WIKTYMOLOGICZNE ASPEKTY CYBERPRZESTĘPCZOŚCI

Brunon Hołyst

Uniwersytet Łódzki

Streszczenie. W pracy analizowana są zjawiska towarzyszące rozwojowi Internetu ze szczególnym uwzględnieniem cyberprzestępczości oraz cyberterroryzmu. Omówione zostały także aspekty psychologiczne i wiktymologiczne związane z przestępczością w cyberprzestrzeni. Przeprowadzono analizę zagrożeń i ryzyka z uwzględnieniem czynników podmiotowych i sytuacyjnych.

Słowa kluczowe: cyberprzestępczość, wiktymologia, cyberprzestrzeń, oprogramowanie złośliwe, ataki sieciowe, technologie informatyczne, ofiary cyberprzestępczości, psychologiczne aspekty cyberprzestępczości, edukacja sieciowa, internet a relacje interpersonalne, tożsamość wirtualna

W ostatnich latach jesteśmy świadkami znaczących zmian technologicznych obejmujących różne sfery życia człowieka. Komputeryzacja i powstanie globalnej sieci pociągają za sobą różnorodne konsekwencje, również te niepożądane. I tak w miarę rozwoju internetu i powstania nowych rodzajów usług pojawiły się także rozmaite zjawiska o charakterze patologicznym czy wręcz przestępnym. Czyny te mają specyficzne cechy odróżniające je od innych przestępstw. Sygnalizuje się problemy dotyczące dwóch podstawowych zagadnień, a mianowicie: zakresu osób, którym można przypisać odpowiedzialność karną, oraz kwestii miejsca popełnienia przestępstwa. Podstawowe znaczenie praktyczne ma w przypadku przestępczości internetowej nakreślenie granic stosowania polskiej ustawy karnej i przypisania na tej podstawie odpowiedzialności za czyny, popełniane z wykorzystaniem internetu.

Kodeks karny z 1997 r. objął swym zasięgiem przestępstwa komputerowe i internetowe. Przyjmuje się, iż przestępstwa internetowe to takie, w przypadku których możliwości oferowane przez internet ułatwiły sprawcy realizację zamierzonego czynu przestępnego albo jego poszczególnych stadiów. O przestępczości internetowej mówi się więc, gdy bez użycia internetu nie mogłoby dojść do popełnienia określonego czynu lub jego dokonanie byłoby znacznie bardziej utrudnionej [1]. Internet charakteryzuje się brakiem scentralizowanej kontroli, ogólnoświatowym zasięgiem i powszechną dostępnością. Nieliczne tylko państwa nie mają serwerów podłączonych do sieci. Nad poszczególnymi fragmentami sieci sprawują kontrolę administratorzy określonych serwerów, natomiast nikt nie kontroluj całości sieci. O dy-

namice rozwoju sieci zadecydowały możliwości, które oferuje, stanowiące wynik wskazanych cech.

Ogromna liczba danych, łatwość publikowania, brak kontroli, a także zasięg geograficzny i struktura sieci sprawiły, że internet zaczął być wykorzystywany do popełniania przestępstw, jednocześnie stwarzając trudności dla wymiaru sprawiedliwości w ich ściganiu. W przypadku przestępstw internetowych przypisanie odpowiedzialności karnej wymaga dokonania oceny, czy i jaki czyn zabroniony popełnia dana osoba, jak również ustalenia, czy w danym przypadku do określenia odpowiedzialności karnej znajdzie zastosowanie polski Kodeks karny. Najpierw określa się więc, czy i przez kogo popełniony został czyn zabroniony, a później dopiero bada się, czy sprawca tegoż czynu może ponieść odpowiedzialność na podstawie zasady terytorialności względnie zasady personalnej, zasady podmiotowej obostrzonej lub zasady represji uniwersalnej [1].

Budowa społeczeństwa informatycznego spowodowała ujemny skutek informatyzacji w postaci cyberterroryzmu. Wyobrażenia terrorystów o potajemnym wdzieraniu się do systemów komputerowych w celu wprowadzenia wirusów, kradzieży wrażliwych informacji, zniekształcenia lub usunięcia stron internetowych albo wyłączenia ważnych służb publicznych niepokoją personel do spraw bezpieczeństwa komputerowego na całym świecie. Głośne ataki na strony e-handlowe Yahoo! i e-Bay w 1999 r. czy kontynuowana cybernetyczna święta wojna (dżihad) przeciw izraelskim i amerykańskim stronom w sieci przez pakistańskich hakerów w ramach pomocy palestyńskiej intifadzie to właśnie przykłady ceberterroryzmu.

Wiele informacji sieciowych ma wpływ nie tylko na rodzaje celów i broni wybieranych przez terrorystów, ale również na metody działania ugrupowań terrorystycznych i strukturę ich organizacji. Kilka z tych najbardziej niebezpiecznych organizacji wykorzystuje technikę informacyjną: komputery, oprogramowanie, urządzenia telekomunikacyjne i internet, w celu lepszej organizacji i koordynacji rozproszonych działań. Podobnie jak wiele korporacji wykorzystujących internet do skuteczniejszych i bardziej elastycznych działań, terroryści wprzęgają siłę informacji technicznej (IT) do tworzenia nowych operacyjnych doktryn i form organizacyjnych. I tak jak firmy prywatne tworzą sojusznicze sieci w celu zaopatrzenia klientów w komplet usług, tak ugrupowania terrorystyczne odchodzą od hierarchicznej biurokracji, stają się zdecentralizowane i często zmieniają sieć ugrupowań złączonych wspólnymi celami.

Powstanie powiązanych sieciowo ugrupowań terrorystycznych stanowi część szerszej koncepcji, określanej przez J. Arquillę i D.F. Ronfeldta jako wojna sieciowa (netwar) [2]. Pojęcie to odnosi się do wyłaniającego się

modelu konfliktów i przestępczości w płaszczyźnie społecznej, obejmującego przedsięwzięcia niewystępujące w tradycyjnej wojnie. W modelu tym uczestnicy działają w małych rozproszonych grupach, które komunikują się, koordynują akcje oraz prowadzą kampanie przez internet bez centralnego dowództwa [3].

Wskazuje się, iż przestępczość związana z elektronicznym przetwarzaniem in formacji, określana w literaturze fachowej mianem przestępczości komputerowej, pojawiła się wraz z powstaniem techniki komputerowej ok. 1940 r. i jej rozwojem [4]. Jedną z najgroźniejszych jej odmian, jaka obecnie funkcjonuje w sieciach komputerowych, budząc zaniepokojenie wśród właścicieli systemów i sieci komputerowych, jest tzw. hakerstwo. Liczba dokonywanych w ostatnim czasie włamań komputerowych (określanych mianem przestępczości nowych czasów) związanych bezpośrednio z hakerstwem znacząco wzrosła.

Hakerstwo jako zjawisko subkulturowe jest najczęściej spotykane wśród szczególnie utalentowanej i zainteresowanej nowoczesnymi technologiami młodzieży obytej z techniką komputerową. Jednak nie jest domeną wyłącznie tej kategorii osób, gdyż czynów hakerskich dopuszczają się także zawodowi informatycy. Aktywność tego rodzaju pozostaje w sferze zainteresowań zorganizowanych grup przestępczych o charakterze mafijnym, a przykładem może być działalność rosyjskich złodziei komputerowych, którzy dzięki swoim umiejętnościom potrafią się włamać za pośrednictwem internetu do każdego systemu komputerowego, jeżeli tylko znajdą się tam dane, jakich potrzebują ich mocodawcy.

Najczęściej wykonywanymi czynnościami rosyjskich hakerów są kradzieże znacznych kwot pieniędzy z banków amerykańskich. Dzięki fikcyjnym firmom, utworzonym specjalnie w tym celu, w jednej z tzw. oaz finansowych dokonują transferu ich do Rosji, gdzie mafia rosyjska wykorzystuje je na potrzeby swojej działalności. Szacuje się, iż chodzi o kwoty rzędu setek milionów dolarów. Rosyjskie mafie wynajmują nie tylko hakerów, którzy łamią systemy zabezpieczeń w firmach lub innych instytucjach dla zdobycia potrzebnych im danych. Odnotowuje się także wypadki, kiedy takich działań dokonują hakerzy w celu zaspokojenia potrzeby uznania i zyskania podziwu w środowisku.

W efekcie rozwoju systemów informatycznych wystąpiły nowe, nieprzewidywalne niegdyś zagrożenia. Pojawił się nawet specjalny termin „wojna informatyczna określający techniki ataku na systemy komputerowe. W świetle tych faktów bezpieczeństwo systemów jest podstawowym problemem naszych czasów. Cyberprzestrzeń łączy tysiące sieci komputerowych na całym świecie, dlatego atak destabilizujący na systemy komputerowe dotknąłby miliony komputerów. Wskazuje się, że wojna informatyczna

(mająca postać: szpiegostwa przemysłowego, ataków hakerów, programów niszczących i wirusów, podsłuchu danych, łamania szyfrów, ataków na prywatność oraz ataków z użyciem bomb mikrofalowych i broni magnetycznej) kosztuje USA od 100 do 300 mld dolarów rocznie [5].

Wskazuje się następujące zagrożenia [6]:

- FBI szacuje, że rocznie traci w wyniku ataków na swoje sieci ok. 7,5 mld do larów,
- DISA (Defense Information SecurityAgency) – specjalna agencja Departamentu Obrony USA (DoD) stwierdziła, że aż 88% komputerów w sieci DoD jest pe netrowanych, a w 96% przypadków włamań ich sprawcy nie zostają wykryci,
- CERT (Computer Emergency Response Team) – specjalny zespół reagujący na zdarzenia w sieci szacuje, że rocznie liczba włamań do sieci wzrasta o 75%,
- rosyjscy hakerzy włamali się przez sieć do kont Citibanku, skąd nielegalnie przelali na inne konta ok. 11,6 mln dolarów,
- program SATAN (Security Administrator Tool for Analyzing Networks), rozprowadzany od 1995 r. darmowo w internecie, służący administratorom do sprawdzania bezpieczeństwa ich serwerów, stał się wytrychem w rękach włamywaczy.

