Zygmunt Płoszyński

Przestępczość internetowa

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 3, 31-56

2012

Zygmunt PŁOSZYŃSKI
Politechnika Koszalińska
Wyższa Szkoła Bezpieczeństwa z siedzibą w Poznaniu

PRZESTĘPCZOŚĆ INTERNETOWA

Wstęp

W ostatnich latach przyjęło się powszechne twierdzenie, że XX wiek był niewątpliwie wiekiem informacji, w którym dokonał się szereg zmian technicznych i społecznych, które spowodowały, że współczesny świat zamienił się w „globalną wioskę". Istotnym czynnikiem, który odegrał kluczową rolę w tym procesie było powstanie Internetu, czyli sieci, która stała się dla swoich użytkowników ogromną biblioteką zawierającą szereg informacji na każdy temat, których poziom pozostawia niekiedy wiele do życzenia, a mimo to stanowiących źródło wiedzy, do jakiego chętnie zaglądają. Ta globalna sieć stała się z czasem między innymi sposobem komunikacji, rodzajem książki adresowej, dzięki której łatwo można dotrzeć do osób lub ważnego rodzaju instytucji. Zarówno rynek handlu, świat nauki, czy biznesu zmieniły się diametralnie dzięki tej formie komunikacji. Również w sferze psychologii społecznej Internet posłużył jako narzędzie do przełamania barier w realizacji ludzkich potrzeb, np. kontaktu z innymi, bycia zauważonym czy nawiązywania i podtrzymywania więzi. Nowa forma komunikacji, jaką jest poczta elektroniczna (e-mail), umożliwiła kontakty z osobami z całego świata, rodziną, przyjaciółmi, partnerami biznesowymi – bez względu na odległość, a jedynym warunkiem jest dostęp do komputera i sieci.

Według wielu badaczy i psychologów, czynnikiem, który szczególnie przyciąga ludzi do Internetu jest łatwość nawiązywania kontaktów z innymi osobami o podobnych zainteresowaniach i upodobaniach. Internet, jako narzędzie w komunikowaniu się, daje nam jednak nie tylko nowe możliwości, ale narzuca pewne ograniczenia i niesie ze sobą określone zagrożenia wynikające z anonimowości w niektórych kontaktach. Wiemy na przykład, że kiedy czytamy list to nie to samo, co rozmowa telefoniczna, a kontakt telefoniczny to nie to samo, co rozmowa twarzą w twarz. Inaczej też odbieramy kontakt z drugim człowiekiem przez Internet. Pomimo rozpowszechnienia się np. kamer internetowych, w Internecie bierzemy pod uwagę głównie znaczenie słów, gubimy w ten sposób bardzo ważne w komunikacji międzyludzkiej sygnały niewerbalne, np. gesty czy mimikę – przekazujące stany emocjonalne. Nie możemy być zatem do końca przekonani o intencjach osoby, z która korespondujemy. Ta anonimowość nie stanowi dla nas problemu dopóki, doputy nie doświadczymy ewentualnych szkód (psychicznych, moralnych, materialnych czy duchowych) wymierzonych w naszą osobę. Czasem kończy się to na kolejnym przykrym doświadczeniu, z którym wolimy i jesteśmy w stanie uporać się we własnym zakresie, jednak bywają też poważniejsze zagrożenia, które w polskim, a niekiedy światowym prawie określono mianem przestępstw.

Rodzi się pytanie, czy w ocenie społeczeństwa Internet stanowi zło konieczne wynikające z postępu cywilizacji, czy też traktowany jest, jako narzędzie konieczne dla funkcjonowania i dalszego rozwoju ludzkości?

Interdyscyplinarny charakter problematyki samej przestępczości, zagrożenie, jakie ze sobą niesie oraz dążenie do niwelacji czy ograniczenia czynników powstawania tego zjawiska powodują, że do tradycyjnej kryminologii włączają się zagadnienia z zakresu socjologii, psychologii, pedagogiki, psychiatrii, genetyki, informatyki i wielu innych. Przedstawiciele tych dyscyplin naukowych dążą do poznania przyczyn, specyfiki i tendencji rozwojowych, charakteru i stopnia zagrożenia poszczególnymi formami przestępczości, proponując jednocześnie różnego rodzaju rozwiązania, których skuteczność jednak pozostaje nadal tematem otwartym.

Patrząc z perspektywy historycznej, człowiek, jako istota myśląca, od początku dążył do poprawienia sytuacji materialnej swojej i osób mu najbliższych przy pomocy różnych środków i sposobów, które do momentu pojawienia się pierwszych norm prawnych, moralnych i religijnych, były akceptowane społecznie niemal w każdej postaci.

Od momentu pojawienia się ogólno przyjętych zakazów i nakazów możemy mówić o jednoczesnym pojawieniu się przestępczości, ponieważ człowiek jest jednostką skłonną do ich łamania. Jednak w miarę upływu czasu, rozwoju cywilizacji, zmian politycznych, społecznych, przestępczość przybierała różne formy, poczynając od zwykłych występków i zbrodni, których może dopuścić się każdy, aż do powstania przestępczości gospodarczej, zorganizowanej i internetowej, charakterystycznych tylko dla niektórych ludzi o określonych właściwościach i umiejętnościach. Uległy również przeobrażeniu motywy działania samych przestępców oraz ich systemy wartości.

Przestępczość

Co rozumiemy przez „przestępczość", a raczej, kto w świetle polskiego prawa jest przestępcą: *odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia*.[1]

Według Hołysta *przestępczość nie jest wyrażeniem ustawowym. Nie stanowi ona również elementu języka prawniczego. Przez „przestępczość" rozumie się w kryminologii zbiór czynów zabronionych przez ustawę pod groźbą kary, które to czyny popełnione zostały na obszarze danej jednostki terytorialnej w danym czasie. Oczywiście, takie określenie przestępczości może budzić wiele zastrzeżeń natury metodologicznej. Bardzo bogata, bowiem intuicyjnie treść tego pojęcia nie znajduje wyrazu w adekwatnej do rzeczywistości definicji operacyjnej. Stąd też za punkt wyjścia do dalszego toku rozważań wypada w tym stanie rzeczy przyjąć na zasadzie konwencji owo tradycyjne rozumienie przestępczości. Opis przestępczości, prezentacja jej podstawowych charakterystyk jakościowych i ilościowych wymaga dokładnego zlokalizowania badanych zjawisk w określonym systemie politycznym i społeczno-ekonomicznym. Rozmiar przestępczości zależy w znacznej mierze między innymi od stopnia zaangażowania członków społeczeństwa w ujawnianiu zaobserwowanej działalności przestępczej, a także od wytworzonego w społeczeństwie klimatu potępienia wobec sprawców przestępstwa. Właściwa atmosfera jest rezultatem stosunku obywateli do wymiaru sprawiedliwości (zwłaszcza w dziedzinie spraw karnych). Istnieje ścisły*

[1] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny z późn. zm. Stan prawny na 1stycznia 2004 r.

związek między działalnością organów ścigania i wymiaru sprawiedliwości a funkcjonowaniem całego aparatu władzy. Z tej właśnie zależności wynika logiczne twierdzenie, że stosunek obywateli do wymiaru sprawiedliwości jest w znacznym stopniu pochodną ogólnego nastawienia społeczeństwa do organów władzy państwowej. Uwzględnienie związków między władzą państwową a społeczeństwem staje się współcześnie metodologicznym nakazem wszelkich rozważań nad strukturą i dynamiką przestępczości, jak i nad efektywnością działań wymiaru sprawiedliwości. Stąd też przestępczość rozpatrywana być może z punktu widzenia jej rozległości, intensywności, struktury i dynamiki.[2]

Ogólnie charakteryzując schemat przestępczości należy stwierdzić, że nie ma takiej cechy lub zespołu cech oraz warunków, które zawsze wiązałyby się z określonym przestępczym lub nie przestępczym zachowaniem. Na podstawie badań wiemy tylko, że osobnicy charakteryzujący się pewnym zespołem cech przeważnie zachowywali się w określony sposób. Istotne jest więc, aby poszukiwać raczej mechanizmu wyznaczającego określone zachowanie, niż jego bezpośrednich przyczyn. O postępowaniu jednostki decyduje bowiem nie pojedynczy czynnik, ale zespół czynników, przy czym każdemu z nich można przypisać niejednakowe znaczenie. Chociaż i przy tak rozważnym postępowaniu badawczym warto pamiętać, że mamy do czynienia tylko z pewnym prawdopodobieństwem.[3]

Hołyst uważa, że *zbiór zachowań ludzkich jest najbardziej heterogenicznym zbiorem, jaki daje się zdefiniować w kategoriach nauk społecznych. Nauka w poszukiwaniu praw abstrahuje od tego, co jest w zachowaniach przypadkowe, jednostkowe, i identyfikuje tylko to, co w nich ogólne, konieczne, istotne. Każde bowiem zachowanie człowieka uwikłane jest w splot nieskończenie wielu determinant, z których jedynie myślowo daje się wyodrębnić pewne grupy. Szczególnym podzbiorem tego najbardziej heterogenicznego zbioru jest zachowanie uznawane w danym społeczeństwie za przestępstwo. Zachowania rozpatrywane w całej swej masie określone są mianem przestępczości. Charakterystyki ogółu zachowań człowieka w określonych warunkach materialnych dokonuje się na podstawie koniunkcji ustaleń biologii, psychologii, socjologii i antropologii, tworzącej ogólną teorię zachowania. Ocenę przestępczości przeprowadza się zgodnie z ustaleniami kryminologii, nauki zmierzającej do wypracowania ogólnej teorii zachowania przestępczego.*

Charakterystyka przestępczości sprowadza się w zasadzie do opisu następujących zagadnień:

- *cechy przestępczości, determinowane typem struktury społecznej;*
- *czynniki środowiskowe, różnicujące nasilenie przestępczości w czasie i przestrzeni;*
- *cechy populacji przestępczej różnicujące przestępczość czasoprzestrzennie;*
- *wyodrębnione formy przestępczości.*[4]

---

[2] B. Hołyst, *Kryminologia*. Podstawowe problemy, Warszawa 1977, s. 65-66

[3] Zeszyty Naukowe, Psyche 5. Szczecin 200, nr 311,s. 71 (w:) Zakrzewski P. Prognozowanie kryminologiczne.

