Aleksandra Łysik
III rok, Niestacjonarne Studia Doktoranckie WE UG

Patologie w cyberprzestrzeni. Psychologia sprawców przestępstw internetowych

Wstęp

Zgodnie z raportem Internet World Stats, liczba osób korzystających z Internetu w czerwcu 2012 r. wyniosła ponad 2,4 mld[1], co oznacza, iż z sieci korzysta ponad 30% mieszkańców ziemi. Jedną z najważniejszych cech Internetu jest więc zarówno jego ogólnoświatowy zasięg i powszechna dostępność, jak i brak zcentralizowanej kontroli. Sytuacja ta spowodowała, że wraz z rozwojem globalnej sieci coraz częściej zaczęło dochodzić do różnego rodzaju nadużyć o charakterze kryminogennym. Powołując się na statystyki Internet Crime Complaint Center (IC3), amerykańskiej instytucji zajmującej się śledzeniem nadużyć w cyberprzestrzeni, w 2011 r. odnotowano ponad 300 tys. zgłoszeń o popełnieniu przestępstwa z wykorzystaniem Internetu, co daje ponad 800 zgłoszeń takich incydentów dziennie. Oznacza to też, iż skala zjawiska przestępczości internetowej wzrosła w 2011 r. o 3,4% w stosunku do roku poprzedniego[2], a co za tym idzie, radykalnie wzrosła też liczba osób łamiących prawo w sieci. Z uwagi na fakt, jak ogromne straty ekonomiczne generują przestępstwa popełniane za pomocą Internetu – zgodnie z opublikowanym w 2014 r. raportem CSIS w skali globalnej sięgają one 415 mld USD rocznie[3], warto przyjrzeć się bliżej temu zjawisku z perspektywy psychologii sprawców.

1. Internet jako środowisko działalności kryminogenne

Przestępczość związana z systemami elektronicznego przetwarzania danych zaczęła rozwijać się w latach 40. XX w. Z uwagi na fakt, iż pierwsze komputery były zarówno duże i kosztowne, jak i nie miały żadnego połączenia z innymi urządzeniami, przez długi czas ich zawartość była w pełni chroniona. Kiedy jed-

[1] Internet World Stats, www.internetworldstats.com {dostęp: 1.01.2014].
[2] Raport Internet Crime Complaint Center IC3, www.ic3.gov {dostęp: 1.01.2014].
[3] *Cyber Crime Causes $445 Billion Loss Annually in Global Economy*, Business2Community, www.business2community.com {dostęp: 1.01.2014].

nak w 1959 r. do użytku wszedł PDP-1, pierwszy komputer, w którym zastosowany został komercyjny podział czasu, a urządzenie to zaczęło być wynajmowane różnym instytucjom, sytuacja ta uległa zmianie. Jako, iż wiele niezależnych osób i przedsiębiorstw korzystało z tej samej maszyny, dane zapisywane w jej pamięci zostały narażone na poważne niebezpieczeństwo. Tym samym zostały otwarte pierwsze drzwi do działań hackerskich, których skala dodatkowo zaczęła przybierać na sile wraz upowszechnieniem rozległej sieci komputerowej.

Zgodnie z raportem CSIS (Centre for Strategic and International Studies), w 2013 r. zjawisko włamania i kradzieży z wykorzystaniem Internetu dotknęło 800 mln ludzi na całym świecie, powodując 150 mld USD strat. Problem ten w szczególności dotyczy Amerykanów (ok. 40 mln obywateli), a także Turków (54 mln), Niemców (16 mln) i obywateli Chin (20 mln)[4]. Cyberprzestępczość ma wpływ na handel międzynarodowy, konkurencyjność innowacji, a także globalny wzrost gospodarczy. Niesie też poważne konsekwencje dla zatrudnienia. Jak zauważa Jim Lewis, ekspert CSIS, w Europie aż 150 tys. osób, a w Stanach Zjednoczonych 200 tys. straciło pracę z powodu strat finansowych spowodowanych przestępczością w Internecie. W Wielkiej Brytanii, cyberprzestępczość odpowiedzialna jest za straty w handlu detalicznym wysokości ponad 850 mln USD, a jej całkowity koszt dla brytyjskiej gospodarki sięgnął 0,47% PKB[5].