Przeprowadzona w 1996 r. przez FBI i CSI (Computer Security Institute) analiza bezpieczeństwa systemów sieciowych 428 organizacji w USA wykazała, że:

- 41% badanych potwierdziło włamanie do ich sieci lub użycie zasobów sieci przez niepowołane osoby; 37% stanowiły instytucje medyczne, a 21% – instytucje finansowe (dane te wskazują, jakie informacje są najcenniejsze dla Amerykanów);
- szpiegostwo gospodarcze było przyczyną 50% ataków (chodzi o wykradanie konkurencji informacji o charakterze ekonomicznym),
- 50% badanych nie miało opracowanych zasad polityki bezpieczeństwa informacji, a z pozostałych 50% – połowa ich nie przestrzegała,
- 20% badanych nie wiedziało, czy ich sieci były atakowane, czy też nie.

W badaniach przeprowadzonych w 1996 r. w 1300 firmach USA i Kanady stwierdzono, że:

- 54% badanych firm poniosło straty w wyniku włamań,
- 78% firm odnotowało straty z powodu wprowadzenia wirusów komputerowych,

– 42% firm zarejestrowało niszczące ataki z zewnątrz, a skutki destabilizacji systemu okazują się bardziej dotkliwe niż włamanie do systemu,
– 25% firm straciło w wyniku włamań ponad 250 tys. dolarów, a 15% – ponad 1 mln; większość firm nie potrafiła określić wielkości wyrządzonych szkód.

Większość ataków jest dokonywanych wewnątrz firm, a ich sprawcami są pracownicy, którzy wykradają informacje lub bezprawnie dostają się do systemu. Dokonanie ataku ułatwia poczucie anonimowości. Specjalne techniki stosowane przez włamywaczy opierają się przede wszystkim na fakcie nieświadomości użytkowników systemów komputerowych, iż te systemy stanowią obiekt ataków. Cechą przestępstwa hakerstwa jest to, że miejsce, gdzie jest ono popełniane, prawie nigdy nie jest miejscem źródła zagrożenia. Narzędziem doskonałym w takich wypadkach jest sam komputer, podłączony do internetu i wyposażony w odpowiednie oprogramowanie.

Wyróżniono dwa sposoby przeprowadzania ataków na systemy komputerowe [4]:

– techniczne, dokonywane dzięki wiedzy informatycznej, jaką posługuje się sprawca takiego przestępstwa, a polegające na wykorzystywaniu siły i oprogramowania posiadanego komputera,
– socjotechniczne, które w gruncie rzeczy polegają na zdobyciu określonej wiedzy na temat atakowanej firmy lub innego „opracowywanego" celu ataku, aby ją następnie wykorzystać do dokonania ataku sposobami informatycznymi. W tym celu potencjalny sprawca zdobywa dane na temat atakowanej instytucji, podając się za jednego z jej pracowników i prosząc o podanie mu hasła dostępu do sieci, ponieważ je zapomniał, bądź też przeprowadza promocję jakiegoś produktu firmy komputerowej, pozostawiając na dyskietce próbkę programu komputerowego z prośbą o jego przetestowanie. W ten sposób w sieci komputerowej jest umieszczany program, za pomocą którego możliwe jest następnie wdarcie się intruza do sieci i pokonanie istniejących w niej zabezpieczeń. W każdym przypadku haker zmierza do przejęcia hasła administratora sieci, gdyż to zapewnia mu bezpośredni dostęp do powłoki programu operacyjnego pracującego w sieci i przejęcie nad nią kontroli.

Według cytowanego autora ataki na sieci i systemy komputerowe mają za zadanie zdobycie odpowiednich informacji poprzez działania polegające na:

– przerwaniu, czyli zniszczeniu części systemu i spowodowaniu jego niedostępności,

– przechwyceniu, co oznacza nic innego jak atak na poufność przesyłanych in formacji bądź danych jedną z możliwych metod – czyli przez podsłuch,
– modyfikacji, polegającej na zdobyciu dostępu i przechwyceniu danych oraz na zmianie pliku z danymi,
– podrobieniu, tj. ataku na autentyczność za pomocą wprowadzenia fałszywych informacji.

Podstawowe rodzaje przestępczości komputerowej polegają przede wszystkim na wykorzystaniu technicznych możliwości, jakimi dysponuje komputer oraz odpowiednie oprogramowanie, ale także na zbieraniu i stosowaniu uzyskanych informacji w prowadzonym ataku na określoną instytucję czy podmiot gospodarczy. Działania takie podlegają karaniu, jak każcie inne przestępstwo pospolite, jednak specyfika dokonywanych w ten sposób przestępstw oraz sposób zbierania materiału dowodowego na potrzeby prowadzonego postępowania wyjaśniającego sprawiają dodatkową trudność organom ścigania i wymiaru sprawiedliwości.

Wnikając do sieci, sprawcy ściągają wiele użytecznych dla siebie programów. Kod znanych programów może być jednak podmieniony lub mogą być dołączane do nich podprogramy o wrogim działaniu, takie jak [6]:

– robak (worm) – jego celem jest powielanie się w komputerach całej sieci. Niezliczona liczba kopii takiego programu powoduje przepełnienie pamięci komputera, a w rezultacie – dezorganizację pracy w całym systemie,
– wirus – w odróżnieniu od robaka spokojnie drzemie ukryty w programie dopóty, dopóki nie zostanie uruchomiony. Po uruchomieniu atakuje system w mniej lub bardziej groźny sposób, osłabiając jego działanie i bezpieczeństwo,
– koń trojański – jest to pozornie użyteczny program, zwykle uruchamiany przez specyficzne dane lub właściwe słowo w dokumencie. Służy przyszłemu włamywaczowi do zdobywania określonych informacji. W pewnych przypadkach program ten powoduje automatyczny wysyłania e-maili zwrotnych z cennymi danymi do jego autora, który później wykorzysta je podczas próby ataku;
– bomba logiczna – uruchamia się w określonym czasie (jest nim np. pewna data lub kluczowe słowo) i wpływa destrukcyjnie na system,
– wrogi aplet Javy – program napisany w języku Java, który jest podstawowym narzędziem programowania w internecie – może zawierać w sobie podprogram o destrukcyjnym działaniu. Podczas ściągania dokumentów i uruchamiania programów w tej technologii atakuje wybrane stacje mimo zabezpieczeń na serwerach sieci.

Zazwyczaj głównym obiektem ataku jest główny serwer sieci, na którym znajdują się wszystkie informacje o atakowanym systemie. Atak jest przeprowadzony w różnych kierunkach w celu stwierdzenia istnienia luk bezpieczeństwa w oprogramowaniu pracującym na serwerze. Luki te są zwykle wynikiem błędów w oprogramowaniu, konfiguracji systemu czy protokołach transmisji danych.

Wyróżnia się następujące rodzaje ataków:

- zgadywanie haseł, stanowiące podstawową metodę, którą zwykle stosują hackerzy; polega ona na zdobywaniu haseł chroniących dostęp do serwera. W tym celu używa się specjalnych programów do ich łamania (tzw. crack), zawierających słowniki różnojęzyczne. Programy te podczas próby zdobycia dostępu do systemu automatycznie podstawiają kolejne wyrazy ze słowników aż do osiągnięcia skutku. Hasła są z reguły proste: najczęściej imię użytkownika konta jest nazwa konta, a zatem zadanie nie jest trudne. Często niektóre konta w ogóle nie są chronione hasłami,
- maskaradę, polegającą na tym, iż po zdobyciu informacji o sieci atakujący może się podszyć pod jeden z komputerów, któremu serwer sieci „ufa" (przez podanie jego numeru IP jako swojego), i w ten sposób może się do niego dostać. Atakujący może np. wysłać dane ze sfałszowanym adresem poczty elektronicznej, które zostaną przez serwer przyjęte. W danych tych może być ukryty koń trojański, który uruchomi program przeszukujący dysk serwera, odnajdzie plik z kontami i hasłami użytkowników i wyśle je e-mailem zwrotnym do fałszywego nadawcy. Atakujący może podszyć się także pod adres serwera www, z którego atakowany serwer ściąga informację. Atakujący przekazuje atakowanemu prośbę o przesłanie żądanej strony www i dostarcza ją prawdziwemu adresatowi. W ten sposób można oszukiwać np. firmę inwestującą na giełdzie, podając fałszywe wyniki i w konsekwencji doprowadzić ją do bankructwa,
- podsłuch, polegający na tym, iż atakujący stosuje monitoring ruchu w sieci i przechwytuje transmisję pomiędzy poszczególnymi komputerami. Przechwycenie transmisji pozwala zdobyć hasło użytkownika, który loguje się właśnie do serwera, a następnie podszyć się pod niego i zdobyć dostęp do wybranego komputera w sieci,
- szukanie luk, wyrażające się w poszukiwaniu słabych stron w systemie zabezpieczeń i stanowiące podstawowy cel ataku przestępców. Luki te są wynikiem błędów w oprogramowaniu lub konfiguracji systemu. Atakujący posługuje się niekiedy specjalnymi skanerami internetowymi – programami sprawdzającymi wybrany system pod kątem istnienia

owych luk. Najbardziej znanym skanerem jest program Satan, napisany specjalnie dla administratorów do sprawdzenia poziomu bezpieczeństwa ich serwerów,