[4] B. Hołyst, *Kryminologia*, op. cit., s. 144

Dodać należy, że *czyny o charakterze przestępczym są również popełniane przez osoby nieletnie, jednak ze względu na wiek sprawców nie są one klasyfikowane jako przestępstwa, lecz jako czyny karalne*.[5]

W celu scharakteryzowania skali zjawiska przestępczości w Polsce posłużę się tabelą z biuletynu statystycznego Komendy Głównej Policji, przyjmując za punkt odniesienia *współczynnik przestępstw stwierdzonych, będący ilorazem liczby przestępstw w odniesieniu do określonej liczby ludności.*[6]

Tabela nr 1: Obraz dynamiki zmian wybranych kategorii przestępstw w Polsce w latach 1993-2003

	1	2	3	4	5	6
2003	1.039	2.322	15.669	14.010	336.143	51.688
2002	1.188	2.345	16.775	14.194	314.929	47.808
2001	1.325	2.339	16.968	14.369	314.820	49.862
2000	1.269	2.399	18.429	14.363	309.846	53.533
1999	1.048	2.029	17.849	12.756	243.537	44.775
1998	1.072	2.174	19.495	13.034	211.651	34.225
1997	1.093	2.260	20.505	13.005	184.368	30.063
1996	1.134	1.985	19.371	11.575	157.479	26.257
1995	1.134	2.267	18.901	10.600	211.602	26.858
1994	1.160	2.039	18.454	9.223	180.514	23.574
1993	1.106	1.976	16.646	7.285	134.089	21.034

	7	8	9	10	11	12
2003	294.654	168.827	1.101.387	147.658	217.598	1.466.643
2002	304.625	163.012	1.083.854	109.698	210.677	1.404.229
2001	325.696	138.817	1.107.073	103.521	179.495	1.390.089
2000	364.786	19.894	1.133.162	84.260	49.488	1.266.910
1999	369.235	20.505	1.020.654	60.393	40.498	1.121.545
1998	355.176	34.442	931.037	78.496	63.509	1.073.042
1997	324.017	40.202	838.941	82.296	71.136	992.373
1996	305.703	34.863	761.664	73.911	62.176	897.751
1995	304.899	35.005	835.641	83.893	55.367	974.941
1994	304.293	32.030	780.781	74.956	50.420	906.157
1993	1.106	1.976	16.646	7.285	134.089	21.034

[5] B. Hołyst, *Przestępczość w Polsce w latach 1989-2002 prognoza do 2008 r*. Warszawa 2001, s. 9
[6] Ibidem

1 – ZABÓJSTWO
2 – ZGWAŁCENIE
3 – USZKODZENIE CIAŁA*
4 – UDZIAŁ W BÓJCE LUB POBICIE
5 – KRADZIEŻ**
6 – KRADZIEŻ ROZBÓJNICZA, WYMUSZENIE ROZBÓJNICZE, ROZBÓJ
7- KRADZIEŻ Z WŁAMANIEM
8 – PRZESTĘPSTWA DROGOWE
9 – PRZESTĘPSTWA O CHARAKTERZE KRYMINALNYM
10 – PRZESTĘPSTWA O CHARAKTERZE GOSPODARCZYM
11 – POZOSTAŁE
12 – RAZEM

* – od września 1998 roku w „nowym" kodeksie karnym: uszczerbek na zdrowiu (bez przestępstw o charakterze wypadku przy pracy)
** – dane za lata 1991-1999 nie obejmują kradzieży o charakterze gospodarczym

Analizując powyższą tabelę widzimy, że w przestępstwach przeciwko życiu i zdrowiu w roku 2003, np. zabójstwach odnotowano blisko 70 przypadków mniej w porównaniu z rokiem 1993. Nieznacznie wzrosła liczba zgwałceń. Ilość bójek i pobić wzrosła do roku 2003 blisko dwukrotnie, tj. aż o 7 000 przypadków więcej niż w roku 1993. Ilość kradzieży w przeciągu dziesięciu lat wzrosła prawie trzykrotnie, natomiast ilość kradzieży z włamaniem wykazuje niewielkie tendencje wzrostowe i utrzymuje się mniej więcej na tym samym poziomie. Dotyczy to również przestępstw drogowych, w których do roku 2000 odnotowano nawet tendencje spadkowe, co tłumaczy się postępem techniki motoryzacyjnej, a tym samym zwiększeniem bezpieczeństwa czynnego i biernego, i co za tym idzie, zmniejszeniem ilości wypadków drogowych. Natomiast od roku 2001 odnotowano znaczny wzrost przestępstw drogowych, bo aż ośmiokrotny, co spowodowane jest nowelizacją w kodeksie karnym, a konkretnie wprowadzeniem przepisu określonego art. 178a KK, traktującego prowadzenie pojazdów w stanie nietrzeźwości, jako przestępstwo, które wcześniej było wykroczeniem.

Na temat przestępczości internetowej brak jest dokładnych danych statystycznych obrazujących skalę tego zjawiska, jest to tzw. „ciemna liczba". *W nowszej literaturze kryminologicznej odróżnia się kilka obszarów ciemnej liczby przestępstw. Pierwszą dziedzinę stanowią przestępstwa, które w ogóle nie doszły do wiadomości organów policji. Do drugiej można zaliczyć przypadki ujawnionych przestępstw, jednakże ich sprawcy nie zostali wykryci. Trzeci obszar wypełniają przestępstwa, których sprawcy zostali wykryci, ale z uwagi na negatywne przesłanki procesowe nie dochodzi do wniesienia aktu oskarżenia lub nie zapada wyrok skazujący. Czwartą dziedzinę stanowią przestępstwa, za które sprawcy zostali skazani prawomocnym wyrokiem sądowym, jednakże nie wszystkie czyny były znane organom policji i objęte aktem oskarżenia.*[7] Ogólne statystyki nie dostarczają nam informacji, czy komputer i zawarte w nim dane są przedmiotem lub środkiem do popełnienia przestępstwa za pośrednictwem Internetu, nie biorąc pod uwagę jego dostępu do sieci.

[7] B. Hołyst, *Kryminologia*. *Podstawowe problemy*. Warszawa 1977, s. 77

Internet

Internet to światowa sieć komputerowa. Określany jako „sieć sieci", gdyż składają się nań mniejsze sieci lokalne i rozległe, połączone ze sobą w różny sposób: specjalnymi kablami, liniami telefonicznymi i modemami, łączami satelitarnymi, światłowodami.[8]

Historia powstania Internetu rysuje się następująco: na początku szczytem marzeń był komputer jakikolwiek. Służył do grania, pisania, rysowania, liczenia. Szybko jednak ludzie zorientowali się, że można znacznie zwiększyć jego możliwości, jeżeli połączy się go z innym komputerem, wówczas można szybko i sprawnie przesyłać dane, drukować na jednej drukarce, przesyłać informacje między użytkownikami.

Tak powstały sieci lokalne, obejmujące swoim zasięgiem kilka komputerów w firmie, cały budynek firmy czy uczelni, kilka budynków. Dawało to wiele dodatkowych możliwości, takich jak poczta elektroniczna, kolektywna praca nad jednym projektem przez wielu pracowników, wspólne korzystanie z tych samych danych.

Powstała wówczas idea połączenia takich sieci lokalnych między sobą – najpierw dla połączenia kilku oddziałów jakiejś instytucji (na początku wojskowej lub uczelni). Do komunikacji między sieciami użyto protokołu IP (ang. *Internet Protocol*, adres IP jest to lokalizacja komputera w sieci, każdy adres zapisuje się jako cztery liczby z zakresu od 0 do 255 oddzielone kropkami)[9] z systemu UNIX (UNIX system operacyjny przeznaczony głównie dla komputerów pełniących rolę serwerów). Pomimo, że powstał w 1969 roku, nadal jest jednym z częściej spotykanych w świecie systemów operacyjnych.

Większość producentów superkomputerów dołącza do nich własną wersję tego systemu. Na bazie UNIX-a powstał też LINUX, czyli system przeznaczony dla komputerów osobistych, choć jest on również z powodzeniem używany w komputerach świadczących różne usługi sieciowe).[10] Protokół ten stał się protokołem obowiązującym w Internecie (od niego właśnie pochodzi nazwa „Internet"). Dziś Internet to tysiące sieci lokalnych połączonych ze sobą, używających do komunikacji protokołu IP. Internet jest instytucją w 100% demokratyczną, tzn., że nie posiada żadnej centralnej władzy. Każdy użytkownik ma równe prawa, zaś każda instytucja, która podłącza swoją sieć do Internetu udostępnia zasoby, które chce rozpowszechnić i może korzystać z zasobów, które udostępniają inni. Zasady podłączenia i korzystania z Internetu, to cały zestaw niepisanych praw i obowiązków dotyczących na równi wszystkich. Jedyną pozostałością władzy centralnej jest przydzielanie numerów IP i adresów internetowych dla sieci lokalnych. Jest to zrozumiałe, jeżeli uświadomimy sobie, że adresy i numery komputerów podłączonych do Internetu muszą być unikalne.[11]

Do Internetu można się dostać na kilka sposobów, różnią się one szybkością połączenia i zakresem dostępnych usług:

- *połączenie przez modem – z Internetu możemy korzystać używając swojego komputera domowego i modemu, łącząc się z najbliższą firmą*

[8] T. Kołodzieczak, J. Zieliński, *Podstawy informatyki*. Warszawa 1997, s. 197
[9] *http://ip.boo.pl/ip-info.php* (pobrano 23.11.2004 r.)
[10] *http://republika.pl/systemyoperacyjne/unix.html* (pobrano 23.11.2004 r.)
[11] B. Leś, *Abc Internetu*. Kraków 2001, s. 13

oferującą usługi podłączenia do Internetu. Używa się tu programów komunikacyjnych i przeglądarek do odpowiednich usług w Internecie. Połączenie takie pozwala korzystać ze wszystkich usług Internetu, ale ze względu na niezbyt dużą szybkość nie jest zbyt wygodne;

- *połączenie stałe – najlepiej, gdy pracujemy w sieci lokalnej, która ma stałe połączenie z Internetem. Można wówczas osiągać szybkość połączenia do 2 MB/s. Jest to najwygodniejsze połączenie z Internetem; korzystają z niego np. naukowcy na uniwersytetach. To właśnie takie małe sieci lokalne tworzą sieć globalną: Internet. Można korzystać ze wszystkich usług: poczty elektronicznej, bibliotek plików, grup dyskusyjnych, World Wide Web;*
- *połączenie przez inne usługi – do Internetu można podłączyć się nie tylko bezpośrednio, ale i przez inne usługi informacyjne, takie jak CompuServe, America Online, czy biuletyny informacyjne BBS. Usługi te posiadają bramy (gateways), czyli programy łączące je z Internetem. W ten sposób można wymieniać pocztę elektroniczną i mieć dostęp do grup dyskusyjnych*.[12]