1.1. Pojęcie i istota przestępstwa komputerowego

Celem zdefiniowania zjawiska przestępczości w Internecie, konieczne jest uprzednie przybliżenie problematyki przestępczości internetowej, jako jednego z rodzajów przestępczości komputerowej.

Ogólną nazwą „przestępstw komputerowych" określany jest się zbiór przestępstw, które charakteryzuje występowanie komputerów oraz informacji w formie cyfrowej. W szerokim rozumieniu przestępczość komputerowa obejmuje tym samym „wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych"[6]. Przestępczość komputerową można więc zdefiniować jako wszelkiego rodzaju naruszenie bezpieczeństwa danych i systemów komputerowych, które skierowane jest przeciwko ich integralności, poufności i dostępności.

Niemniej powyższa definicja nie stanowi normatywnego określenia omawianego zjawiska. Należy bowiem podkreślić, iż z uwagi na nieustanny rozwój infrastruktury informatycznej i nowych technologii, pojęcie przestępczości kompu-

---

[4] *Ibidem*.

[5] *Cyber Crime Causes $445 Billion Loss Annually in Global Economy*, Business2Community, www.business2community.com [dostęp: 01.01.2014].

[6] K.J. Jakubki, *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" 1996, nr 12, s. 34.

terowej często definiowane jest *ad hoc* i używane w znaczeniu operacyjnym[7]. Co więcej, nazwą „przestępstw komputerowych" objęte zostały dwa rodzaje działań: zarówno te, w których komputer jest celem ataku, jak i te, w których komputer wykorzystywany jest wyłącznie jako narzędzie.

Do pierwszej z grup należą czyny wymierzone w funkcjonowanie systemów operacyjnych oraz oprogramowania. W przypadku ich zaistnienia, system komputerowy staje się przedmiotem ataku, a popełnienie tego czynu nie byłoby możliwe poza środowiskiem cyberprzestrzeni. Do drugiej grupy należą czyny polegające na posługiwaniu się elektronicznymi systemami przetwarzania danych, w przypadku których komputer jest wyłącznie narzędziem, instrumentem w rękach sprawcy.

Na podstawie powyżej charakterystyki przestępstw komputerowych można podjąć próbę zdefiniowania przestępstwa internetowego, jako każdego rodzaju czynu zabronionego, do popełnienia którego wykorzystano sieć Internet lub w przypadku którego usługi sieciowe, bądź też usługi oferowane przez człowieka za pośrednictwem sieci, umożliwiły jego realizację.

1.2. Klasyfikacja przestępstw internetowych

Przestępstwa internetowe, podobnie jak przestępstwa komputerowe, można podzielić na dwie kategorie w zależności od roli, jaką sieć/komputer odegrała w realizacji czynu zabronionego.

Przestępstwa internetowe *sensu stricte,* czyli w ujęciu ścisłym, związane są bezpośrednio z usługami oferowanymi przez Internet, takimi jak możliwość publikowania stron WWW oraz przesyłania danych. W takim rozumieniu, przestępstwo stanowi więc każda odmiana czynu zabronionego, którego główne czynności zostały dokonane za pośrednictwem sieci, a do zaistnienia których mogło dojść wyłącznie dzięki specyficznym możliwościom technicznym przez nią oferowanych. O ile więc przestępstwo rozpowszechniania treści nazistowski popełnić można w telewizji, radiu, czy prasie, o tyle posłużenie się do tego celu witryną WWW nadaje internetowy charakter temu czynowi, utrzymując jednocześnie zastosowanie tego samego artykułu Kodeksu Karnego. Analogiczna sytuacja dotyczy transferu danych za pośrednictwem sieci, którego wykorzystanie umożliwia popełnienie internetowej odmiany przestępstw określonych w ustawie o ochronie praw autorskich i prawach pokrewnych.

Przestępstwa internetowe *sensu largo*, tj. w ujęciu szerokim, stanowią natomiast wszelkie odmiany czynów zabronionych, których popełnienie stało się możliwe dzięki usługom oferowanym przez człowieka za pośrednictwem Inter-

[7] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno- kryminalistyczne*, Kantor Wydawniczy Zakamycze, Kraków, 2000, s. 14.

netu. Tak więc jak w przypadku przestępstw internetowych *sensu stricte* główna czynność wykonawcza, jak np. opublikowanie na stronie WWW nielegalnych treści, występuje i ogranicza się wyłącznie do zasobów sieci, o tyle w przypadku przestępstw internetowych *sensu largo* czynność podejmowana za pomocą Internetu jest jedynie środkiem dodatkowym, prowadzącym do celu, który zostanie zrealizowany poza nią. Jednym z przykładów takiej działalności może być płatność w sklepie internetowym, dokonywana przy użyciu skradzionej karty kredytowej – choć transfer danych koniecznych dla finalizacji transakcji, jak numer karty czy dane osobowe jej właściciela, następuje za pośrednictwem sieci, to cel, jakim jest przysporzenie majątkowe, realizowany jest poza siecią i nie jest z nią już bezpośrednio związany[8].