– blokowanie serwisów, polegające na destabilizowaniu sieci przez wyłączanie na serwerze internetu takich serwisów jak poczta elektroniczna. Atak polega na wysyłaniu potoku informacji powodujących przeładowanie pamięci serwera, a w konsekwencji jego destabilizację. Jeden z najbardziej znanych ataków tego typu polega na wysyłaniu dużej liczby pakietów inicjujących połączenia dla wybranej usługi (np. poczty elektronicznej). Serwer nie nadąża za realizacją połączeń i blokuje dostęp do danej usługi. W ten sposób hakerzy mogą sabotować działanie poczty elektronicznej na serwerach dostawców internetu,
– socjotechnikę, oznaczającą w żargonie hakerskim manipulowanie ludźmi w taki sposób, aby ujawnili poufne informacje ułatwiające włamanie do systemu komputerowego. Przed dokonaniem ataku na wybraną sieć atakujący przeprowadza specjalny wywiad na temat wybranej firmy o: osobach w niej zatrudnionych, konfiguracji sieci, zasobach systemu, hasłach użytkowników itp. Może też wykorzystywać element zaskoczenia, np. dzwoniąc do administratora sieci, przedstawiając się jako szef jednego z działów i prosząc o zmianę hasła swojego konta. Wielu użytkowników systemu zapisuje swoje hasła na kartkach i chowa je pod klawiaturą lub do szuflady, a czasem nakleja na monitor komputera. Haker, podając się za pracownika serwisu, może te kartki łatwo odnaleźć. Inny sposób polega na dokładnym przeglądaniu za wartości śmietników znajdujących się na zapleczach firm, gdzie czasami można znaleźć np. stare notesy z telefonami i hasłami, rejestry zatrudnionych, dane techniczne o sprzęcie komputerowym stanowiące cenne źródło informacji o firmie,
– terroryzm sieciowy, polegający na tym, iż różne organizacje terrorystyczne szantażują jakąś firmę, grożąc zniszczeniem danych lub destabilizacją systemu. W przypadku instytucji finansowej lub laboratorium badawczego, gdzie sieć zarządza wszystkimi procesami, problem ten nabiera wielkiej wagi. Współcześnie istnieją narzędzia, za pomocą których można zdezorganizować pracę całego systemu informatycznego bez wchodzenia do niego i bez odcinania zasilania. Chodzi o tzw. bomby mikrofalowe generujące duży impuls fali elektromagnetycznej o odpowiedniej częstotliwości, powodujący zakłócenie i destabilizację pracy wszystkich urządzeń elektronicznych. Taka bomba, znajdująca się w neseserze terrorysty (który np. jako biznesmen podejmuje pieniądze w banku), może w jednej chwili – nie budząc żadnych podejrzeń – zdezorganizować bankowy system informacyjny.

Wyróżnia się pięć podstawowych grup włamywaczy [6]:

- turystów, których celem jest zdobycie dostępu do czyjegoś konta, aby rozpocząć wędrówkę po internecie,
- wandali, dążących do zniszczenia w systemie czegokolwiek bądź dla zabawy, bądź w określonym celu, np. sformatowania dysku, wprowadzenia wirusa lub wrogiego appletu Jayy, zmiany stron www,
- zdobywców, których celem jest wejście każdym możliwym sposobem do systemu, aby pokazać swoje umiejętności, choć zazwyczaj czynią to przez złamanie systemu zabezpieczeń,
- szpiegów, wchodzących do systemu w konkretnym celu, np. wykradzenia in formacji lub destabilizacji systemu,
- cyberterrorystów, którzy, stosując specjalne techniki, destabilizują pracę systemów informatycznych; najczęściej szantażują wybrane firmy, żądając ogrom nych okupów.

Wykorzystując zarówno luki bezpieczeństwa w systemach, w których pracują serwery internetu, błędy w protokołach transmisji danych i konfiguracji serwerów www, jak również destabilizując systemy zabezpieczeń, hakerzy dążą do zdobycia dostępu do informacji w wybranej sieci przez internet. Wszelkie informacje o metodach włamań znajdują się w sieci, a hakerzy wymieniają się doświadczeniami na specjalnych, zamkniętych listach dyskusyjnych. Zwraca się uwagę, iż haker poza tym, że interesuje się zabezpieczeniami sieci komputerowych firm i urzędów, w gruncie rzeczy jest anarchistą [4]. Obowiązujący go kodeks honorowy zabrania mu korzystania z nielegalnie zdobytych danych, chociaż niektórzy kradną drobne sumy na własne potrzeby.

Odmianą hakera jest phreaker, który jest także anarchistą. Wykorzystuje zdobyte przez siebie umiejętności do włamywania się wszędzie tam, gdzie najtrudniej się włamać. Może być bardzo niebezpieczny w sytuacji, kiedy znajdzie się w posiadaniu tajnych danych, bo wówczas ujawni je bez wahania. Zwykle człowiek ten jest bardzo młody i podatny na wszelkiego rodzaju wpływy, co może spowodować dodatkowe zagrożenia. Może się to zdarzyć w sytuacji, gdy znajdzie się pod wpływem poglądów reprezentowanych przez radykalną organizację.

W odróżnieniu od dwóch poprzednich rodzajów przestępców komputerowych tzw. kraker nie ma żadnych zahamowani i nie przestrzega żadnego z kodeksów honorowych. Zajmuje się nie tylko przełamywaniem wszelkiego rodzaju zabezpieczeń sieci i systemów komputerowych, lecz także ściąganiem tajnych danych w celu ich dalszej odsprzedaży temu, kto więcej za nie zapłaci. Włamuje się do systemów bankowych, dokonując tam niewielkich kradzieży. Potrafi być jednak groźny, zwłaszcza gdy, przebywając w danej

sieci, zakaża wirusem komputerowym oraz kiedy ma trudności z pokonaniem zabezpieczeń. Głównym źródłem jego utrzymania jest zajęcie polegające na przełamywaniu kodów zabezpieczających gry komputerowe oraz łamanie blokad znajdujących się w telefonach komórkowych.

Złodziej komputerowy działa na zlecenie i może przejmować cudzą korespondencję, podsłuchiwać oraz przejmować pliki, włamywać się do wskazanych komputerów w celu zdobycia określonych danych, o które zabiega jego zleceniodawca, albo też zarażać wirusami firmowe sieci na zlecenie konkurencji czy dokonywać na własny lub cudzy rachunek nielegalnych przelewów bankowych i tak naprawdę to jest jego główne zadanie. Zwraca się uwagę, iż polscy hackerzy tworzą zamknięte, kilkusetosobowe środowiska, aktywne głównie w dużych miastach, takich jak Warszawa, Poznań, Wrocław czy Gorzów Wielkopolski. Pierwsze włamania do sieci komputerowych w Polsce miały zazwyczaj charakter poznawczy. Młodzi ludzie, w większości studenci korzystający z sieci uczelnianej, często usiłowali się dostać do innego komputera podłączonego do sieci, po to aby udowodnić sobie, że są w stanie złamać istniejące zabezpieczenia.

Pierwsze głośne włamanie do sieci internetu w Polsce miało miejsce 13 grudnia 1995 r. Było to włamanie do węzła sieci NASK (Naukowej Akademii Sieci Komputerowej) w Warszawie, a zakończyło się modyfikacją pierwszej strony www tej instytucji. Haker występujący pod pseudonimem „Gumiś", zaprotestował w ten sam sposób przeciwko nowemu cennikowi usług NASK, w którym wprowadzono zasadę opłaty za ruch w miejsce używanej powszechnie w internecie stałej odpłatności za przepustowość łącz. Kolejnego włamania dokonano w nocy z 3 na 4 maja 1997 r. na serwer Biura Informacyjnego Rządu RP. Ataku dokonali dwaj szesnastoletni chłopcy, używając gotowych przepisów, pozyskanych za pośrednictwem internetu. Dzięki atakowi pozwolono im na zmodyfikowanie głównej strony www tej instytucji. W wyniku takich działań okazało się, że instytucje rządowe nie mają zabezpieczeń przed tego rodzaju włamaniami.

8 sierpnia 1997 r. obiektem zamachu stał się największy serwer FTP w Polsce, słynna „słoneczna strona (sun site), zlokalizowany w ICM (Interdyscyplinarnym Centrum Modelowania Matematycznego i Komputerowego). Hakerom udało się dotrzeć do plików umieszczonych w tzw. powłoce (secure shell) systemu operacyjnego, do którego dostęp ma wyłącznie administrator sieci. Dzięki tym zabiegom podłożyli oni tzw. konia trojańskiego, modyfikując w ten sposób udostępniane na serwerze źródła programu SSH.

W przypadku ataku na systemy bankowe niewiele zazwyczaj wiadomo o tego rodzaju zdarzeniach, gdyż banki ukrywają takie incydenty w obawie przed utratą zaufania dotychczasowych klientów. Dane, jakimi dysponują

organy ścigania, są niepełne, zaś ciemna liczba popełnionych i niewykrytych ataków na sieci komputerowe wynosi 90–95% [4]. Na świecie często dochodzi do działań pojedynczych hakerów lub całych grup, do ataków na największe firmy internetowe, najpopularniejsze strony www (World Wide Web) oraz na serwery instytucji bankowo-finansowych o charakterze strategicznym w wielu krajach. Ataki takie zarejestrowano w wielu krajach świata, a zwłaszcza w Stanach Zjednoczonych Ameryki Północnej, gdzie do zwalczania tego rodzaju przestępczości są używane wyspecjalizowane służby:
FBI, NSA czy też CIA. Wynika to przede wszystkim z tego, że większość systemów obronnych i bankowych opiera swoje funkcjonowanie na tym, że sieci te są podłączone bezpośrednio do ogólnoświatowej „pajęczyny internetu. Działania zmierzające do przejęcia kontroli nad ich funkcjonowaniem polegają przede wszystkim na pokonaniu wielu zabezpieczeń stosowanych przez poszczególnych operatorów sieciowych. Najczęściej stosowanymi urządzeniami są tzw. ściany ognia, stanowiące jeden z istotnych elementów polityki bezpieczeństwa sieci i systemów komputerowych.

Wskazuje się, iż jedną z podstawowych kwestii wymagających rozstrzygnięcia jest ustalenie, kto winien ponosić odpowiedzialność za przestępstwo popełnione w sieci [1]. Nie chodzi tu jednak o analizę, czy w konkretnej sytuacji spełnione są przesłanki opisane w art. 1 Kodeksu karnego stanowiące podstawę przyjęcia odpowiedzialności karnej, to jest: zachowanie będące czynem zabronionym pod groźbą kary, zawinionym, lecz o zakreślenie kręgu podmiotowego osób, które ponosić będą odpowiedzialność karną w związku ze stwierdzonym przestępstwem internetowym [7].