Sieć internetowa stała się najpopularniejszym medium ostatnich lat, jednak korzystanie z Internetu niesie za sobą pewne ryzyko: *prawdziwe problemy zaczynają się, kiedy w rachubę wchodzą pieniądze. Nikt nie chce, aby informacje o jego kontach bankowych, kartach kredytowych i dokonywanych transakcjach dostały się do publicznej wiadomości. Jednocześnie reklamy wielu firm na stronach internetowych kuszą nas możliwością szybkich i łatwych zakupów czy skorzystania z usług oferowanych za pośrednictwem sieci bez wychodzenia z domu. Kilka banków oferuje pełną obsługę kont za pośrednictwem Internetu. Za wiele przydatnych informacji dostępnych w Internecie można zapłacić kartą kredytową W podobny sposób można zapłacić za programy shareware – od razu zarejestrować kopię programu i otrzymać kod aktywacyjny. Rynek usług internetowych zaczyna się coraz intensywniej rozwijać. Dla zapewnienia bezpieczeństwa transakcji dokonywanych za pośrednictwem Internetu firma Netscape opracowała standard szyfrowania danych SSL – Secure Sockets Layer. Standard ten wykorzystywany jest przez większość firm świadczących usługi w zakresie zakupów internetowych i usług bankowych przez Internet. Firmy świadczące usługi z wykorzystaniem protokołu SSL muszą być zarejestrowane w tak zwanym urzędzie certyfikacyjnym CA zdefiniowanym w przeglądarce, więc samo wykorzystanie protokołu SSL jest potwierdzeniem wiarygodności strony internetowej. Istota działania protokołu SSL polega na szyfrowaniu wszystkich informacji przesyłanych pomiędzy klientem a serwerem. Odbywa się to niezauważalnie dla użytkownika. Podstawowym problemem – jeśli chodzi o bezpieczeństwo posługiwania się tym protokołem – były amerykańskie ograniczenia eksportowe pozwalające na wykorzystanie w programach sprzedawanych poza terytorium USA klucza 40-bitowego, który można było rozszyfrować wykorzystując odpowiedni sprzęt i oprogramowanie. Obecnie nowe wersje przeglądarek obsługują klucz 128-bitowy. Zastosowanie protokołu SSL*

[12] T. Kołodziejczak, J. Zieliński, *Podstawy informatyki*. Warszawa 1997, s. 198

z kluczem 128-bitowym można uznać za bezpieczny sposób przesyłania danych i zawierania transakcji przez Internet. Niektóre polskie banki umożliwiają pełną obsługę kont z poziomu przeglądarki Internetowej.[13]

Przestępczość w Internecie

Powszechny dostęp do Internetu sprawia, że coraz większa liczba osób narażona jest na niebezpieczeństwa, jakie łączą się z korzystaniem z sieci. Zagrożenia te mogą dotyczyć:

- Wykorzystywania wad oprogramowania i błędnej konfiguracji;
- Podsłuchiwania wymiany danych, manipulacji w pakietach danych, przejmowania sesji, podszywania się;
- Rozprzestrzeniania się wirusów i robaków internetowych;
- Zapychania łączy i blokowania usług.

Na atak narażone są w szczególności systemy wymiany informacji (usługi) ogólnodostępne i korporacyjne, oprogramowanie (systemy operacyjne, aplikacje), bazy danych, sieci rozległe (łącza, routery) oraz pojedyncze komputery użytkowników.[14]

Według Horoszkiewicza „system komputerowy narażony jest na cztery podstawowe niebezpieczeństwa:

- ujawnienie przechowywanej i przetwarzanej informacji;
- utratę lub zniekształcenie danych;
- wymuszenie przerwy w pracy systemu (poprzez uszkodzenie aplikacji, systemu operacyjnego, lub samego sprzętu komputerowego);
- wykorzystanie go do celów sprzecznych z przyjętym porządkiem prawnym (np. rozpowszechnianie informacji nielegalnych – pornografii, treści rasistowskich, obraźliwych, nawołujących do przestępstwa, produkcja fałszywych dokumentów) i regułami obowiązującymi w przedsiębiorstwie (np. wykorzystywanie służbowego sprzętu do celów prywatnych, nieraz komercyjnych).

Przyczyny zaistnienia niekorzystnych zjawisk dla systemów komputerowych oraz zawartych w nich informacji mogą być bardzo różne. Obejmują zarówno zdarzenia losowe (np. awarie systemu zasilania, klimatyzacji, instalacji wodociągowej, katastrofy budowlanej, itp.), awarie techniczne sprzętu oraz oprogramowania komputerowego a także ludzkie działania, nieumyślne (błędy) i umyślne – a więc działania przestępne. Wyraźnie należy stwierdzić, że przestępstwa komputerowe są tylko częścią potencjalnych zagrożeń dla systemu informatycznego, ale jako działania celowe powodują z reguły najdotkliwsze straty.

Omawiane zjawisko przestępczości komputerowej, popełnianej na szkodę internetowych systemów, najczęściej wiąże się z brakiem ściśle określonych procedur postępowania użytkowników tych sieci, łamaniem procedur bezpieczeństwa w przypadku ich wdrożenia, a przede wszystkim małego zrozumienia zarówno zasad działania systemów komputerowych, a także niedoceniania wartości zawartych w nich danych."[15]

---

[13] B. Leś, *Abc Internetu*. Kraków 2001, s. 53-55
[14] A. Misiuk, J. Kosiński, *Przestępczość teleinformatyczna*. Szczytno 2002, s. 96-97
[15] J. Horoszkiewicz, *Przestępczość komputerowa*. Szczytno 2001, s. 8

Jak zauważa Jerzy Wójcik „wykorzystanie systemów komputerowych i towarzyszące mu zagrożenia można w sposób syntetyczny scharakteryzować następująco:

- już na początku lat pięćdziesiątych komputeryzacja była wykorzystywana do sterowania rutynowymi czynnościami w gospodarce i administracji. Jednakże dopiero w latach sześćdziesiątych ujawniono pierwsze, a w latach siedemdziesiątych poważniejsze wypadki oszustw, sabotażu, a także szpiegostwa gospodarczego z wykorzystaniem komputerów;
- masowe przetwarzanie informacji danych osobowych przez tworzenie banków danych rozpoczęło się w latach sześćdziesiątych. Wkrótce brak ograniczeń związanych z dostępem do tych danych odebrano jako zagrożenie praw obywatelskich;
- otwarte systemy sieciowe, które pojawiły się w latach siedemdziesiątych szybko stały się obiektem nadużyć określanych, jako hacking;
- upowszechnienie komputerów osobistych w latach osiemdziesiątych spowodowało masowe zjawisko sporządzania pirackich kopii programów;
- rozwinięcie sieci bankomatów w latach osiemdziesiątych natychmiast skutkowało nadużyciami za pomocą kart magnetycznych;
- powszechność poczty elektronicznej, mailbox-ów, ISDN, a także ścisłe powiązania między systemami przetwarzania danych a telekomunikacją umożliwiły powszechne komunikowanie oraz wykorzystywanie do celów przestępnych, np. do zacierania śladów przestępstwa."[16]

Spośród najbardziej rozpowszechnionych przestępstw dokonywanych za pośrednictwem Internetu można wyróżnić następujące:

„Hacking – nieuprawnione wejście do systemu komputerowego – art. 267 k.k., który mówi, że: „kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2."[17] §2 tegoż artykułu mówi, że „tej samej karze podlega ten, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym."[18]

Jest to najbardziej swoiste ze wszystkich przestępstw, które można popełnić w sieci. W większości cyberoszustw, cyberkradzieży, hacking jest elementem koniecznym do ich zaistnienia.

Typowymi sposobami stosowanymi przez hackerów komputerowych są:

- „**Koń trojański**" jest to program, który pełni specjalne funkcje (przydatne dla hackera), udając inny program. Przykładem może być tutaj podmieniony program logujący, który poza tym, że loguje użytkownika, zapisuje wprowadzone hasło do pliku, tak, aby później hacker z łatwością mógł je odczytać. Stosowane są także "konie trojańskie", działające na zasadzie klient/serwer. Składają się one z programu, dzięki któremu

[16] J.W. Wójcik, *Hacker. Geniusz czy przestępca*, (w:) „Magazyn Kryminalny 997", 1996, s. 27
[17] Ustawa z dn. 06 czerwca 1997 r., „Kodeks karny" z późn. zm., stan prawny na dzień 01.01.2004 r.
[18] Ibidem

można niejako "wydawać polecenia", oraz "sługi" – zainstalowanego w obcym komputerze programu, wykonującego różnego rodzaju zadania;
- „**Back door**" dosłownie "tylne drzwi". Jest to program (często koń trojański) instalowany głównie na serwerze, umożliwiający hackerowi dostanie się do niego z ominięciem zabezpieczeń. Jest to bardzo często stosowana technika, za której pomocą hacker może wielokrotnie powracać nawet na bardzo dobrze zabezpieczony serwer, bez konieczności ponownego włamywania się;
- „**Exploit**" jest to program, który wykorzystuje różne dziury w systemach, mogący mieć wpływ na ich działanie, zawieszać je lub nawet przejąć nad nimi kontrolę. Najczęściej exploitem jest program dla Unixa lub Linuxa (czyli systemu operacyjnego nie tak rozpowszechnionego jak Windows). Jednocześnie jest to często źródło, z którego każdy administrator lub hacker może się zapoznać z jego działaniem i wykorzystać go do własnych celów. Dla Windows także istnieje wiele różnych exploitów, lecz ustępują tym z innych systemów;
- **IP spoofing** jest to bardzo skuteczna i często stosowana technika, która umożliwia podszycie się pod inny komputer. Jest kilka jego odmian – można stosować odpowiednie oprogramowanie na własnym komputerze, lecz także można odpowiednio podrzucić program do obcego komputera, dzięki któremu zamiast do tego komputera, informacje przekazywane będą do własnego. Do spoofingu należy także wysyłanie poprzez otwarty port ICQ dowolnych informacji, podając jako nadawcę cudzy numer identyfikacyjny;
- „**Sniffing**" dosłownie "wąchacz". Jest to niezwykle efektywna technika służąca do podsłuchiwania pakietów pomiędzy komputerami. Dzięki niej można np. przechwycić wysyłane i niezwykle istotne dane, np. hasła, kody dostępu itp. Sniffer umieszczony w odpowiednim miejscu w sieci, staje się bardzo niebezpiecznym narzędziem w rękach hackera.

Hacking sam w sobie można zdefiniować jako łamanie zabezpieczeń dla samej przyjemności i satysfakcji pokonania barier technicznych.