2. Postać cyberprzestępcy

Celem pracy wielu naukowców jest lepsze zrozumienie przestępców, ich motywów i sposobów postępowania. Psychologia kryminalna jest dziedziną nauki, która opiera się na studiowaniu umysłu przestępcy oraz dociekaniu, co skłania go do działania niezgodnego z prawem, będącego odstępstwem od przyjętych norm społecznych. Jednym z głównym zadań psychologów kryminalnych jest tym samym tworzenie sylwetek przestępców, czyli charakterystyk ich osobowości, które opracowywane są na podstawie informacji zebranych na miejscu dokonania przestępstwa. Profil sprawcy jest więc jego psychologiczną oceną, choć dokonaną na wyrost, bowiem przed ustaleniem jego tożsamości. Niemniej, składa się on z zestawu określonych cech, które prawdopodobnie są wspólne dla osób popełniających określony rodzaj przestępstw.

2.1. Kategorie przestępców internetowych

Przestępstwa internetowe można podzielić na dwie kategorie: przestępstwa *sensu stricte,* czyli te, których dokonanie nie byłoby możliwe poza siecią oraz *sensu largo,* do których dokonania Internet posłużył jedynie jako dodatkowe narzędzie. Powyższą klasyfikację można analogicznie odnieść do przeprowadzenia podziału przestępców działających w Internecie.

Do pierwszej z omawianych grup należą ci przestępcy, dla których sieć jest głównym „aparatem" służącym do popełniania czynów zabronionych. Najczęściej spotykani z nich to nieuczciwi pracownicy oraz tzw. przestępcy „w białych kołnierzykach", którzy dokonują przestępstw urzędniczych, a także oszuści komputerowi. Dzięki globalnemu zasięgowi Internetu i oferowanym przez niego

[8] M. Sowa, *Ogólna charakterystyka przestępczości internetowej*, „Palestra" 2001, nr 5–6, s. 25.

usługom, takim jak poczta elektroniczna, czy czaty, naciągacze są w stanie dotrzeć do nieograniczonej liczby potencjalnych ofiar. Najczęściej dokonywane przez nich przestępstwa to wyłudzenia, oszustwa dotyczące kart kredytowych i aukcji internetowych, wszelkiego rodzaju piramidy finansowe i rzekome okazje inwestycyjne.

Internet jest także głównym środowiskiem działania wszystkich hackerów, włamywaczy sieciowych i wandali. W społeczności hackerskiej istnieje jednak podział na dwie grupy tego typu przestępców; „czarne kapelusze" i „białe kapelusze". „Czarne kapelusze" to hakerzy, którzy włamują się do systemów komputerowych w celu osiągnięcia korzyści majątkowej lub rozgłosu, natomiast „białe kapelusze", to zaś hackerzy, którzy wyszukują luki w oprogramowaniu, mając w zamyśle zwiększenie bezpieczeństwa systemów komputerowych[9].

Drugą grupę przestępców w cyberprzestrzeni stanowią ci, którzy z Internetu korzystają jedynie marginalnie. Są to przestępcy, którzy wykorzystują sieć do wyszukiwania kolejnych ofiar, jak np. seryjni gwałciciele czy pedofile. Są to również przestępcy, którym komputery i sieć służą do gromadzenia i przechowywania danych z prowadzonej działalności przestępczej, nielegalnego hazardu bądź też handlu narkotykami. Wykorzystując możliwości Internetu, mogą oni przesyłać informacje z jednego w miejsca w drugie, chroniąc je tym samym przed groźbą dostania się w ręce przedstawicieli prawa. Ostatni z nich, to przestępcy pracujący w grupach, jak np. terroryści, którzy wykorzystują usługi internetowe, takie jak poczta elektroniczna czy pokoje czatowe, do komunikowania się ze swoimi wspólnikami. Choć korespondowanie samo w sobie nie jest przestępstwem, to przestępstwo to stanowi planowanie i przygotowywanie nielegalnej działalności.