Oprócz osób popełniających czyny zabronione poprzez głoszenie zakazanych treści na stronach sieci i nielegalne rozpowszechnianie cudzych utworów czy też dokonujących przestępstw przeciwko ochronie informacji i przeciwko mieniu, czyli sprawców wykonawczych, odpowiedzialność będą ponosić także pomocnicy. Udzielanie pomocy może wyrażać się w udostępnianiu programu komputerowego służącego przełamywaniu haseł dostępu do systemów komputerowych. Efektem określonego przestępstwa może być także umożliwienie innym osobom popełnienia odrębnego czynu zabronionego, pozostającego w związku z pierwszym przestępstwem w takim sensie, że bez zaistnienia pierwszego czynu nie byłoby możliwe popełnienie drugiego. Przykładowo: nielegalne rozpowszechnianie cudzego programu komputerowego za pośrednictwem sieci umożliwia innym użytkownikom internetu popełnienie przestępstwa opisanego w art. 278 2 Kodeksu karnego, czyli uzyskanie bez zezwolenia cudzego programu komputerowego w celu osiąg nięcia korzyści majątkowej.

Wymienia się pięć podmiotów, które potencjalnie mogłyby ponosić odpowiedzialność cywilnoprawną za udostępnianie materiałów w sieciach. Należą do nich [8]: dysponent i operator sieci telekomunikacyjnej (przedsiębiorstwo telekomunikacyjne); dostawca dostępu do internetu, tj. ten, kto oferuje i umożliwia dostęp, nie posiadając wpływu na treść przekazywanych komunikatów; autor i dostawca materiałów wprowadzanych do sieci; dostawca usług sieciowych, np. udostępniający miejsce na swoim serwerze; użytkownik końcowy. Warto zwrócić uwagę, iż ten sam podmiot może łączyć różne funkcje, np. gdy dostawca dostępu do sieci jest jednocześnie dostawcą usług sieciowych. Odnośnie do dokonanego rozróżnienia pomiędzy autorem i dostawcą materiałów oraz użytkownikiem końcowym wyjaśnić należy, iż pewne czyny popełniane mogą być jedynie przez autorów i dostawców materiałów wprowadzanych (rozpowszechnianie zakazanych treści, niektóre przestępstwa naruszenia praw autorskich), zaś inne jedynie przez użytkowników końcowych (przestępstwa przeciwko ochronie informacji, przestępstwa przeciwko mieniu, niektóre przestępstwa naruszenia praw autorskich inne niż popełnianie przez dostawców materiałów). Kategorie tych czynów są zasadniczo rozłączane, tj. inne przestępstwa popełnić może autor lub dostawca materiałów wprowadzanych do sieci, inne natomiast użytkownik końcowy.

Przeciwko przypisywaniu odpowiedzialności karnej dysponentom sieci telekomunikacyjnej oraz dostawcom dostępu do internetu przemawia argument, iż otwierają jedynie drogę do cudzych treści, podobnie jak poczta, telekomunikacja czy przedsiębiorstwo transportowe. Zdaniem niektórych autorów bezdyskusyjna pozostaje kwestia odpowiedzialności autora materiałów wprowadzonych do sieci jako sprawcy wykonawczego [1]. Sprawcą takim jest zarówno autor konkretnego tekstu naruszającego prawo, jak i osoba, która taki tekst umieszcza na swojej stronie sieci, zgadzając się i identyfikując z jego treścią.

Problem nie dotyczy sytuacji, w której przytoczenia cudzego tekstu dokonano celem podjęcia z nim polemiki. Sprawcą wykonawczym będzie ten użytkownik końcowy, który za pośrednictwem internetu popełnia konkretny czyn zabroniony. Oczywiście nie popełnia czynu zabronionego użytkownik, który dzięki sieci zapoznaje się z treściami przez prawo zakazanymi, a głoszonymi przez osoby trzecie.

Wskazuje się, iż najwięcej uwagi poświęcić trzeba kwestii odpowiedzialności dostawcy usług sieciowych, czyli osoby pośredniczącej w dostarczaniu materiałów pochodzących od osób trzecich pośredniczących względnie dostarczających środków technicznych, bez których nie mogłoby dojść do dokonania przez inną osobę czynu zabronionego. W przypadku przestępstw popełnianych w internecie istotne jest określenie, na jakich zasa-

dach odpowiedzialność ponosić powinni właściciele (administratorzy) serwerów, na których umieszczone zostały treści zakazane przez prawo bądź za pomocą których popełniono inny czyn zabroniony, oraz osoby pro wadzące katalogi internetowe, w których zawarte zostały adresy stron sieci zawierających treści zabronione.

Odnośnie do dokonanego rozróżnienia pomiędzy autorem i dostawcą materiałów oraz użytkownikiem końcowym wyjaśnić należy, iż pewne czyny popełniane mogą być jedynie przez autorów i dostawców materiałów wprowadzanych (rozpowszechnianie zakazanych treści, niektóre przestępstwa naruszenia praw autorskich), zaś inne jedynie przez użytkowników końcowych (przestępstwa przeciwko ochronie informacji, przestępstwa przeciwko mieniu, niektóre przestępstwa naruszenia praw autorskich inne niż popełnianie przez dostawców materiałów). Kategorie tych czynów są zasadniczo rozłączane, tj. inne przestępstwa popełnić może autor lub dostawca materiałów wprowadzanych do sieci, inne natomiast użytkownik końcowy.

Przeciwko przypisywaniu odpowiedzialności karnej dysponentom sieci telekomunikacyjnej oraz dostawcom dostępu do internetu przemawia argument, iż otwierają jedynie drogę do cudzych treści, podobnie jak poczta, telekomunikacja czy przedsiębiorstwo transportowe. Zdaniem niektórych autorów bezdyskusyjna pozostaje kwestia odpowiedzialności autora materiałów wprowadzonych do sieci jako sprawcy wykonawczego Sprawcą takim jest zarówno autor konkretnego tek stu naruszającego prawo, jak i osoba, która taki tekst umieszcza na swojej stronie sieci, zgadzając się i identyfikując z jego treścią.

Problem nie dotyczy sytuacji, w której przytoczenia cudzego tekstu dokonano celem podjęcia z nim polemiki. Sprawcą wykonawczym będzie ten użytkownik końcowy, który za pośrednictwem internetu popełnia konkretny czyn zabroniony. Oczywiście nie popełnia czynu zabronionego użytkownik, który dzięki sieci zapoznaje się z treściami przez prawo zakazanymi, a głoszonymi przez osoby trzecie.

Wskazuje się, iż najwięcej uwagi poświęcić trzeba kwestii odpowiedzialności dostawcy usług sieciowych, czyli osoby pośredniczącej w dostarczaniu materiałów pochodzących od osób trzecich pośredniczących względnie dostarczających środków technicznych, bez których nie mogłoby dojść do dokonania przez inną osobę czynu zabronionego. W przypadku przestępstw popełnianych w internecie istotne jest określenie, na jakich zasadach odpowiedzialność ponosić powinni właściciele (administratorzy) serwerów, na których umieszczone zostały treści zakazane przez prawo bądź za pomocą których popełniono inny czyn zabroniony, oraz osoby pro wadzące katalogi internetowe, w których zawarte zostały adresy stron sieci zawierających treści zabronione.

Zapewnienie dostępności strony sieci innym jej użytkownikom wymaga, by były one zapisane w postaci pliku komputerowego na twardym dysku serwera, czyli komputera niebędącego zazwyczaj własnością autora strony. Miejsce na serwerach udostępniane jest przez wiele firm odpłatnie bądź nawet nieodpłatnie, a strony sieci może właściwie każdy użytkownik komputera stworzyć za pomocą łatwo dostępnych programów. W efekcie powszechna jest możliwość stworzenia własnej strony i umieszczenia jej w sieci. Powstaje problem, czy administratorzy serwera zatrudnieni przez właściciela zobowiązani są do dbania, aby treści umieszczane na stronach sieci znajdujących się na serwerach nie naruszyły prawa, a jeżeli łamią prawo, to na jakich zasadach administratorzy serwerów zezwalających na umieszczenie na nich stron bez kontroli ich treści mogą ponosić odpowiedzialność karną właśnie za umożliwienie bądź ułatwienie inny osobom popełnienia przestępstwa.

Odpowiedzialność za pomocnictwo jako zjawiskową postać przestępstwa, którego istotą jest ułatwienie popełnienia przez inną osobę czynu zabronionego, przewiduje Kodeks karny w art. 18 & 3 [7]. Zwraca się uwagę, iż udzielanie pomocy, o charakterze fizycznym polega przykładowo na dostarczeniu narzędzia. Narzędziem tym może być każdy przedmiot ułatwiający dokonanie czynu zabronionego, przy czym nie jest wówczas konieczny osobisty kontakt udzielającego pomocy ze sprawcą [7]. Karalne pomocnictwo może polegać także na zaniechaniu – wówczas na pomocniku spoczywać musi prawny, szczególny obowiązek niedopuszczenia do popełnienia czynu zabronionego. Istotą strony podmiotowej pomocnictwa jest zamiar bezpośredni lub wynikowy, przy czym pomocnik musi mieć wyobrażenie konkretnego czynu zabronionego. Dla przypisania odpowiedzialności nie jest wystarczający zamiar, aby inna osoba popełnia dowolny czyn zabroniony. Kwestia ta jest bardzo istotna w przypadku rozważań dotyczących przestępczości internetowej obejmującej czyny polegające na głoszeniu treści zakazanych przez prawo.