Nie zmienia to jednak faktu, że integralność systemu jest zachwiana i mamy do czynienia z naruszeniem prawa. Nie jest bowiem możliwe wyraźne oddzielenie hackingu niepowodującego żadnych negatywnych skutków, od Hawkingu, w efekcie którego powstaną szkody. Najbardziej dobitnym przykładem takiego działania jest sprawa grupki młodych niemieckich hackerów, którzy włamali się do kilku amerykańskich systemów komputerowych, a następnie sprzedali wiedzę uzyskaną podczas cybernetycznej podróży byłej radzieckiej służbie wywiadowczej KGB. Sami „klasyczni hackerzy" twierdzą, że ich celem nie jest nigdy spowodowanie szkody, lecz tylko zabawa. Dlatego wprowadzają osobną kategorię „crackerów", którzy dokonują włamań, aby uzyskiwać z tego powodu korzyści."[19]

Pojawienie się zjawiska hackingu pociągnęło za sobą skutki w postaci utworzenia nowych przepisów w polskim ustawodawstwie, regulujących odpowiedzialność karną za popełnianie tego przestępstwa. „Należy zgodzić się z panującym poglądem, że artykuł 267 k.k. jest w rzeczywistości rozszerzoną artykułu 172 k.k. chroniącego tajemnicę korespondencji, który nie przystawał do

[19] *http://www.vaglą.pUskrYpts/cybercrime.htm*, (pobrano 21.07.2004 r.)

dzisiejszych realiów technicznych przekazywania i przechowywania informacji. Nie można jednak zawężająco interpretować zapisu o „przełamaniu" zabezpieczeń systemu. Błędem byłoby zastosowanie analogii z wykładni przepisów dotyczących pokonania zabezpieczenia z typowej kradzieży z włamaniem. Stąd też wejście do systemu bez uprawnienia musi być postrzegane wyłącznie przez skutek a nie przez metodę działania sprawcy. Bowiem niezależnie od zastosowanej metody działania, należy udowodnić, iż przestępca i jego wejście do systemu nie ma umocowania w żadnych uprawnieniach nadawanych użytkownikom przez administratora systemu. Z kolei obejście zabezpieczeń systemowych, jest jakby wejściem do pomieszczenia nie przez zamknięte np. na kłódkę drzwi, ale przez niezabezpieczone okno, które przez przeoczenie nie zostało zamknięte. Jednak fakt istnienia zabezpieczeń wskazuje wyraźnie, że intencją właściciela jest udostępnienie zasobów systemowych jedynie uprawnionym, tj. posiadającym odpowiednie klucze dostępu użytkownikom. Analizując najczęściej spotykane działania hackera oraz idee, jakie mu przyświecają, należy stwierdzić, że celem jest nieuzyskanie określonej informacji pochodzącej z systemu (np. jakiegoś pliku tekstowego czy graficznego), ale wyłącznie pokonanie zabezpieczeń tego systemu i całkowite opanowanie go. Wynikać to może z faktu, że rzadko kiedy włamywacz wie, czego szuka w systemie. Najczęściej wchodzi do systemu szukając tam jakiejś informacji. Nie konkretnej informacji, ale informacji jakiejkolwiek. Dopiero potem, gdy takie informacje zdobędzie, ocenia ich przydatność. Aby dostać się do najciekawszych informacji dla dalszej działalności hackerskiej, włamywacz stara się za wszelką cenę uzyskać uprawnienia administratora, albowiem wówczas ma praktycznie nieograniczony dostęp do zasobów komputera, tj. do wszystkich znajdujących się tam danych. Omawiany w tej części art. 267 k.k. przewiduje ponadto sześć alternatywnych sposobów karalnego naruszenia tajemnicy korespondencji:

- otwarcie zamkniętego pisma nieprzeznaczonego dla sprawcy;
- ukrycie cudzej korespondencji przed adresatem, zanim adresat się z nią zapoznał;
- przyłączenie się do przewodu służącego do przekazywania wiadomości;
- podstępne uzyskanie nadanej przy użyciu środków telekomunikacji wiadomości przeznaczonej dla innej osoby;
- przekazanie innej osobie wiadomości uzyskanej jednym z wymienionych wyżej sposobów.

Należy podkreślić, że odpowiedzialność karna z artykułu 267 k.k. jest uzależniona od skutku przestępczego działania, jakim jest „uzyskanie informacji" – w tym wypadku przez hackera. Okazuje się jednak, że samo skopiowanie przez sprawcę plików danych zawierających informacje, z którymi nie zdążył się on jeszcze zapoznać, może nie wyczerpywać znamion ustawowych omawianego przestępstwa. Tym samym, szczególnie groźna forma hackingu, polegająca na kradzieży informacji na cudze zlecenie, pozostawałaby praktycznie poza zakresem penalizacji art. 267§ 1 k.k."[20]

Warunkiem zakwalifikowania hackingu, jako przestępstwa jest jego szkodliwość społeczna, a hacking jest szkodliwym społecznie bez względu na intencje sprawcy. „Nawet hacking uprawiany dla „dreszczu emocji", bez zamiaru

[20] J. Horoszkiewicz, *Przestępczość komputerowa*. Szczytno 2001, s. 16-18

wyrządzenia szkody lub popełnienia przestępstwa, niesie zagrożenia i może powodować szkody. Z punktu widzenia administratorów sieci i systemów komputerowych, jest więc zjawiskiem niepożądanym, które narusza ich prawo do niezakłóconego zarządzania systemem i pociąga za sobą koszty zbadania stanu jego zabezpieczeń i ponownej instalacji oprogramowania. Cel i sposób działania sprawcy nie stanowią elementów konstytuujących odpowiedzialność karną za „nielegalny dostęp". Mogą tę odpowiedzialność jedynie limitować, jeśli strona wprowadzi do swojego ustawodawstwa ograniczenia. Na tym tle należy stwierdzić, że karalność hackerstwa na gruncie polskiego Kodeksu karnego podlega o wiele dalej idącym ograniczeniom niż to dopuszcza projekt konwencji."[21]

Rodzajem przestępstw dokonywanych poprzez Internet są różnego rodzaju oszustwa, określone w art. 287 k.k. Przepis ten mówi, że: „Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat pięciu."[22]

„Komputery w podmiotach gospodarczych są w większości przypadków wykorzystywane do dokumentowania lub prowadzenia różnego rodzaju operacji księgowych i finansowych. Wobec powyższego, rzeczą oczywista jest, że w tej sferze mogą być również narzędziem wykorzystywanym do różnego rodzaju nadużyć. Straty, do jakich dochodzi w wyniku oszustw komputerowych, mogą być bardzo poważne i stanowią rezultat trojakiego rodzaju manipulacji:

- danymi, które wprowadza się do komputera (manipulacje na wejściu);
- programem służącym do przetwarzania danych;
- rezultatami tych przetworzeń (manipulacje na wyjściu)."[23]

Internet stwarza wprost nieograniczone możliwości na dokonywanie oszustw. Powstały już nawet wyspecjalizowane grupy przestępcze, których jedynym polem działania jest Cyberprzestrzeń. Oszustwo w sieci jest integralnie połączone z hackingiem komputerowym, jako elementem koniecznym do dokonania tego typu przestępstwa.

„Podstawowym oszustwem jest posługiwanie się skradzionym wcześniej numerem karty kredytowej. Typowa struktura gangu komputerowego, składa się z wielu wyodrębnionych grup, z których każda ma inne zadanie. Pierwszym etapem jest zawsze zdobycie koniecznych informacji. W tym celu dochodzi do włamań do systemów informatycznych organizacji, dokonujących jakichkolwiek transakcji w cyberprzestrzeni. Spotyka się działania bardziej prymitywne – drobni przestępcy, często bardzo młodzi ludzie, zbierają numery kart w sklepach czy restauracjach. We Francji aresztowano niedawno kelnera współpracującego z taką grupą. Zanim dokonał zapłaty rachunku z karty kredytowej otrzymanej od klienta, starannie odpisywał numery kart, które następnie dostarczał w ręce gangu. Dysponując numerem karty, dokonuje się zakupów w sklepach internetowych, wypożycza samochody, a nade wszystko okrada banki, kasy i ubezpieczycieli. Wladimir Levin, wykorzystując gry komputerowe i dane osobiste, siedząc przed komputerem w biurze firmy AO Saturn w St. Petersburgu oszukał Citibank na

[21] A. Adamski, *Przestępczość w cyberprzestrzeni*. Toruń 2001, s. 19-20
[22] Ustawa z dn. 6 czerwca 1997 r., Kodeks karny z poźn. zm. Stan prawny na 01.01.2004 r.
[23] J. Horoszkiewicz, *Przestępczość komputerowa*. Szczytno 2001, s. 25-26

10 milionów dolarów. Kolejnym rodzajem oszustwa jest manipulacja programem. Polega na takim przygotowaniu programu i „wszczepieniu" go do systemu, aby system wykonywał określone czynności bez woli operatora. Typowym przykładem takiej działalności jest włamanie się do systemu bankowego i podrzucenie programu „obcinającego" minimalne kwoty z rachunków bankowych i przesyłanie ich na jedno konto. Ze względu na olbrzymią liczbę rachunków, straty liczone są w milionach dolarów.

Innymi klasycznymi oszustwami tego typu są fałszerstwa listy płac. Po włamaniu się do systemu obsługującego taką listę, wstawia się „martwe dusze", osoby nieistniejące, których pobory przelewane są na określone konto cyberprzestępcy. Sytuacja taka miała miejsce przede wszystkim w USA i Niemczech. Jest to działanie skomplikowane i wymagające już dużej wiedzy informatycznej.

W lutym 1997 roku Sąd Federalny w Nowym Jorku nakazał zamknięcie jednej ze stron WWW. Była to strona prezentująca treści pornograficzne, więc cieszyła się dużym powodzeniem. Jednakże zanim można było zobaczyć jej zawartość, niezwykle pomysłowy twórca nakazywał skopiowanie krótkiego programu, mającego „zdekodować" obraz. Program owszem, dekodował obraz, ale również, całkowicie zaskakując odbiorców, przekierunkowywał ich rozmowy telefoniczne z lokalnych dostarczycieli Internetu (providerów) na numery telefoniczne w Mołdawii, za stawkę dziesięciokrotnie większą. Ponad 800 tysięcy minut było naliczonych dla użytkowników z USA. Sprawcy nie złapano. Odpowiedzialność karna za większość oszustw może wypływać z przepisów dotyczących klasycznego oszustwa. Jednak coraz częściej zauważa się konieczność specjalnego uregulowania tych kwestii.[24]

Projekt konwencji Rady Europy następująco definiuje oszustwo komputerowe: „wprowadzenie, zmiana, usunięcie lub zablokowanie danych komputerowych albo inna ingerencja w proces przetwarzania danych, w zamiarze przysporzenia sobie lub innej osobie nienależnej korzyści majątkowej. Definicja ta ma wiele cech wspólnych z ujęciem istoty oszustwa komputerowego w zaleceniu RE z 1989 roku także pod tym względem, że konstytuuje typ przestępstwa skutkowego. O dokonaniu oszustwa komputerowego, według projektu konwencji, decyduje wywołanie skutku w postaci utraty własności przez osobę pokrzywdzoną przestępstwem. Jest to ujęcie węższe aniżeli to, jakie przyjął polski ustawodawca w art.287 k.k., który przewiduje typ przestępstwa określany mianem „oszustwa komputerowego". Istota tego czynu polega, bowiem na usiłowaniu uzyskania korzyści majątkowej lub spowodowania szkody przez manipulowanie zapisem na komputerowym nośniku informacji albo innym oddziaływaniu na automatyczne przetwarzanie informacji."[25]

Opisując przestępcze metody popełniania oszustw, K. Jakubski stwierdza, że: „najczęstszymi formami popełniania oszustwa komputerowego są:

- **manipulacja danymi**, polegająca na wprowadzeniu nieprawdziwych danych w celu uzyskania nienależnych korzyści majątkowych. Forma ta jest najbardziej rozpowszechniona, bowiem nie wymaga od sprawcy żadnej szczególnej wiedzy lub umiejętności. Zmian danych dokonują

[24] *http://www.vagla.pllskrypts/cybercrime.htm*,(pobrano 22.07.2004 r.)
[25] A. Adamski, *Przestępczość w cyberprzestrzeni*. Toruń 2001, s. 47-48

z reguły operatorzy sprzętu, choć mogą to czynić także osoby włamujące się do systemu komputerowego. Jak się ocenia w krajach wysoko rozwiniętych, w wyniku włamań do systemów komputerowych banków, kas i ubezpieczycieli, straty ponoszone przez te instytucje w przestępstwie manipulacji danymi są wielokrotnie większe niż na skutek napadów i wymuszeń. D.B. Francis podaje, że amerykański bank w wyniku „tradycyjnego" napadu traci średnio około 8 000 dolarów, podczas gdy przeciętne oszustwo komputerowe „kosztuje" bank około pół miliona dolarów. Polski przykład manipulacji danymi to między innymi wprowadzanie tzw. „martwych dusz" do systemu informatycznego Zakładu Ubezpieczeń Społecznych;

- **manipulacja programem**, polegająca na takim przygotowaniu programu lub jego modyfikacji, aby program wykonywał określone czynności niezależnie od woli operatora. Jedną z odmian takich manipulacji jest metoda „salami", w której np. program bankowy, przy rozliczaniu wkładów płatnych na każde żądanie, samodzielnie dokonuje zmniejszania rachunku o minimalne kwoty i przekazuje je na uprzywilejowany rachunek sprawcy przestępstwa, lub osoby przez niego wskazanej. Ten sposób działania przestępnego wymaga dużej wiedzy informatycznej i sporych umiejętności w zakresie programowania, dlatego sprawcę należy typować wśród twórców oprogramowania, specjalistów z poszkodowanej instytucji lub włamywaczy do systemów komputerowych;
- **manipulacja wynikiem**, zwana inaczej manipulacją urządzeniami wyjścia/wejścia, polegająca na wykorzystywaniu ogólnie dostępnych peryferii komputerów i systemów w celu dokonania przestępstwa. Przykładem takich działań są przestępstwa dokonywane na szkodę banków i ich klientów za pomocą bankomatów, które są jedynie terminalami (czyli urządzeniami wejścia i wyjścia danych). Postacie zjawiskowe tego typu nadużyć są bardzo różne – od prostych fałszerstw kart (podrobienie, skopiowanie lub przerobienie oryginalnej karty, wytworzenie nowej karty płatniczej z tzw. „białego plastiku") po fałszerstwa elektroniczne, wykorzystujące w swoich metodach najnowsze zdobycze techniki."[26]

Wszystkie oszustwa komputerowe są uznawane za przestępstwa trudne do ścigania. Proces ujawniania, wykrywania, dowodzenia czy zapobiegania, wymaga współdziałania organów ścigania i poszkodowanego przestępstwem komputerowym, który nie zawsze jest zainteresowany ujawnieniem słabości własnego systemu z uwagi np. na obawę utraty zaufania klientów.

Kolejnym przestępstwem, jest sabotaż komputerowy określony w art. 269 k.k., który mówi, że: „kto na komputerowym nośniku informacji niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 2 – tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając

[26] K. Jakubski, *Postępy kryminalistyki*, Zeszyt 1, 1997, s. 6-43

nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji."[27]

Pojęcie „sabotażu komputerowego" obejmuje swym znaczeniem takie zjawiska jak:

- wirusy komputerowe;
- programy-robaki;
- bomby logiczne.

„Wirusy komputerowe to programy, które po dostaniu się do komputera, błyskawicznie rozchodzą się do innych programów i po pewnym czasie powodują olbrzymie szkody, często nieodwracalne. Dostają się one do komputerów na wszelakie sposoby – przez dysk, dyskietkę, bezpośrednio z Internetu, czy też przez E-mail. Jednak zawsze ukryte są w jakimś programie, gdyż same, będąc programem, muszą zostać otwarte, aby mogły działać. Sam fakt, iż np. dostało się wirusa nie stanowi zagrożenia, dopóki samemu nie wprowadzi się go do własnego systemu. Dlatego też cyberprzestępcy coraz lepiej maskują swoją "broń". Z każdym rokiem wzrasta liczba i rodzaj wirusów komputerowych. Wirusy można podzielić na:

- zdolne do rozmnażania się (samokopiowania);
- zdolne do przechwytywania programu gospodarza podczas pracy oraz obejmowania kontroli nad systemem.

Wirus komputerowy stał się bardzo niebezpieczna bronią w rękach osoby, chcącej sparaliżować system komputerowy, a co za tym idzie – określoną dziedzinę życia. Wraz z coraz większym rozwojem komputeryzacji, rozpowszechnianie wirusów komputerowych będzie stawało się coraz groźniejszym przestępstwem.

Już dziś, większość służb specjalnych na całym świecie, obawia się pojawienia się cyberterrorysty, który zamiast bomb, porywania samolotu – po prostu wprowadzi do systemu niepozorny program, który w przeciągu kilkunastu minut będzie w stanie unieruchomić całe państwo. Pierwsze doświadczenia z przestępstwami sabotażu komputerowego polegającego na rozpowszechnieniu wirusa na olbrzymią skalę mamy już za sobą.

26 marca 1999 roku, w wielu skrzynkach pocztowych na całym świecie, pojawił się wirus nazwany Melissa. Jego twórca skonstruował go w niezwykle przebiegły sposób. Pojawiał się on jako załącznik do poczty elektronicznej, która przychodziła od znajomych, z którymi na co dzień prowadzona była korespondencja. Natychmiast po wejściu do komputera, dołączał się ten wirus do pierwszych 50 adresów z listy adresowej. Spowodowało to lawinowy i nieprawdopodobnie szybki rozwój i rozprzestrzenianie się wirusa. Otwarcie wiadomości zainfekowanej wirusem Melissa powodowało, że wirus „zarażał" programy w najbardziej popularnym edytorze tekstów – Word. W ciągu 5 dni wirus zaatakował w samych tylko Stanach Zjednoczonych ponad milion komputerów osobistych.

1 kwietnia 1999 roku, członkowie specjalnego oddziału ds. przestępczości technologicznej z New Jersey i agenci specjalni FBI, aresztowali podejrzanego o stworzenie wirusa 31-letniego Davida Smitha. Ten przyznał się do zarzucanego mu czynu. 9 grudnia 1999 roku Stanowy Sąd Najwyższy, a następnie Sąd

[27] Ustawa z dn. 06 czerwca 1997 r., Kodeks karny z poźn. zm., stan prawny na dzień 01.01.2004 r.

Dystryktowy orzekł najwyższą możliwą karę dla tego typu przestępstwa – 10 lat pozbawienia wolności za przestępstwo stanowe i 5 lat pozbawienia wolności za przestępstwo federalne, ponadto Smith będzie musiał zapłacić 400 tysięcy dolarów grzywny. Straty na jakie oszacowano skutki Melissy, wyniosły ponad 80 milionów dolarów. Prokurator Robert Cleary stwierdził, że wreszcie pokazano, iż wirusy komputerowe to nie jest „gra", lecz poważne przestępstwo.

Po raz pierwszy prawo karne tak surowo zostało wykorzystane w przestępczości internetowej.

Programy – robaki są bardzo podobne do wirusów, nie potrzebują jednak istnienia programu-nosiciela. Pojawiają się w sieciach komputerowych i komputerach wielodostępnych, wykorzystując łączność między komputerami i użytkownikami, jako nośnik transmisji. Po raz pierwszy pojawiły się w 1988 roku, kiedy amerykański student zablokował ponad 6 tysięcy komputerów, w ciągu kilku dni.

Bomby logiczne – jest to programowa instrukcja, powodująca wykonanie określonych kodów programowych, w ściśle określonych warunkach i mogąca sparaliżować cały system.

Sabotaż komputerowy stanowi coraz większy problem, gdyż coraz większa część społeczeństwa jest uzależniona od sprawnie działającego systemu komputerowego. Na całym świecie powstały i powstają instytucje, mające przewidywać i błyskawicznie reagować na przypadki cyberterroryzmu. Według prognoz jednej z takich instytucji ze Stanów Zjednoczonych, możliwe akcje cyberterrorystyczne to np.:

- cyberterrorysta rozmieści kilka skomputeryzowanych bomb w mieście, wszystkie transmitują określony kod, który dociera do każdej z nich. Jeśli transmisja zostanie przerwana, bomby zostaną symultanicznie zdetonowane;
- cyberterrorysta będzie jednocześnie zręcznym hackerem, dokona włamania do systemu finansowego państwa grożąc jego całkowitym paraliżem, będzie wysuwał żądania;
- cyberterrorysta zaatakuje system kontroli powietrznej i doprowadzi do zderzenia dwóch samolotów pasażerskich, grożąc następnymi;
- cyberterrorysta dokona zmian w komputerowych recepturach, na podstawie których produkowane będą lekarstwa (wystarczy choćby zmiana proporcji);
- cyberterrorysta zmieni zasadniczo ciśnienie w gazociągach, powodując eksplozję. Sieć komputerowa jest wprost wymarzonym polem działania dla terrorystów."[28]

Sabotaż komputerowy, inaczej ataki, których celem jest „spowodowanie zakłóceń w funkcjonowaniu systemów komputerowych lub całkowite zablokowanie ich działania, stanowią obecnie jedną z bardziej rozpowszechnionych, także w polskiej domenie Internetu kategorię zamachów na bezpieczeństwo elektroniczne przetwarzanej informacji. Zamachy te są wymierzone w dostępność informacji, czyli atrybut decydujący o zaufaniu do techniki komputerowej, a ich szkodliwość jest wprost proporcjonalna do stopnia zależności danej organizacji lub instytucji od technologii informatycznej.

[28] *http://www.vagla.pl/skrypts/cybercrime.htm*, (pobrano 22.07.2004 r.)

