany*	***cybercrime***	**cyberprzestępstwo**
17.	2011	**Rządowy program Francji:** *Défense et sécurité des systèmes d'information. Stratégie de la France*	***cybercriminalité***	**cyberprzestępstwo**
18.	2011	**Rządowy program Holandii:** *The National Cyber Security Strategy (NCSS). Success through cooperation*	***cybercrime***	**cyberprzestępstwo**
19.	2013	**Rządowa polityka Polski:** *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*	**cyberprzestępstwo**	***cybercrime*** **(oficjalna wersja ang.)**

Źródło: Opracowanie własne.

Po podsumowaniu najistotniejszych elementów występujących w definicjach analizowanych pojęć można wskazać następujące cechy charakteryzujące fenomen nowoczesnej przestępczości:

- systemy teleinformatyczne oraz sieci mogą służyć zarówno do popełniania tradycyjnych przestępstw (np. oszustwo, zniewaga), jak i przestępstw, które pojawiły się dopiero wraz z pojawieniem się cyberprzestrzeni (np. włamywanie się do zasobów komputerów, przechwytywanie transmisji danych),
- przestępstwa popełniane w cyberprzestrzeni nie ograniczają się metodologicznie wyłącznie do dokonywania określonych czynności technicznych, mających na celu np. przełamanie zastosowanych na serwerze zabezpieczeń, ale mogą polegać także na wykorzystywaniu metod socjotechnicznych, które wprowadzają użytkownika w błąd (np. podanie swojego hasła do skrzynki pocztowej w przekonaniu, że aktywuje nowe, darmowe usługi),
- regulacja karna penalizująca poszczególne cyberprzestępstwa nie musi odnosić określonego czynu wprost do systemów teleinformatycznych. Zakwalifikowanie popełnionego czynu do cyberprzestępczości powinno się odbywać na podstawie kryteriów materialnych, odwołujących się do sposobu oraz miejsca popełnienia danego czynu, nie zaś formalnych,
- systemy oraz sieci mogą być wykorzystywane w zjawiskach przestępnych jako narzędzie oraz jako cel. W przypadku przestępstw zamykających się w całości w cyberprzestrzeni te dwa rodzaje przeznaczenia występują równolegle,
- pojawienie się cyberprzestrzeni wykreowało nowe środowisko dla działań bezprawnych, co spowodowało nie tylko to, że miejscem popełniania nowoczesnych przestępstw jest logiczny obszar domeny cyfrowej, lecz także zmieniło sposób rozumienia dobra prawnie chronionego stanowiącego przedmiot zamachu. Cyberprze-

stępczość często jest kierowana zarówno przeciw samemu bezpieczeństwu systemów teleinformatycznych, jak i bezpieczeństwu danych przetwarzanych w tych systemach w postaci elektronicznej. W zależności od rodzaju danych możliwe jest też dalsze kwalifikowanie czynu np. jako kradzież (w przypadku przesuwania aktywów finansowych między kontami w atakowanej usłudze bankowości elektronicznej),

- przestępczość w cyberprzestrzeni może być popełniana przez bezpośrednie działanie sprawcy bądź przez zautomatyzowane działania odpowiednio przygotowanego systemu lub oprogramowania. Przykładem jest umieszczenie wirusa komputerowego, który może wykraść dane oraz wysyłać je do osoby, która go stworzyła, nawet po kilku latach od umieszczenia go w sieci,
- z uwagi na sposób popełniania cyberprzestępstw ściganie ich sprawców wymaga podejmowania wielu czynności technicznych pozwalających na odnajdywanie elektronicznych dowodów przestępstwa. Pozyskiwanie takich dowodów wymaga przede wszystkim zabezpieczania fizycznych nośników danych oraz tzw. logów wskazujących na historię ruchu sieciowego,
- pośród najczęściej wymienianych cyberprzestępstw można wymienić: bezprawny dostęp do danych lub do systemu (dostęp do systemu nie musi wiązać się z dostępem do chronionych danych, może ograniczać się jedynie do części konfiguracyjnej), uszkadzanie danych, zakłócanie poprawnego funkcjonowania systemu, udostępnianie narzędzi służących do popełniania przestępstw w cyberprzestrzeni (na przykład tzw. exploitów będących gotowymi programami przystosowanymi do wykorzystania określonej podatności systemu), propagowanie w sieciach treści zabronionych czy nielegalne powielanie materiałów chronionych prawami autorskimi lub naruszanie takich praw w inny sposób. Należy dodać, że każde z cyberprzestępstw może być popełnione na wiele sposobów technicznych – nazywanych także atakami – odnoszących się do modus operandi sprawcy.