Zwraca się uwagę, iż pomocnictwa nie stanowi samo umożliwienie umieszczenia dowolnych treści na serwerze, co pozwala przenieść ciężar rozważań z pierwszej części ustawowej definicji na zdanie drugie, mówiąc o szczególnym obowiązku niedopuszczenia do popełnienia czynu zabronionego. Samo bowiem udostępnienie miejsca na serwerze nie może powodować odpowiedzialności karnej gdyż nie od jego właściciela zależy sposób, w jaki zostanie wykorzystany. W przypadku pomocnictwa przez zaniechanie czynności wbrew szczególnemu obowiązkowi konieczne jest, aby pomocnik znajdował się wobec dobra chronionego w pozycji gwaranta nienastąpienia skutku. Obowiązek określający pozycję gwaranta musi mieć

charakter prawny. Gwarantem ustanowione są osoby charakteryzujące się szczególnym stosunkiem do określonego dobra prawnego.

Praktycznie wszystkie z istniejących firm udostępniających miejsca na serwerach zarówno odpłatnie, jak i nieodpłatnie, zastrzegają w regulaminach, że użytkownicy nie mogą na stronach sieci umieszczać treści umieszczać treści niezgodnych z polskim prawem, a złamanie tego zakazu stanowi podstawę do usunięcia takiej strony [7]. Mimo iż regulamin rozpatrywany jako umowa cywilnoprawna wiąże jedynie strony umowy, a osoby trzecie nie mogą w treść stosunku prawnego ingerować ani obowiązków stron egzekwować, to jednak należy rozważyć, czy poprzez ustanowienie takiego regulaminu administrator nie podjął się pełnienia roli gwaranta niewystąpienia czynu zabronionego, przez co umowa wywrzeć może skutki nie tylko w sferze prywatnoprawnej. Stanowiłoby to przejęcie przez administratora na siebie odpowiedzialności za to, aby stron sieci, za pomocą których użytkownicy popełniają przestępstwa, na administrowanych serwerach nie utrzymywać.

Nie jest na ogół możliwe kontrolowanie treści nowych stron przed ich umieszczeniem na serwerze zarówno ze względów technicznych, jak i wobec faktu, iż stanowiłoby to zakazaną cenzurę prewencyjną. Ponieważ gwarant powinien jednak podejmować czynności prowadzące do zmniejszenia niebezpieczeństwa popełnienia czynów zabronionych, to obowiązkiem administratora byłoby stworzenie takiego właśnie systemu kontroli, aby strony łamiące prawo sprawnie wykrywać i niezwłocznie po tym je usuwać bądź blokować. Niedbałe przeprowadzenie takiej kontroli bądź w ogóle jej zaniechanie rodzić powinno, w razie wystąpienia przestępstwa, odpowiedzialność administratora jako pomocnika, który „wbrew prawnemu szczególnemu obowiązkowi niedopuszczenia do popełnienia czynu zabronionego swoim zachowaniem ułatwia innej osobie jego popełnienie. Stopień staranności winien być wówczas dochowany z punktu widzenia racjonalnie działającego gwaranta, tj. podmiotu znającego określoną dziedzinę działalności, znającego przyjęty na siebie obowiązek odpowiednio ukierunkowanego działania oraz mającego postawę sumiennego wykonawcy obowiązku.

Zwraca się uwagę, iż należy nie zapominać o argumentach przeciwników nałożenia na dostawców usług sieciowych obowiązku monitorowania treści udostępnianych za ich pośrednictwem. Dostawcy mają ograniczone możliwości bieżącego nadzorowania materiałów wprowadzanych do sieci za ich pośrednictwem, gdyż jeśli będą decydować, czy określona treść jest zgodna z prawem, może to naruszać konstytucyjne prawo wolności słowa oraz dostępu do informacji, a także ograniczać sferę prywatności użytkowników [8].

W przypadku popełnienia przestępstwa przez sprawcę wykonawczego późniejsze usunięcie strony sieci, za pomocą której popełniono czyn zabroniony, nie od wróci negatywnych skutków ani też nie zwolni sprawcy wykonawczego z odpowiedzialności, lecz takie postępowanie administratorów, a szczególnie działanie podejmowane z własnej inicjatywy, a nie po interwencji osób trzecich, stanowić winno podstawę do przyjęcia, iż po stronie administratora brak było zamiaru ewentualnego przyjęcia odpowiedzialności za pomocnictwo. Podkreśla się, iż zamiar bezpośredni po stronie administratora, a więc chęć popełnienia przestępstwa internetowego przez inną osobę, występować może jedynie sporadycznie. Co więcej, usuwanie stron WWW łamiących prawo spełnia także funkcje prewencji generalnej poprzez zamanifestowanie osobom chcącym takie strony umieścić, że działania przestępne nie będą tolerowane. Taką politykę największych firm-dostawców usług sieciowych dostrzegają już potencjalni twórcy takich stron.

Osoby prowadzące katalogi stron sieci są również grupą, która może ponosić odpowiedzialność w związku z popełnionym przestępstwem internetowym. Ważną cechą internetu jest to, iż samo stworzenie i umieszczenie witryny na serwerze nie jest wystarczające dla dotarcia do szerszego kręgu odbiorców. Liczba dokumentów zawartych w sieci umożliwia użytkownikowi odnalezienie interesujących go informacji bez pomocy wyspecjalizowanych narzędzi. Służą temu właśnie katalogi tematyczne oraz tzw. wyszukiwarki internetowe, np. Google czy Yahoo, które dokonują przeglądu indeksowanych stron sieci z uwagi na obecność na nich wskazanych przez użytkownika kluczowych haseł.

Kwestia czasu popełnienia czynu zabronionego jest ważnym problemem, ponieważ przypisanie odpowiedzialności za pomocnictwo możliwe jest wówczas, gdy zaszło przed dokonaniem czynu zabronionego lub w jego trakcie. Artykuł 6 & 1 Kodeksu karnego stanowi, iż czyn zabroniony uważa się za popełniony w czasie, w którym sprawca działał lub zaniechał działania, do którego był zobowiązany. W przypadku przestępstw internetowych polegających na prezentowaniu treści przez prawo zakazanych czy też naruszeń praw autorskich stan bezprawności utrzymuje się przez cały okres, w którym strona sieci zawierająca taką treść znajduje się na serwerze. Sytuacja taka jest odmienna od np. wydrukowania określonego tekstu w prasie lub wypowiedzi w radiu lub telewizji w tych przypadkach sprawca po dokonaniu czynu nie ma już możliwości ingerencji w treść ani nie ma możliwości jej wycofania.

W przypadku stron sieci autor cały czas może swobodnie ich treść zmieniać lub usuwać. W takiej zaś sytuacji czyn zabroniony należy uznać za popełniany w ciągu całego okresu utrzymywania się stanu bezprawnego

[7]. W razie głoszenia treści zakazanych przez prawo lub nielegalnego udostępniania utworu możliwe jest zatem postawienie osobom prowadzącym katalog czy też administratorowi serwera za rzutu pomocnictwa w popełnieniu czynu zabronionego przez cały okres, w którym strona taka znajduje się na serwerze bądź odsyłacz do niej pozostaje w katalogu.

Obowiązkiem osób prowadzących katalog winno być przygotowanie systemu kontroli wpisywanych adresów, tak aby eliminować strony sieci, za pomocą których popełniane są czyny zabronione, zaś wykazany stopień staranności powinien wpływać na ocenę możliwości przypisania zamiaru ewentualnego [1].

Biorąc pod uwagę zarówno niebezpieczeństwa, jak i korzyści wynikające z funkcjonowania internetu, pierwszeństwo przyznać należy zdecydowanie tym drugim.

Z tego względu wszelkie kroki mające na celu limitowanie możliwości wprowadzania do sieci własnych materiałów muszą być podejmowane w sposób ostrożny i wyważony.

Wątpliwości budzić może przede wszystkim sposób realizacji obowiązku monitorowania przez właścicieli serwerów materiałów umieszczanych na tych serwerach przez osoby trzecie. Prowadzi to bowiem do sytuacji, kiedy to administrator decyduje, czy konkretne treści są legalne, czy nie. Ponieważ ograniczanie wolności słowa następować może jedynie na podstawie ustaw, to tylko powołane ku temu organy mogą te ograniczenia egzekwować,a warunek taki w sposób ewidentny nie był wówczas spełniony. Można wyobrazić sobie sytuację, w której administrator serwera usuwa stronę, traktując ją za łamiącą prawo, a następnie autor strony przed sądem uzyskuje korzystne rozstrzygnięcie, wskazując, iż prawa nie naruszył.

W przypadku zmiany treści obowiązku monitorowania zawartości serwera po przez przyjęcie, że administrator winien jedynie współpracować z policją w razie wykrycia zakazanych materiałów bez możliwości ich usuwania, może z kolei po wstać sytuacja, w której administrator poniósłby odpowiedzialność karną z tytułu rozpowszechniania treści naruszających przepisy prawa. Uznać jednak na leży, że propozycja pierwsza jest rozsądniejsza prawdopodobieństwo opisanej sytuacji jest niższe i pociąga za sobą zdecydowanie mniejsze ewentualne szkody niż całkowite zaniechanie usuwania stron sieci w oczekiwaniu na decyzję prokuratora bądź sądu. Nie istnieje inna metoda regulacji i kontroli treści prezentowanych w internecie niż działania organów wymiaru sprawiedliwości. Decydującą rolę odgrywać jednak powinny, w opinii cytowanego powyżej autora, instytucje powołane do zwalczania przestępczości, a przyznanie prawa kontroli nad treściami

prezentowanymi w internecie np. utworzonemu dla tego celu urzędowi będzie ustanowieniem niedopuszczalnej cenzury.

Zgodnie z regulacjami przyjętymi w różnych państwach europejskich dostawca usług sieciowych ponosi odpowiedzialność tylko wtedy, gdy można od niego wymagać uznania określonego materiału za nielegalny lub gdy zaniechał usunięcia takiego materiału po tym, jak określono jego nielegalny charakter. Rozwiązanie takie wydaje się najrozsądniejsze. Nałożenie natomiast zbyt daleko idących obowiązków może zahamować rozwój internetu zaangażowanie dostawców usług w rozwój sieci będzie tym mniejsze, im większy będzie zakres ich odpowiedzialności, ze względu na zbyt wysokie ryzyko podejmowania takiej działalności.