Zakres ochrony prawnej prawidłowego funkcjonowania systemów komputerowych i telekomunikacyjnych został ujęty w projekcie konwencji RE szeroko. Ochrona prawna przysługuje każdemu operatorowi i użytkownikowi systemu teleinformatycznego, o ile dojdzie do umyślnego i poważnego zakłócenia działania tego systemu przez osobę do tego nieuprawnioną w następstwie ataku logicznego lub fizycznego na system. Rodzaj informacji i charakter związanych z nią dóbr prawnych – naruszonych w wyniku sabotażu komputerowego – nie stanowią według cytowanej definicji elementów konstytutywnych przestępstwa. Nie ma również takiego znaczenia status podmiotów pokrzywdzonych przestępstwem. W obu tych aspektach definicja sabotażu komputerowego w polskim Kodeksie karnym wyraźnie odbiega od powyższego ujęcia."[29]

Jak stwierdza K. Jakubski „sabotaż komputerowy bardzo często połączony jest z szantażem komputerowym, gdzie sprawca w zamian za spełnienie jego warunków, najczęściej finansowych, gotów jest odstąpić od sparaliżowania systemu komputerowego w sobie tylko znany sposób."[30]

Kolejnym przestępstwem występującym w cyberprzestrzeni jest podsłuch komputerowy, który ustawodawca ujął w art. 267 § 2 k.k. „Rozwój współczesnych technik ukrytego uzyskiwania informacji stanowi poważne zagrożenie dla systemów informatycznych. Pozwalają one na inwazyjne i nieinwazyjne uzyskanie komputerowych danych. Informacje uzyskiwane takimi metodami mogą pochodzić zarówno z nośników danych stanowiących integralne części systemów komputerowych, jak z linii służących do transmisji danych (np. kabli, dzięki którym funkcjonuje sieć, czy sygnałów radiowych przenoszących takie informacje). Techniki te, mimo czasem bezpośredniego kontaktu z wykorzystywanymi urządzeniami, pozwalają na uzyskanie informacji z „podsłuchiwanego, podglądanego" obiektu w sposób niepozostawiający śladów. Przełamuje więc zasady jej poufności i ograniczonego dostępu do niej, możliwego wyłącznie dla jej dysponenta i osób przez niego uprawnionych. Spenalizowany w§ 2 omawianego już art. 267 (§ 1 tegoż artykułu poddaje karze uzyskanie informacji poprzez wejście do systemu bez upoważnienia, czyli tzw. włamanie komputerowe – hacking) podsłuch komputerowy, sprowadza zachowanie się sprawcy do ukierunkowanego na uzyskanie informacji, do której posiadania sprawca nie jest uprawniony, zakładania lub posługiwania się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym. Przestępstwo usankcjonowane w tym przepisie nie powinno być postrzegane jedynie jako podsłuch komputerowy sensu stricto, albowiem jak wynika z powołanej treści, penalizuje również zwykły podsłuch telefoniczny. Warto podkreślić, że istnieje również specjalistyczne oprogramowanie służące do przechwytywania informacji przesyłanych w trakcie transmisji danych komputerowych. Przykładem takiego oprogramowania są dostępne na stronach Internetu tzw. „skanery sieciowe", umożliwiające uzyskanie kopii danych przesyłanych pomiędzy komputerami. Wykorzystanie tego oprogramowania wymaga jednak wcześniejszego podłączenia się fizycznego do przewodu zapewniającego przesyłanie takich informacji (w tym także łączy telekomunikacyjnych). Współczesne techniki przechwytywania informacji

[29] A. Adamski, *Przestępczość w cyberprzestrzeni*. Toruń 2001, s. 31-32

[30] Materiały z seminarium naukowego nt. *Techniczne aspekty przestępczości teleinformatycznej*, Szczytno 8-9.06.1998

umożliwiają również podsłuchiwanie transmisji komputerowych bez wykorzystania inwazyjnej metody kontaktu z urządzeniami komputerowymi. Są to urządzenia umożliwiające przechwytywanie takich informacji z określonej odległości od przewodu sieci. Techniki te wykorzystują urządzenia i oprogramowanie zdolne do odtworzenia danych przesyłanych w trakcie transmisji na podstawie przechwyconych zmian pola elektromagnetycznego, wytwarzanego przez taki przewód skutkiem przesyłanych przez niego danych, które na czas takiej transmisji są niczym innym jak tylko impulsami prądowymi."[31]

Współczesne techniki przechwytywania informacji są poważnym zagrożeniem dla systemów informatycznych.

„Obecna technika umożliwia przechwytywanie wszelkich danych z dużych odległości bądź przy użyciu specjalnych narzędzi, co zawsze stanowi poważne zagrożenie dla przyszłego bezpieczeństwa określonego systemu komputerowego. Możliwy jest nie tylko zdalny podsłuch, ale i podgląd, a więc prowadzenie pełnej kontroli bez wiedzy właściciela systemu. Współczesne urządzenia umożliwiają dokonanie przechwycenia danych nawet z odległości kilku kilometrów."[32]

Projekt konwencji RE problem podsłuchu komputerowego ujmuje następująco: „niezależnie od stosowanej techniki podsłuchu, każda bezprawna ingerencja w poufność międzyludzkiej komunikacji, stanowi naruszenie prawa do prywatności korespondencji i jako taka powinna być kara niesankcjonowana. Wychodząc z tego założenia, Komitet Ekspertów RE określił swoje stanowisko w przedmiocie karalności nielegalnego przechwytywania danych podając, że każda strona podejmie środki ustawodawcze i inne, niezbędne do uznania za przestępstwo w jej prawie krajowym umyślnego przechwytywania za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi z systemu informatycznego przekazującego takie dane informatyczne, bez uprawnienia. Strony mogą wprowadzić wymóg popełnienia przestępstwa z zamiarem uzyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym (art. 3 projektu Konwencji). Ograniczenie zakresu kryminalizacji podsłuchu komputerowego do przypadków, w których sprawca przestępstwa posługuje się urządzeniami technicznymi, ma na celu uniknięcie nadmiernej kryminalizacji życia.

Rozwój możliwości technicznych i operacyjnych sprzętu komputerowego powoduje, że właściwie nie ma dziś już dokumentu w rozumieniu klasycznym, który nie mógłby być sfałszowany przy zastosowaniu sprzętu komputerowego. Utrudnienia w popełnieniu tegoż przestępstwa sprowadzać się będą zazwyczaj do problemów materiałowych, surowcowych, przełamania zabezpieczeń technicznych dokumentu."[33]

Jedną z groźniejszych metod działania sprawców fałszerstw w teleinformatyce jest „duplikowanie kart bankomatowych przy użyciu wyrafinowanego wyposażenia. Wokół czytników instalowane są skanery pasków magnetycznych. Dzięki nim można pozyskać wszystkie dane zapisane na pasku wsuwanej lub wysuwanej

[31] J. Horoszkiewicz, *Przestępczość komputerowa*. Szczytno 2001, s. 24-25
[32] Materiały z seminarium naukowego, nt. *Techniczne aspekty*…
[33] J. Horoszkiewicz, op. cit., s. 30

karty. Właśnie dlatego niektóre typy bankomatów przesuwają kartę w nierównym tempie lub nawet na chwilę zmieniają kierunek ruchu. To akurat nie jest groźny objaw, a wręcz przeciwnie – taki bankomat lepiej pilnuje naszej własności. Niepokojące są raczej czytniki kart wysunięte, nawet nieznacznie, poza płaszczyznę bankomatu, ponieważ istnieje wtedy możliwość zainstalowania skanera, który przecież nie musi być duży. Ale niektóre wysunięte podajniki są tak skonstruowane, że właśnie instalacja skanera jest mocno utrudniona – chwyta się tylko róg karty (np. w bankomatach PKO S.A. produkcji NCR)."[34]

Konwencja RE problem fałszerstwa komputerowego traktuje w następujący sposób: „chodzi o ochronę autentyczności danych mających znaczenie prawne. Autentyczność danych jest w projekcie konwencji rozumiana podobnie jak autentyczność dokumentów w polskim prawie. Chodzi, zatem o „prawdziwość" danych (dokumentu) ze względu na ich (jego) pochodzenie od organu lub osoby oznaczonej jako wydawca (danych) dokumentu. Przedmiotem wykonawczym omawianego przestępstwa może być dokument elektroniczny lub podpis elektroniczny, a sposobem jego dokonania wprowadzanie zmian do elektronicznego zapisu informacji o znaczeniu prawnym przez osobę do tego nieuprawnioną, posługiwanie się cudzym podpisem elektronicznym, bądź nieautoryzowane generowanie danych lub całych dokumentów elektronicznych mających wartość dowodową. Istotę fałszerstwa komputerowego projekt konwencji definiuje jako umyślne i bezprawne wprowadzenie, modyfikację, usunięcie lub zablokowanie danych, następstwem czego jest powstanie danych nieautentycznych, które zgodnie z zamiarem sprawcy mają być uznane lub wykorzystane w obrocie prawnym, jako autentyczne. Dopuszcza się przy tym możliwość ograniczenia zakresu karalności fałszerstwa komputerowego ze względu na szczególny (oszukańczy lub nieuczciwy) zamiar sprawcy. Zakres ochrony prawno-karnej dokumentu elektronicznego w ustawodawstwie polskim jest o wiele szerszy niż to przewidują standardy europejskie. Mankamentem regulacji polskiej jest niefortunny zwrot „zapis na komputerowym nośniku informacji" i niepotrzebne mnożenie bliskoznacznych mu terminów na gruncie innych ustaw."[35]

Jednym z groźniejszych przestępstw internetowych stwarzających niebezpieczeństwo dla kraju jest szpiegostwo komputerowe albo wywiad komputerowy, określone w art. 130 § 2 i 3 k.k., który mówi, że: „kto biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej podlega karze pozbawienia wolności na czas nie krótszy niż 3 lata, oraz kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w§ 2, gromadzi je lub przechowuje, włącza się do sieci komputerowej w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8."[36]

Pojęcie szpiegostwa komputerowego obejmuje również „szpiegostwo przemysłowe, którego celem może być uzyskanie informacji o znaczeniu technicznym bądź technologicznym, przechowywanych w zasobach systemów komputerowych inwigilowanego przedsiębiorcy. W związku z takim zachowaniem

[34] *http://www.kartyonline.net/niusy.php?id=991*, (pobrano 22.07.2004 r.)
[35] A. Adamski, *Przestępczość w cyberprzestrzeni.* Toruń 2001, s. 45-46
[36] Ustawa z dn. 06 czerwca1997 r., Kodeks karny, z późn. zm. stan prawny na dzień 01.01.2004 r.

sprawcy, może dojść do naruszenia nie tylko przepisów karnych uznawanych za stricte komputerowe (nieuprawnione wejście do systemu), ale również naruszających ochronę informacji, która stanowi tajemnicę przedsiębiorstwa, przemysłową, handlową, państwową (np. wojskową) itd. Do metod szpiegostwa wykorzystujących przedmioty związane z systemami informatycznymi, należy zaliczyć zarówno kradzież czy zbieranie komputerowych nośników informacji jak i zbieranie wydruków komputerowych, jeżeli zawarte w nich informacje stanowią informację nie podlegającą upublicznieniu ze względu na przysługującą im ochronę prawną. Istotą przestępstwa określonego w art. 130 § 3 k.k. jest postać szpiegostwa, polegająca np. na włączeniu się do sieci komputerowej w celu uzyskania wiadomości o charakterze tajemnicy państwowej lub służbowej, których udzielanie obcemu wywiadowi może wyrządzić szkodę RP. Karalne jest również takie działanie sprawcy, które przewiduje art. 130 k.k., a popełniony czyn godzi w interesy państwa sojuszniczego pod warunkiem, że państwo to zapewnia wzajemność w tym względzie. W komentarzach do Kodeksu karnego zwraca się uwagę na fakt, iż chodzi tu jedynie o członkostwo w sojuszach wojskowych. W polskim przypadku chodzi o działalność na szkodę państw należących do struktur NATO."[37]