Pełne ujęcie zjawiska cyberprzestępczości wymaga, w ocenie autora, łącznego objęcia wszystkich wskazanych powyżej cech, wynikających z definicji różnych pojęć.

Bibliografia:

1. Adamski A., *Prawo karne komputerowe*, Warszawa 2000, C.H. Beck.
2. Aldrich R.W., *Cyberterrorism and Computer Crimes*: *Issues Surrounding the Establishment of an International Legal Regime* [online], http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf.
3. Bequai A., *Computer Crime*, Heath 1978, Lexington Books.
4. Cross M., Shinder D.L., *Scene of the Cybercrime*, Burlington 2008, Syngress.
5. Doyle C., *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* [online], Congressional Research Service, http://www.fas.org/sgp/crs/misc/97-1025.pdf.
6. Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, Zakamycze.
7. Fortinet G.L., *Fighting Cybercrime: Technical, Juridical and Ethical Challenges* [online], http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.
8. Goodman M., *Making Computer Crime Count*, „FBI Law Enforcement Biulettin" 2001, t. 70, s. 10–17.

9. Jarrett H.M. i in., *Prosecuting Computer Crimes*, Washington DC 2010, Office of Legal Education, Executive Office for United States Attorneys, Department of Justice.
10. Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.
11. Parker D.B., C*rime by Computer*, New York 1976, Scribner.
12. Reyes A., *Cyber Crime Investigations*, Burlington 2007, Syngress.
13. Schjolberg S., *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva* [online], http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.
14. Sieber U., *Computercriminalitat und Strafrecht*, Köln 1977, Heymann.

Abstrakt

Artykuł stanowi próbę uporządkowania siatki pojęciowej stosowanej w prawie do określenia gałęzi przestępczości zwanej popularnie „komputerową". W tekście zostają przytoczone definicje pojęć: nadużycie komputerowe, przestępstwo związane z komputerem, bezprawne użycie komputera, przestępstwo komputerowe oraz cyberprzestępstwo, używane w rozlicznych dokumentach prawnych, zarówno krajowych, jak i międzynarodowych. Rozważania definicyjne wskazują na swoistą ewolucję rozumienia tego, czym charakteryzuje się omawiana dziedzina czynów bezprawnych. We wnioskach dokonano syntetycznego zestawienia najważniejszych cech definicyjnych wymienionych pojęć oraz wskazano ich najistotniejsze elementy wspólne.

Słowa kluczowe: definicje prawne, cyberprzestępstwo, przestępstwo komputerowe, bezprawne użycie komputera, przestępstwo związane z komputerem.

Abstract

The article is an attempt to regulate terminology that is used in law to define the kind of crime referred to as "computer crime". It contains such definitions as: computer abuse, computer-related crime, unlawful use of computer, computer crime or cybercrime, used in numerous national and international documents. Considerations that have been carried out point out to a kind of evolution in the understanding of what the unlawful activities discussed herein refer to. Conclusions contain a synthetic specification of key definition characteristics of the listed terms, as well as their common elements.

Keywords: legal definitions, cybercrime, computer crime, unlawful use of computer, computer-related crime.