Projekt konwencji Rady Europy o przestępstwach w sieci wprowadza odpowiedzialność osób prawnych za przestępstwo komputerowe, jednakże ogranicza ją je dynie do przypadków uzyskania korzyści majątkowej przez daną osobę prawną, a popełnione przez osobę fizyczną działającą indywidualnie bądź w ramach organu, posiadającą decydującą pozycję w ramach tejże osoby prawnej; odpowiedzialność można również przypisać w sytuacji, gdy popełnienie przestępstwa zo stało umożliwione przez brak nadzoru lub kontroli ze strony osoby fizycznej, o której mowa wyżej. Wyraźnie podkreśla się, że przepis ten nie dotyczy przestępstw popełnionych przez klientów, użytkowników lub osoby trzecie, a ograniczony jest ściśle do przestępstw popełnionych przez osoby o decydującej pozycji w ramach osoby prawnej, dokonanych dla osiągnięcia przez osobę prawną korzyści majątkowej. Objaśnienia zawarte w projekcie wprost wskazują, że odpowiedzialności nie ponosi pomocnik, któremu nie można przypisać zamiaru popełnienia przestępstwa [1].

Warto zwrócić uwagę na możliwości zapobiegania tego typu przestępczości m.in. przez stosowanie kompleksowych metod zabezpieczeń sieci komputerowych. Najważniejszym elementem bezpieczeństwa danej organizacji jest spójna polityka bezpieczeństwa, określająca następujące etapy procesu zabezpieczania informacji [6]. Na etapie pierwszym zachodzi budowanie podstawy analizowanie przez kierownictwo firmy jej potrzeb i możliwości, określenie wartości posiadanych danych, wyznaczenie osób odpowiedzialnych za wdrożenie procesu zabezpieczenia informacji. Na etapie drugim mamy do czynienia z prowadzeniem dokumentacji systemu informatycznego, usuwaniem błędów w tym systemie oraz uświadamianiem jego użytkownikom grożących niebezpieczeństw (zapisywanie haseł, wirusy itp.).

Na etapie trzecim ma miejsce podnoszenie poziomu bezpieczeństwa systemu wprowadzanie rozwiązań technicznych zabezpieczających informacje w systemie komputerowym organizacji (ściany ognia, systemy: kon-

troli dostępu, szyfrujące, monitorowania); szkolenie personelu w zakresie zasad bezpiecznego korzystania z systemu oraz przygotowanie odpowiednich dokumentów określających prawa i obowiązki jego użytkowników. Wreszcie na etapie czwartym dostrzec można kontrolę obiegu dokumentów sprawdzanie założeń polityki bezpieczeństwa określonych w dokumentach, ich zastosowania w praktyce i przestrzegania w organizacji.

Zwraca się uwagę, iż zabezpieczenie systemu informatycznego nie kończy się na ustaleniu zasad polityki bezpieczeństwa i wprowadzaniu ich w życie. Jest to proces ciągły, wymagający stałej kontroli oraz weryfikacji ze względu na zmiany stosowanych technologii informatycznych. Do niedawna jeszcze nikt nie zdawał sobie sprawy, iż internet będzie jednym z najważniejszych wynalazków XX wieku [9]. Przepływ informacji stał się o wiele szybszy i tańszy niż dotychczas. Internet oraz komputer, tak jak większość wynalazków technicznych, są po prostu narzędziami [10]. Dotychczasowe doświadczenia wskazują, że narzędzia te będą wykorzystywane również przez przestępców, których ofiarą z racji upowszechnienia tych wynalazków może praktycznie już dzisiaj stać się dosłownie każdy człowiek.

Zagrożenia związane ze stosowaniem nowych technologii wiążą się nie tylko z zagrożeniami przybierającymi postać zachowań ściśle przestępnych, ale również z różnymi patologiami i niebezpieczeństwami w różnych sferach życia społecznego. Jednym z takich obszarów jest edukacja. Zagrożenia występujące na tym polu są tym groźniejsze, iż dotyczą zazwyczaj ludzi młodych, o nieukształtowanej jeszcze osobowości. W rozważaniach dotyczących kwestii wykorzystywania mediów i technologii informatycznej w edukacji zazwyczaj w pierwszym rzędzie akcentuje się pozytywne aspekty zastosowań czy to w edukacji w ogóle, czy w specyficznych dziedzinach kształcenia [11]. Podejście takie jest całkowicie zrozumiałe, jeżeli bierze się pod uwagę rozliczne korzyści, jakie wiążą się z takim postępowaniem. Wśród tych korzyści wymienia się m.in.:

– możliwość indywidualizowania przebiegu uczenia się zachodzącego w toku nauczania, a więc dostosowanie jego tempa i zakresu do możliwości ucznia,
– uzyskiwanie natychmiastowych informacji zwrotnych w toku uczenia się, co ma duże znaczenie dla utrzymywania motywacji do uczenia się,
– wykrywanie na podstawie diagnozy słabych stron ucznia,
– stwarzanie sprzyjających warunków do opanowywania i ćwiczenia różnych umiejętności: od stosunkowo prostych sensoryczno-motorycznych aż do złożonych, obejmujących podejmowanie decyzji i rozwiązywanie problemów przez uczestniczenie w zadaniach symulacyjnych tak

skomplikowanych, jak kierowanie przedsiębiorstwem czy postępowanie w sytuacjach kryzysowych.

Pamiętając o rozlicznych korzyściach wynikających z wykorzystywania technologii informacyjnej w sferze edukacji, nie należy wszakże zapominać o różno rodnych zagrożeniach, jakie mogą towarzyszyć temu procesowi. Ogólnie można powiedzieć, iż autorzy podejmujący problem zagrożeń związanych z powszechnym stosowaniem technologii informatycznej w edukacji reprezentują przynajmniej dwa podejścia. Zwolennicy pierwszego podejścia podejmują problem za grożeń w kontekście ogólnie negatywnego stosunku do zjawiska wkraczania technologii informatycznej, jako przejawu szerszego zjawiska technicyzacji, do tych sfer życia, w których tradycyjnie przywiązywano duże znaczenie do relacji międzyludzkich [12]. Chodzi tutaj o takie dziedziny, jak: medycyna, psychoterapia czy właśnie edukacja.

Źródeł zagrożeń ze strony techniki, w tym technologii informatycznej, upatruje się w tym, iż dehumanizuje ona kontakty międzyludzkie, utrudnia bądź uniemożliwia tworzenie więzi międzyludzkich, a w konsekwencji obniża efektywność profesjonalnych oddziaływań. Współcześnie znacznie częściej stykamy się z podejściem, w którym sygnalizowanie zagrożeń związanych z zastosowaniem technologii informatycznej w edukacji nie wynika z totalnej negacji tejże technologii czy technicyzacji życia w ogóle. Wskazuje się, iż komputer, jak i zresztą wszelkie wytwory techniki wymyślone przez człowieka, są jedynie narzędziami, które mogą być wykorzystywane w sposób przynoszący korzyści bądź też szkody [13].

Zagrożenia psychologiczne i społeczne stanowią istotną, chociaż naturalnie nie jedyną [15], kategorię problemów związanych ze stosowaniem mediów i technologii informatycznej w sferze edukacji. Kwestie te przedstawimy, wskazując konkretne zagrożenia dotyczące funkcjonowania człowieka w sferze poznawczej, emocjonalnej, wolicjonalno-refleksyjnej oraz w dziedzinie relacji interpersonalnych.

Zwraca się uwagę na to, iż korzystanie z identycznych programów komputerowych uniformizuje nawyki percepcyjne, sposoby ujmowania i porządkowania in formacji, a w konsekwencji może prowadzić do psychicznego upodabniania się ludzi. Zjawisko to określa się mianem „kolektywizacji umysłów" [16]. Inne, pokrewne zagrożenie dotyczy sytuacji, w których uczenie się na drodze gromadzenia bezpośrednich doświadczeń z trójwymiarowego świata zostaje zastąpione przez pracę z komputerem. Podaje się w tym kontekście przykład dziecka, które rozpoczyna pracę z programem graficznym. Dzięki realizacji opcji zawartych w tym programie, np. rysowania linii prostych i figur geometrycznych, wypełniania określonych obszarów kolorem, dziecko może wykonać prawidłowe rysunki. Tak naprawdę jednak nie uczy się ono rysować, lecz obsługiwać program komputerowy [14].

Wskazuje się, iż tzw. nauczanie wspomagane komputerowo computer-assisted instruct stanowi jedynie bardzo efektywne zastosowanie prawidłowości, które są podstawą nauczania programowanego. Zadanie komputera sprowadza się do: zadawania pytania, oceny odpowiedzi i ewentualnego odesłania do alternatywnych odpowiedzi, utrwalania wiedzy przez powtarzanie [28]. Współcześnie można zaobserwować próby bardziej złożonego postępowania w postaci tzw. inteligentnego kształcenia wspomaganego komputerem (inteWgent computer-assisted instruction), których istota polega na inspirowaniu uczących się do dialogu z maszyną. Niemniej jednak pozostają wątpliwości, czy maszyna, której działanie opiera się na zaprogramowanych regułach, zdolna jest do postrzegania problemów.

W hipermedialnych strukturach informacyjnych obserwuje się tendencję do po sługiwania się obrazami. Mówi się wręcz o walce pomiędzy kulturą słowa drukowanego a kulturą obrazu. Współczesny uczeń coraz rzadziej czyta książki, natomiast coraz częściej ogląda telewizję, sięga po programy multimedialne czy też poszukuje informacji w internecie. Dominacja wzrokowo-przestrzennych kodów w obsłudze komputerów stanowi efekt zacierania się różnic pomiędzy technologią telewizyjną a komputerową. Zjawisko to sprzyja rozwojowi myślenia konkretno obrazowego, upośledza natomiast myślenie abstrakcyjne [16].