Innym poważnym zagrożeniem dla ludzkości występującym również w Internecie jest terroryzm. „Wprawdzie Kodeks karny nie definiuje pojęcia terroryzmu w sposób bezpośredni, niemniej jednak zachowania uznawane za takowe, znajdują swoje odbicie w Kodeksie karnym pod postaciami inaczej określanych czynów zabronionych. Terroryzm komputerowy może przybierać różną formę. Może to być np. żądanie powstrzymania się od określonych działań lub uniemożliwienie dalszego funkcjonowania określonych urządzeń, będące efektem zablokowania ich lub zniszczenia (najczęściej danych lub programów komputerowych). Do dokonania tego przestępstwa może na przykład dojść w wyniku działania sprawcy polegającego na podłożeniu ładunku wybuchowego pod centrum informatyczne albo celowe zawirusowanie systemu komputerowego, jak i w skutek niedbalstwa lub lekkomyślności (np. w wyniku błędu hackera albo zaniechania realizacji procedur nadzorujących sieć komputerową, dokonane przez odpowiedzialnego za nie pracownika). Do terroryzmu mogą mieć również zastosowanie przepisy art. 163-169 k.k. Sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w znacznych rozmiarach – art. 165 § 1 ustęp 4. Przestępstwo polega na zakłócaniu, uniemożliwianiu lub wpływaniu w inny sposób na automatyczne przetwarzanie, gromadzenie albo przesyłanie informacji. Czyn taki zagrożony jest karą pozbawienia wolności od 6 miesięcy do lat 8. za popełnienie przestępstwa określonego w tym przepisie może odpowiadać sprawca, który np. zagroził bezpieczeństwu powszechnemu związanemu z funkcjonowaniem lotniska, stacji kolejowej, urządzeń dostarczających wodę, gaz, energię dla ludności, monitorowaniem danych na oddziale intensywnej terapii, ochroną obiektów bankowych, wojskowych, itp., np. przez wprowadzenie wirusa do programu komputerowego sterującego określonymi urządzeniami lub uniemożliwiając całkowicie pracę takich urządzeń.

Nieumyślne zakłócenie automatycznego przetwarzania informacji związane ze sprowadzeniem niebezpieczeństwa powszechnego – art. 165 § 2 k.k.

[37] J. Horoszkiewicz, *Przestępczość komputerowa*. Szczytno 2001, s. 31

Sprawcami tego przestępstwa będą przede wszystkim uprawnieni użytkownicy sieci komputerowej (lekkomyślność lub niedbalstwo). Nie można jednak wykluczyć winy nieumyślnej w działaniu hackera, który atakując określone bazy danych, w sposób niezamierzony zniszczy lub uszkodzi inne dane lub oprogramowanie atakowanego komputera.

Zamach terrorystyczny na statek morski lub powietrzny – art. 167 § 2 k.k. „Jeżeli sprawca zamachu terrorystycznego niszczy, uszkadza lub czyni niezdatnym do użytku urządzenie nawigacyjne albo uniemożliwia jego obsługę, gdy urządzenie to służy do przetwarzania danych niezbędnych w komunikacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5."[38]

Do innych przestępstw popełnianych w Internecie należą:

„**Rozpowszechnianie treści rasistowskich** – już w latach osiemdziesiątych sieci komputerowe były wykorzystywane przez grupy neonazistowskie, takie jak: Ku-Klux-Klan, Ruch Oporu Białych Aryjczyków do głoszenia swoich poglądów. Organizacje także publikowały w Internecie nazwiska żydowskich „wrogów", z zachęta do stosowania przemocy. Pojawił się natomiast problem z penalizacją tego typu zachowań, gdyż zgodnie z amerykańskim orzecznictwem, aby wypowiedź nie była chroniona przez wolność słowa wyrażoną w pierwszej poprawce do Konstytucji USA, musi wywołać możliwość natychmiastowego działania niezgodnego z prawem. Dlatego też propaganda rasistowska w sieci nie może być przedmiotem sankcji kryminalnych. Potencjalni antagoniści nie mają, bowiem ze sobą kontaktu fizycznego i mogą być oddaleni nawet o kilkaset kilometrów.

W Niemczech zarówno prawicowi jak i lewicowi ekstremiści, jako jedni z pierwszych zaczęli używać poczty elektronicznej, aby usprawnić komunikację. Prawicowcy założyli sieć 10 mailboxów, zwanych "Thule-Network", w której rozpowszechniali propagandowe materiały. Bardzo szybko zaczęły powstawać gry komputerowe udostępniane publiczności, których celem była dezintegracja mniejszości narodowych i cudzoziemców. Na przykład w grze pt. "Menager w obozie koncentracyjnym" młodzież musiała decydować, czy człowiek narodowości tureckiej miał być wysłany do pracy w kopalni, czy też natychmiast zagazowany. Niemieckie służby bezpieczeństwa starają się zwalczać te przejawy rasizmu, lecz napotykają na problemy związane ze ściganiem. "Thule – Network" zostało zlikwidowane dopiero pod koniec 1994 roku przez agencję dochodzeniową Badenii – Wirttenbergii.

Rozpowszechnianie pornografii – jest to jedno z najbardziej nagminnych zjawisk w dzisiejszym Internecie. Ze względu na olbrzymią skalę tego zjawiska, ograniczę się tutaj tylko do pewnych ogólnych założeń.

Ze względu na ogólną dostępność, Internet, stanowi swoisty poligon doświadczalny dla wszelakich pomysłów i sposobów zarabiania pieniędzy. Jednym z najlepszych sposobów zarabiania pieniędzy w Internecie, jest założenie popularnej strony, którą będzie odwiedzało wielu gości. Pozwoli to na umieszczenie dużej ilości reklam, banerów, odnośników. Jedną z największych widowni mają strony z zawartością materiałów pornograficznych. Abstrahuję już tutaj od definicji, co już jest pornografią, a co nie. Nawet jeśliby zdać się tylko na subiektywne odczucia konkretnej osoby, to z całym przekonaniem należy

[38] J. Horoszkiewicz, *Przestępczość komputerowa*. Szczytno 2001, s. 31-32

stwierdzić, iż dotarcie do strony pornograficznej, nawet osobie mającej najłagodniejsze kryteria, nie zajmie więcej niż kilka minut. Problem pornografii jest problemem, który zawsze będzie wywoływał gwałtowne dyskusje. Nie wdając się w nie, należy zauważyć, że w Internecie nie ma, jak na razie, możliwości kontroli dostępu do stron pornograficznych. Nawet, jeżeli przyjmiemy, że osoba dorosła ma prawo oglądać to, co zechce (pod warunkiem, że nie jest pokazywane przestępstwo), to obecnie nie da się zagwarantować zamknięcia dostępu przed dziećmi. Nie ma bowiem sensownego systemu weryfikacji wieku.

Pornografia w Internecie istnieje w wielu postaciach: listy dyskusyjne, zdjęcia, przekazy "na żywo" poprzez kamery podłączone do komputera. O ile problem „zwykłej" pornografii jest trudny do rozwiązania, to z całą pewnością na błyskawiczną reakcję zasługuje problem pornografii z wykorzystaniem dzieci.

Na całym świecie można spotkać prawno-karne regulacje dotyczące pornografii dziecięcej. U podstaw tychże regulacji tkwi przeświadczenie, że wszelkie zdjęcia i filmy powstają w wyniku przestępstwa dokonywanego ze szczególną krzywdą na dzieciach. Pornografia dziecięca jest niczym innym jak zapisem molestowania seksualnego nieletnich. Jedną z najnowszych form rozpowszechniania pornografii w Internecie, jest produkcja i dystrybucja zdjęć, w których nieletni zostali wygenerowani komputerowo. Są tylko tworem grafiki komputerowej. W takim wypadku w większości krajów nie można już mówić o prawno-karnie relewantnej pornografii dziecięcej, gdyż odpada aksjologiczna przesłanka penalizacji. Żadne dziecko nie jest bowiem krzywdzone. Sąd Najwyższy USA uznał także, iż nie popełnia się przestępstwa, jeśli dorosłe osoby są ucharakteryzowane na nieletnich. Wykorzystują to twórcy stron internetowych, tworząc ich coraz więcej, używając przy tym osób, które tylko "odgrywają" rolę nieletnich. Wydaje się, że i takie działanie powinno znaleźć się w zakresie stosowania przepisów karnych, gdyż bardzo często stanowi przyczynek do popełniania prawdziwych przestępstw z udziałem nieletnich.

Pedofile znaleźli w sieci warunki do dokonywania i propagowania przestępstw seksualnych z udziałem dzieci oraz szybki sposób dotarcia do potencjalnych ofiar na całym świecie. Wykorzystują oni każdy sposób, by zbliżyć do swej ofiary – na przykład podają się za nastolatków w grupach dyskusyjnych, przebywają w „chat-roomach" dla młodzieży. Nawiązują kontakt, który potem przeradza się w zależność fizyczną. Często niszcząc psychikę dziecka. 15-letni Sam Manzi był napastowany seksualnie przez 43-letniego mężczyznę, którego spotkał w grupie dyskusyjnej na America On-line. Później Sam Manzi został oskarżony o molestowanie i zabójstwo 11-letniego chłopca. Pedofile wymieniają między sobą zdjęcia i filmy z pornografią dziecięcą. Mimo szeregu aktów prawnych, walka z tą plagą jest niezwykle trudna. Niezwykle zatem istotne jest dopasowywanie już istniejącego prawa do rzeczywistości komputerowej.

W 1994 roku amerykańskie służby specjalne poinformowały policję brytyjską o zidentyfikowaniu strony internetowej zawierającej pornografię dziecięcą.

Po dotarciu na strony Wydziału Metalurgii Uniwersytetu w Birmingham, odnaleziono tysiące zdjęć przedstawiających stosunki seksualne z udziałem nieletnich. Zdjęcia zgromadził jeden z pracowników Uniwersytetu. Postawiono mu zarzut naruszenia przepisów Ustawy o Ochronie Dzieci z roku 1978, oraz Ustawy o Rozpowszechnianiu Pornografii z roku 1959.

W trakcie procesu sędzia stanął przed problem, gdyż obrona wykazywała, iż wyżej powoływane akty penalizują rozpowszechnianie zdjęć, a to, co stanowi zawartość komputera, nie podlega zakresowi obowiązywania tych przepisów. Sędzia podjął precedensową w Wielkiej Brytanii decyzję, iż zdjęcia istniejące tylko w sieci komputerowej, podlegają tym samym rygorom, jak tradycyjne fotografie.