Wielka łatwość umieszczania i dystrybucji informacji w internecie powoduje, że mamy obecnie do czynienia z sytuacją określaną mianem „informacyjnego smogu", analogicznie do zjawiska smogu przemysłowego charakterystycznego dla cywilizacji przemysłowej [17]. Duża liczba tych informacji pochodzi ponadto od osób niekompetentnych, w związku z czym zapoznanie się z owymi informacjami może w większym stopniu utrudnić niż ułatwić zrozumienie jakiegoś przedmiotu.

Wskazuje się również, że nadmiernie częste korzystanie przez ucznia z hiper medialnych struktur informacyjnych może prowadzić do tego, co określa się mianem „elektronicznego encyklopedyzmu", czyli dysponowania przez uczniów ogromem informacji, często nieuporządkowanych i nieprzetworzonych, a najczęściej wręcz zbędnych. Uczniowie stają się kolekcjonerami informacji, natomiast występuje u nich deficyt wiedzy [18]. Warto przypomnieć w tym kontekście słowa angielskiego poety T.S. Eliota, iż wiedza może zatracać się w morzu informacji, a mądrość w potoku wiedzy.

Zwraca się uwagę na jeszcze jedno zagrożenie związane z lawiną informacji przy ograniczonych możliwościach ich przetwarzania przez człowieka, a w konsekwencji na utrudnienie dokonania wyboru. Chodzi mianowicie o problem manipulacji. W sytuacji nadmiaru informacji rzadko możemy pozwolić sobie na przemyślaną analizę wszystkich aspektów danej sytuacji

czy zagadnienia, częściej będziemy zmuszeni polegać na pojedynczych elementach czy aspektach jako wskazówkach. Jak pisze psycholog społeczny R. Cialdini [19]. „Dopóki owe pojedyncze wskazówki są rzetelne [...] nie ma niczego złego. Problem zaczyna się wtedy, kiedy z jakiegoś powodu te normalnie rzetelne wskazówki staną się niegodne zaufania i prowadzić nas będą na manowce błędnych decyzji i szkodliwych działań [...]. Jednym z takich powodów są sztuczki niektórych zawodowych praktyków wpływu społecznego [...]"

W związku z rozpowszechnianiem się technologii informatycznej i stosowaniem komputerów zwiększa się liczba przypadków lęków i niepokoju, jakie budzi praca związana z używaniem komputera czy nawet z samym kontaktem z nim, a także towarzyszących im takich objawów jak bóle głowy, ogólne podrażnienie, koszmary nocne. Mogą również występować reakcje charakterystyczne dla ogólnej reakcji stresowej, takie jak: podwyższony poziom noradrenaliny i adrenaliny we krwi, przyspieszone tętno, wzrost ciśnienia w naczyniach krwionośnych.

Wskazuje się, iż jedną z przyczyn, która warunkuje powstanie komputerofobii, są trudności w opanowaniu obsługi komputera, zwłaszcza wtedy, gdy jest to istotne z uwagi na wykonywaną pracę. Zwraca się uwagę, że niepokój odczuwany w kontakcie z komputerem może mieć podłoże „w ciągłym współzawodnictwie we współczesnym świecie, gdzie umiejętność obsługi komputera i kompetencja w tym zakresie jest niezbędna do odniesienia sukcesu" [20].

Zjawisko komputerofobii występuje w szczególnym nasileniu w kształceniu osób dorosłych w związku z tym, iż wraz z wiekiem zmniejsza się plastyczność umysłu, możliwość uczenia się, a więc coraz trudniej zmienić można przyzwyczajenia i adaptację do nowych warunków. Nie chodzi przy tym jedynie o sam fakt przystosowania się do korzystania z komputera, ale również o przystosowanie się do zmian wynikających z ciągłego postępu technicznego, do instalowania coraz to nowych programów i urządzeń. W badaniach obejmujących grupę ponad tysiąca nauczycieli stwierdzono, że problem komputerofobii występuje również wśród nauczycieli czynnych zawodowo. W związku z dużym tempem zachodzących zmian można będzie oczekiwać konieczności praktycznie ciągłego dostosowywania się do nich użytkowników, a także wystąpienia problemów doświadczanych w tym zakresie nie tylko przez kształcących się dorosłych [20].

Współcześnie problem komputerofobii dotyczy jednak nie tylko osób dorosłych. W czasopiśmie naukowym „Educational and Psychological Measurement" regularnie pojawiają się doniesienia z prac psychometrów poświęconych konstruowaniu specjalnych testów do pomiaru lęku przed komputerem (computer anxiety scale) [21]. Fakt ten, poza samymi donie-

sieniami naukowymi o występowaniu omawianego fenomenu w populacji uczniów różnych typów i poziomów szkół, zdaje się świadczyć o tym, iż zagrożenie, jakie wywołuje kontakt z komputerem i posługiwanie się nim, nie jest zjawiskiem incydentalnym.

Obecnie internet zapewnia szybki dostęp do wszelkiego rodzaju informacji także niedostępnych w inny sposób. Pozwala również szybko porozumiewać się z innymi osobami, znajdującymi się w miejscach bardzo odległych. W związku z tym systematycznie wzrasta liczba osób spędzających przed komputerem bardzo dużo czasu, nierzadko zaniedbujących wskutek tego inne obowiązki, również naukę. Mówi się więc coraz powszechniej o zaburzeniu określanym różnymi nazwami: uzależnienie od internetu, siecioholizm, cyberzależność, infoholizm itp. [22]. Według badań Center for On-line Addiction przeprowadzonych na grupie 17 tys. internautów 6% spośród nich przejawia zachowania kwalifikujące się do leczenia, a 30% korzysta z internetu „aby uciec od złych myśli", co stanowi prostą drogę do uzależnienia.

Do najczęściej opisywanych skutków uzależnienia od internetu należą:

- zaniedbywanie nauki lub pracy,
- utrwalenie postawy egocentrycznej,
- zaburzenia w sferze własnej tożsamości,
- zawężenie zainteresowań,
- zubożenie języka (posługiwanie się slangiem, skrótami itp.).

Niektórzy badacze wskazują, iż zachowania polegające na nadużywaniu korzy stania z internetu nie tyle wynikają z, „uzależniających" właściwości samego medium, ile stanowią konsekwencję pewnych trudności przeżywanych przez jednostkę czy też wyraz określonych nieprawidłowości osobowościowych [23]. Zatem uzależnienie od internetu mogłoby stanowić ucieczkę od problemów czy też poczucia samotności bądź też wiązać się ze skłonnością do zachowań kompulsywnych, stanowić formę przejawiania się tzw. „nałogowej osobowości" współczesnych czasów [24].

W badaniach przeprowadzonych przez R. Krauta i jego współpracowników uzyskano dane empiryczne świadczące o występowaniu wśród osób często korzystających z internetu lekkich stanów depresyjnych, w postaci tzw. obniżonego samopoczucia [9]. Osoby te częściej niż inni użytkownicy deklarowały doświadczanie takich emocji, jak: smutek, przygnębienie, poczucie winy. Pomimo uzyskanych wyników fakt powstawania depresji (Stanów depresyjnych) u użytkowników internetu wywołuje pewne kontrowersje [25].

W perspektywie bardziej ogólnej zwraca się uwagę, iż upowszechnianie elektronicznych środków przetwarzania informacji powoduje przejmowanie

pewnych funkcji poznawczych oraz kontrolnych przez maszynę [16]. Aktywność człowieka może zostać uzależniona od maszyn i sieci informatycznych, a zjawisko to może dotyczyć zarówno jednostek, jak I całych grup społecznych. W przypadkach skrajnych może dojść do sterowania człowiekiem, w tym także uczącym się, przez ma szynę. W skali globalnej takie tendencje wiązałyby się ze zmniejszaniem autonomii i niezależności poznawczej, wykształcaniem się swoistej bierności poznawczej, a w konsekwencji obniżaniem się kreatywności człowieka.

Zwraca się uwagę, iż w komunikacji zachodzącej za pośrednictwem internetu informacje o własnej tożsamości są niedostępne dla partnerów interakcji, co umożliwia manipulowanie swoją tożsamością. „W cyberprzestrzeni każdy może mieć tyle «elektronicznych osobowości ile zdoła wykreować" [23]. Manipulacja własną tożsamością może mieć charakter gry prowadzonej z innymi uczestnikami komunikacji. W trakcie tej gry jednostka może nie tylko ukrywać pewne informacje przed innymi, ale może także je rozmyślnie fałszować. Takie postępowanie może mieć charakter zabawy, niemniej jednak może kształtować i utrwalać pewne nieprawidłowe sposoby funkcjonowania społecznego oparte na kłamstwie i manipulacji. W przypadku jednostek charakteryzujących się specyficznym typem osobowości, tzw. osobowością z pogranicza (borderline), dla której zaburzenia tożsamości są cechą osiową, udział w tego typu grach może mieć zdecydowanie negatywne konsekwencje.

Jedną z konsekwencji upowszechniania się zastosowania mediów i techniki informatycznej w edukacji będzie, być może nie gwałtowne i całkowite, ale Stopniowe i częściowe zastępowanie bezpośrednich kontaktów ucznia z nauczycielem kontaktami pośrednimi czy też wręcz zastąpienie nauczyciela przez maszynę. Trudno jest przewidzieć konsekwencje takiego procesu, gdyby miał on rzeczywiście nastąpić. Dotyczy to zwłaszcza zastąpienia nauczyciela (czy też bezpośredniego kontaktu z nauczycielem) w takich oddziaływaniach, jak: wzbudzanie motywacji poznawczej do uczenia się, prezentowanie wzorca zachowań, stymulowanie do dyskusji, dialogu. Współcześnie dyskusja z komputerem to najczęściej wymiana rozkazów i oczekiwań; maszyna nie odbiera wrażeń ani nie odczuwa emocji, nie jest podmiotem rozumienia ani też nie jest zdolna do osiągania wglądu.

Zaobserwowano, iż u osób często korzystających z internetu dochodzi nie tylko do zmian wcześniej opisanych, ale również do zaburzenia relacji interpersonalnych, utraty zainteresowania różnymi formami aktywności społecznej itp. [26]. U osób tych stwierdza się również zwiększony poziom poczucia osamotnienia. Co ważne, zmiany te zaobserwowano nawet wówczas, gdy dominujące wykorzystanie internetu miało charakter społeczny, a więc np. dotyczyło elektronicznej komunikacji z członkami rodziny, znajomymi

czy osobami nieznanymi. Niektórzy autorzy formułują nawet wniosek, iż internet zaczyna zastępować bliskie relacje interpersonalne, a czyniąc to w sposób powierzchowny, wywołuje w konsekwencji poczucie osamotnienia, które może potęgować Stany depresyjne, co już wcześniej sygnalizowaliśmy.

Zwraca się uwagę, iż internet dzięki swoim interakcyjnym właściwościom może stać Się atrakcyjnym partnerem, zastępującym rzeczywiste kontakty społeczne. Wskazuje się, iż zwiększa się liczebnie nowa kategoria ludzi zwanych „elektronicznymi odludkami", którzy potrafią perfekcyjnie posługiwać się Sprzętem komputerowym, ale są w znacznym stopniu pozbawieni podstawowych umiejętności społecznych dotyczących nawiązywania i utrzymywania bliskich relacji interpersonalnych [13].

Anonimowość oraz wzrastająca wolność od norm społecznych, którą zapewnia komunikacja za pośrednictwem sieci komputerowych, może wyzwalać zachowania agresywne, skłaniać do otwartego manifestowania czy też wręcz propagowania po staw społecznie szkodliwych takich jak rasizm. Wiadomo, iż anonimowość osób kontaktujących się za pośrednictwem sieci ogranicza możliwość kar i sankcji społecznych za niewłaściwe zachowanie. Psychologowie zwracają uwagę, że u niektórych ludzi w trakcie tego rodzaju komunikacji może dojść do osłabienia mechanizmów kontroli wewnętrznej, które nie wystąpiło by w bezpośredniej, nie anonimowej interakcji [27].

Ryzyko związane z zagrożeniami, jakie zostały przedstawione w odniesieniu do różnych sfer funkcjonowania podmiotu, może zmieniać się w zależności od występowania pewnych dodatkowych czynników (warunków). Ogólnie można wyróżnić dwie kategorie takich czynników: (1) czynniki podmiotowe oraz (2) czynniki sytuacyjne.

W grupie czynników podmiotowych możemy wyróżnić kategorię czynników rozwojowych oraz czynników indywidualnych. Czynniki rozwojowe (czyli wieki związany z nim poziom rozwoju umysłowego, emocjonalnego i społecznego) mogą w istotny sposób determinować ryzyko związane z określonymi zagrożeniami. I tak, jeżeli chodzi o problemy dotyczące np. trudności występujących w związku z zalewem informacji i koniecznością dokonywania selekcji materiału czy też uzależnienia od internetu, to większe ryzyko występuje w przypadku osób młodszych. W przypadku natomiast np. komputerofobii większy poziom ryzyka charakteryzuje osoby dorosłe.

W odniesieniu do czynników indywidualnych jako podkategorii uwarunkowań podmiotowych największe znaczenie należałoby przypisywać występowaniu pewnych specyficznych właściwości osobowości osób uczących się. Chodzi mianowicie o to, iż pewne specyficzne cechy osobowości czy też charakteryzowanie się pewnym typem osobowości może sprzyjać rozwinięciu się określonych zagrożeń. Na przykład skłonność do zachowań kom-

pulsywnych może sprzyjać uzależnieniu od internetu, a tzw. osobowość histrioniczna podleganiu wpływom o charakterze manipulacyjnym, osobowość pograniczna (borderline) zaburzeniom tożsamości.

Z uwagi jednak na relatywnie krótki okres wykorzystywania technologii komputerowej nie mamy dostatecznych danych umożliwiających nam ocenę jej efektywności, czyli dokonania rachunku strat i korzyści. Historia uczy nas ponadto, iż to, co okazywało się korzystne w skali lat, niekoniecznie było oceniane jako wartościowe w skali dziesięcioleci. Brak jest jednak reguł i zasad, które mogłyby stano wić oparcie dla decydentów; istnieją tylko bardzo ogólne wskazówki, jak ta, która nakazuje zachowanie ostrożności. Stosowanie technologii komputerowej na skalę masowej powinno przypominać zachowanie lekarza, który, wprowadzając nowe lekarstwo do terapii, musi uważnie śledzić wszelkie działania uboczne.

Psychologiczne zagrożenia związane z zastosowaniem mediów i technologii informatycznej w edukacji mogą wiązać się z niebezpieczeństwem bezpośredniego zakłócenia oddziaływań społecznych, jak również mogą wpływać na efektywność tych oddziaływań w sposób pośredni, np. poprzez wpływanie na stan emocjonalny osób kształcących się. Psychologiczne zagrożenia związane z zastosowaniem mediów i technologii informatycznej w edukacji należy rozpatrywać w kontekście korzyści i zalet, jakie niesie ich wykorzystywanie. Należy przyjąć, iż generalnie technologia zwiększa możliwości człowieka, natomiast zastosowaniu technologii powinno towarzyszyć przewidywanie możliwych zagrożeń i przeciwdziałanie im [10]. Wydaje się, iż nie należy również bagatelizować tych zagrożeń, które mają ograniczony zasięg z tej racji, iż dotyczą jedynie pewnych charakterystycznych grup, np. osób o specyficznych cechach osobowości.

Literatura

[1] M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, Prokuratura i Prawo 202, nr 4, s. 62–79.
[2] J. Arquilla, D.F. Ronfeldt, *The Adwent of Netwar, Santa Monica*, Calif., 1996.
[3] B. Hołyst, *Terroryzm*, t. 1, Warszawa 2009, s. 754.
[4] M. Białkowski, *Haking – przestępczość nowych czasów*, Przegląd Policyjny, 2002, nr 12, s. 138–148.
[5] Information Warfare, Thunders Mouth Press, New York 1996.
[6] M. Byczkowski, *Bezpieczeństwo systemów sieciowych*, Postępy Kryminalistyki, 1997, nr 1, s. 62–73.

[7] K. Buchała, A Zoll, *Kodeks karny. Komentarz. Część ogólna*, t. 1, Warszawa 1998.
[8] J. Barta, R. Markiewicz, *Internet a prawo*, Warszawa 1998.
[9] R. Kraut, M. Patterson, V. Lundmark, S. Kiesler, *Internet paradox: A social technology that reduces social involvment and psychological well-being*, American Psychologist, 1998, nr 53, s. 1017–1031.
[10] P. Wallace, *Psychologia Internetu*, Poznań 2001.
[11] S. Juszczyk, *Nowoczesne media dydaktyczne w edukacji lingwistycznej*, Kognitywistyka i Media Edukacji, 1993, s. 107–109.
[12] D. Sloan, *Introduction: On raising critical questions about the computer in education*, w: D. Sloan (red.), The Computer in Education. A critical Perspective, New York 1985.
[13] J. Morbitzer, *Technologia informacyjna – kodeks zagrożeniowym*, w: J. Migdałek, B. Kędzierska (red.), Informatyczne przygotowanie nauczycieli w okresie zmian i transformacji, Kraków 2002.
[14] J. Morbitzer, *Technologia informacyjna*, Warszawa 1998.
[15] M. Tanaś, *Medyczne skutki uboczne kształcenia wspomaganego komputerem*, Toruńskie Studia Dydaktyczne, 1993, s. 107–109.
[16] J. Bobryk, *Technika elektroniczna, komunikacja masowa a procesy psychiczne*, w: I. Kurcz, J. Bobryk (red.), Psychologiczne studia nad językiem i dyskursem, Warszawa 2001.
[17] D. Shenk, *Data Smog. Surviving for Information Glut*, San Francisco 1998.
[18] R. Pachociński, *Czy szkoła przygotowuje do zmian?*, Społeczeństwo Otwarte, 1997, nr 4 s. 35–39.
[19] R. Cialdini, *Wywieranie wpływu na ludzi*, Gdańsk 1994, s. 248.
[20] B. Siemieniecki, *Edukacja humanistyczna i komputery*, w: J. Gajda, S. Juszczyk, B. Siemieniecki, K. Wenta, Edukacja medialna, Toruń 2002, s. 183.
[21] G.A. Marcoulides, *Measuring computer anxiety: the Computer Anxiety Scale*, Educational and Psychological Measurement, 1989, nr 49, s 733–740; G.A. Marcoulides, B.T. Mayes, R.L. Wiseman, Measuring computer anxiety in the work environment, Educational and Psychological Measurement, 1995, nr 55, s. 604–810.
[22] A. Jakubik, *Zespół uzależnienia od internetu*, Studia Psychologica, 2002, nr 3, s. 133–142.
[23] K. Majgier, *Internet jako przestrzeń komunikacyjna*, Przegląd psychologiczny, 2000, nr 43, s. 157–172.
[24] J. Mellibruda, *Nałogowa osobowość naszych czasów*, Nowiny Psychologiczne, 1996, nr 2, s. 5–14.

[25] J.S Shapiro, *Loneliness: Paradox or artifact?*, American Psychologist, 1999, nr 54, s. 782–783.
[26] K.S Young, *Caught in the Net: How to Recognize the Signs of Internet Addiction and Winning Strategy for Recovery*, New York 1994.
[27] E. Reid, *Communication and communities Internet Relay Chat: Construciting communities*, w: P. Ludlow (red.), Conceptual Issues on the Electronic Frontier, Melbourne 1996.
[28] M.H. Dembo, *Stosowana psychologia wychowawcza*, Warszawa 1998.

VICTIMOLOGICAL ASPECTS OF CYBECRIME

Abstract. We analyze the phenomena associated with the development of the Internet with particular emphasis on cybercrime and cyberterrorism. Were also discussed psychological and victimological aspects of crime in cyberspace. An analysis of threats and risks with regard to subjective and situational factors is presented.

Keywords: cybercrime, victimology, cyberspace, malware, network attacks, information technology, the victim of cybercrime, psychological aspects of cybercrime, education network, internet and interpersonal relationships, virtual identity