Niezmiernie rzadko można stwierdzić i udowodnić bezpośredni kontakt pedofila ze swoją ofiarą za pośrednictwem Internetu. Wymaga to żmudnego śledztwa i sporej wiedzy fachowej. Policja brytyjska w połowie lat 90-tych, dostała sygnały, iż na terenie Wielkiej Brytanii działa szczególnie aktywny sieciowo pedofil. Specjalne jednostki Scotland Yardu, rozpoczęły akcję o kryptonimie „Sturburst".

W jej wyniku aresztowano Adriana McLeish'a, 45-letniego księdza z Gilesgate, w Wielkiej Brytanii. Posiadał on największą ujawnioną do tej pory kolekcję zdjęć przedstawiających pornografię dziecięcą. Wymieniał także z innymi pedofilami tysiące e-maili zawierających niedozwolone materiały. Przyznał się także do wykorzystywania seksualnego dwóch chłopców w wieku lat 12 i 18, których wcześniej poznał w sieci internetowej. Policja ustaliła, iż podłączał się do Internetu za pośrednictwem co najmniej czterech różnych dostawców usług sieciowych. Używał także szyfru, który uniemożliwiał odczytywanie jego korespondencji i sposobu połączenia przez osoby trzecie. Jego hasło dostępu brzmiało: „Ponad Księżycem jest szeroki i radosny uśmiech". Dzięki dokładnemu sprawdzeniu uzyskano dowody, iż McLeish wysyłał zdjęcia do co najmniej jednego z dwóch napastowanych chłopców. Przechwycono także jego wypowiedź w sieci, że nie zaprzestanie wykorzystywania tego chłopca. W sumie znaleziono u niego w komputerze 998 plików, z których każdy jeden zawierał do 15 zdjęć pornograficznych.

Handel narkotykami i lekarstwami – obecni handlarze narkotyków coraz częściej używają Internetu jako miejsca przeprowadzania swoich transakcji. Wykorzystują do tego formułę sieci, jako „sklepu".

W Internecie możemy spotkać trzy rodzaje „aptek":

- Odpowiednik tradycyjnych aptek, w których wymagane jest przedstawienie ważnej recepty od licencjonowanego lekarza (w postaci fax-u, lub w formie zeskanowanej w e-mailu) przed dostarczeniem wymaganego lekarstwa. Choć już tutaj pojawia się problem, gdyż niektóre leki mogą być całkowicie legalne w jednym kraju, a w innym mogą nie być dopuszczone do używania (choćby z powodu niedokończonej procedury zatwierdzającej);
- Apteki, w których można za pośrednictwem sieci uzyskać „diagnozę" będącą podstawą uzyskania recepty i dostarczenia następnie leku, całkowicie bez fizycznego kontaktu z lekarzem. Takie apteki zazwyczaj używają sieciowego kwestionariusza lekowego, w którym "pacjent" opisuje swój stan zdrowia, obecnie używane lekarstwa i historię choroby. Na tej podstawie lekarz wydaje "diagnozę". Wielokrotnie może to stanowić próbę uniknięcia ewentualnej odpowiedzialności karnej, poprzez powoływanie się na wprowadzenie w błąd przez klienta, który będąc całkowicie zdrowy chciał uzyskać określone lekarstwa. Póki praktyki takie nie są zakazane, w istocie trudno jest doprowadzić do skazania prowadzącego taką „aptekę";

- Trzecią kategorię stanowią apteki, gdzie bez jakichkolwiek formalności można zakupić wszelkie lekarstwa. W tych przypadkach oferujący takie usługi jest częstokroć zupełnie nieznany, a ponadto wykorzystuje wszelkie możliwe sposoby, aby ukryć prawdziwe miejsce działania i utrudnić jego wykrycie. Tym sposobem handlarze narkotyków znajdują miejsce, które jest doskonałą okazją do rozszerzenia terytorium ich działania.

Należy podkreślić, że prowadzenie postępowania w stosunku do tego typu aptek, o których wiadomo, że mają siedzibę w danym kraju (a więc zasadniczo typy a) i b) nie jest łatwe. Zależy to od sposobu interpretacji istniejącego już prawa. Jednak prawdziwych trudności nastręcza konieczność współpracy międzynarodowej, bez której nie będzie można uruchomić żadnych procedur sprawdzających.

Konkludując należy stwierdzić, że przestępstwa w Internecie mają cechy w znacznym stopniu utrudniające ich wykrycie oraz udowodnienie. Według FBI mniej niż 15% spraw ujawnianych jest przez organy ścigania. Wykrywanie tych przestępstw wymaga, oprócz głębokiej wiedzy, wielkiego nakładu sił i środków, umożliwiających zlikwidowanie tej przewagi, którą posiadają cyberprzestępcy.

Z każdym dniem, z każdą chwilą, w sieci znajduje się coraz więcej użytkowników. Co za tym idzie, zwiększają się przestępstwa, zwiększa się liczba ofiar. Z całą pewnością uregulowanie kwestii prawa cybernetycznego, stanowi największe wyzwanie dla prawa karnego w XXI wieku."[39]

Jak się zabezpieczyć przeciw przestępczości teleinformatycznej – kilka metod zapobiegania nadużyciom bezpieczeństwa sieci. „Ujawniające się coraz nowsze rodzaje naruszeń bezpieczeństwa wymagają opracowania doskonalszych technik zabezpieczenia się przed nimi. Na rynku pojawiło się wiele rozwiązań służących do ochrony zarówno dużych korporacji, mniejszych firm jak i pojedynczych użytkowników Internetu. Są to między innymi:

- firewalle – ściany ogniowe (m.in. Check Point, IPFilter, Cisco PIX Firewall);
- IDS – systemy wykrywania intruzów (m.in. Real Secure, Dragon, Snort, Tripwire);
- Honeypots (m.in. CyberCop Sting – Deception Toolkit);
- standardy Request for Comments (RFC);
- RFC 2644 – zapobiegający atakom typu smurf;
- RFC 2827 uniemożliwiający wysyłanie pakietów z adresem źródłowym pochodzącym z innej (nie własnej) klasy adresowej – antyspoofing.

Każde zdarzenie związane z sesją użytkownika na komputerze lub serwerze jest zapisywane do specjalnego pliku rejestrów. Pliki te tworzą historię działania systemu. Stanowią zapis przeszłości komputera, który ułatwia śledzenie i rozpoznawanie problemów lub ataków. Rejestry mogą być wykorzystywane przy odbudowie systemu (np. po włamaniu), ale także w prowadzeniu dochodzenia.

Każdy log powinien zawierać nazwę programu, funkcji, priorytetu, właściwej treści komunikatu oraz czas zdarzenia."[40]

---

[39] *http://www.vagla.pUskrypts/cybercrime.htm*, (pobrano 22.07.2004 r.)
[40] A. Misiuk, J. Kosiński, *Przestępczość teleinformatyczna*, Szczytno 2002, s. 103

Zakończenie

Internet spełnia znaczącą rolę w kształtowaniu świadomości społecznej o współczesnym świecie, stanowi jeden z wielu czynników istotnych dla rozwoju człowieka XXI wieku.

Uzasadnionym jest domniemanie, iż wraz ze zjawiskiem rozwoju sieci internetowej, łatwości dostępu do niej i zwiększania się liczby internautów, zwiększać się będzie nadal skala przestępczości oraz będą modyfikować się sposoby dokonywania przestępstw w cyberprzestrzeni. Dlatego niezmiernie istotne jest podjęcie działań zmierzających do ograniczenia tego zjawiska przez wszelkie instytucje wychowawcze, opiekunów, rodziców, jak również organy wszelkie ścigania.

Streszczenie

Internet spełnia znaczącą rolę w kształtowaniu świadomości społecznej o współczesnym świecie, stanowi jeden z wielu czynników istotnych dla rozwoju człowieka XXI wieku. Współczesne techniki przechwytywania informacji są poważnym zagrożeniem dla systemów informatycznych. Jedną z groźniejszych metod działania sprawców fałszerstw w teleinformatyce jest „duplikowanie kart bankomatowych przy użyciu wyrafinowanego wyposażenia. Wokół czytników instalowane są skanery pasków magnetycznych. Uzasadnionym jest domniemanie, iż wraz ze zjawiskiem rozwoju sieci internetowej, łatwości dostępu do niej i zwiększania się liczby internautów, nadal zwiększać się będzie skala przestępczości oraz będą modyfikować się sposoby dokonywania przestępstw w cyberprzestrzeni.

Summary

Internet fulfills a significant role in shaping public awareness about the contemporary world, it is one of many factors relevant to the development of man of the twenty-first century. Modern techniques for intercepting information, have become a serious threat to computer systems. One of the most dangerous methods of perpetrators of fraud in ICT is to "duplicate ATM cards using sophisticated equipment. The magnetic stripe scanners are installed around the card readers. It is reasonable to presume that together with the phenomenon of web development, easy access and increasing number of Internet users, the crime rate will continue to increase and the methods of crime in cyberspace will be modified.

Bibliografia

1. Adamski A., *Przestępczość w cyberprzestrzeni*. Toruń 2001
2. Hołyst B., *Kryminologia*. Podstawowe problemy, Warszawa 1977
3. Hołyst B., *Przestępczość w Polsce w latach 1989-2002 prognoza do 2008 r*. Warszawa 2001
4. Horoszkiewicz J., *Przestępczość komputerowa*. Szczytno 2001
5. Jakubski K., *Postępy kryminalistyki*, Zeszyt 1, 1997
6. Kołodzieczak T., Zieliński J., *Podstawy informatyki*. Warszawa 1997
7. Leś B., *Abc Internetu*. Kraków 2001
8. Materiały z seminarium naukowego nt. Techniczne aspekty przestępczości teleinformatycznej, Szczytno 8-9.06.1998 r.

9. Misiuk A., Kosiński J., *Przestępczość teleinformatyczna*. Szczytno 2002
10. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny z późn. zm. Stan prawny na 1stycznia 2004 r.
11. Wójcik J.W., *Hacker. Geniusz czy przestępca*, (w:) „Magazyn Kryminalny 997", 1996
12. Zeszyty Naukowe, Psyche 5. Szczecin 200, nr 311,s. 71 (w:) Zakrzewski P. Prognozowanie kryminologiczne
13. *http://ip.boo.pl/ip-info.php* (pobrano 23.11.2004 r.)
14. *http://republika.pl/systemyoperacyjne/unix.html* (pobrano 23.11.2004 r.)
15. *http://www.vaglą.pUskrYpts/cybercrime.htm*, (pobrano 21.07.2004 r.)
16. *http://www.vagla.pllskrypts/cybercrime.htm*,(pobrano 22.07.2004 r.)
17. *http://www.kartyonline.net/niusy.php?id=991*, (pobrano 22.07.2004 r.)
18. *http://www.vagla.pUskrypts/cybercrime.htm*, (pobrano 22.07.2004 r.)