2.2. Motywy przestępczego działania

W wielu jurysdykcjach ważnym elementem udowodnienia przestępstwa jest wskazanie istnienia tzw. przestępczego trójkąta, czyli środków (sposobu popełnienia przestępstwa), możliwości (tj. znajdowania się w odpowiednim miejscu w odpowiednim czasie) i motywu (przyczyny, dla których zostało ono popełnione). Co więcej, zrozumienie powodu popełnienia czynu jest ważne również w dwóch punktach prowadzenia śledztwa: najpierw gdy tworzy się profil psychologiczny podejrzanego, a następnie gdy dochodzi do przedstawienia sprawy przed sądem[10].

Jednym z najpowszechniejszych motywów popełniania przestępstw w Internecie jest chęć zabawy. Do grupy przestępców kierujących się tym motywem należą głównie młodzi hakerzy, tzw. „pionierzy", którzy chcą sprawdzić swoje

[9] D.L. Shinder, *Cybeprzestępczość, Jak walczyć z łamaniem prawa w sieci,* Helion, Gliwice 2001, s. 134.
[10] *Ibidem*, s. 122.

umiejętności i włamując się do sieci, zdobyć nowe doświadczenia. Podobne motywy kierują tzw. „graczami", dla których szczytem ambicji jest pokonanie administratorów systemów, czemu towarzyszy poczucie wygranej potyczki. Działania ich są na ogół mało szkodliwe i nie towarzyszą im złe intencje.

Źródłem wielu przestępstw w sieci jest również ludzka słabość do pieniędzy i chęć zysku. „Hackerstwo dla dolarów" mieści w sobie wiele innych grup przestępstw, takich jak oszustwa, defraudacje, czy szpiegostwo firmowe. Przestępcy popełniający powyższe czyny to najczęściej osoby wykształcone, lecz którym nie powiodło się w życiu tak, jak tego oczekiwały i których kariera zawodowa uległa zatrzymaniu. Często przepełnieni są oni złością, gniewem i nienawiścią, a jednym z powodów ich działalności jest chęć zemsty za – ich zdaniem – dokonane krzywdy.

Kolejny źródłem działalności przestępczej w sieci są motywy polityczne, które przyświecają działalności ekstremistów i organizacji terrorystycznych. Współcześnie media elektroniczne stały się nie tylko nośnikiem dla przekazu ideologicznego ugrupowań terrorystycznych, ale także formą ich *modus operandi*. Odkąd terroryści zauważyli, jak skutecznym narzędziem do rozpowszechniania informacji jest Internet, Al Kaida, Hezbollah czy Hamas uczyniły z niego swój główny kanał propagandowy. Tym samym dziś, organizacje te nie wysyłają też już swoich żądań do władz za pomocą listów ani też nie informują dziennikarzy telefonicznie, że są odpowiedzialne za przeprowadzenie zamachu – mają one własne serwisy informacyjne, fora i telewizje internetowe.

W końcu, jednym z motywów działalności przestępczej w Internecie, są zaburzenia na tle seksualnym. Do tej grupy sprawców możemy zaliczyć pasywnych i aktywnych pedofilii, seryjnych gwałcicieli oraz seryjnych morderców seksualnych. Niemniej, należy podkreślić, iż w ich przypadku Internet nie jest bezpośrednim narzędziem, służącym do popełnienia przestępstwa, lecz dodatkowym, ułatwiającym dotarcie do potencjalnej ofiary.

2.3. Sylwetka przestępcy internetowego

Filmy, takie jak „Gry wojenne" czy „Hakerzy", ukazują hollywoodzką wizję cyberprzestępców, uproszczoną i uromantycznioną. Hakerzy są niezrozumianymi geniuszami o złotych sercach, usiłującymi ocalić świat przed wpływem potężnego i złego rządu. Co więcej, każdego, kto wierzy w wolność dystrybucji wolnego oprogramowania przedstawiają jako niebezpiecznego pirata, zdecydowanego walczyć na śmierć i życie o fundamenty społeczeństwa kapitalistycznego.

Również dziś, w powszechnym mniemaniu utarł się stereotyp dotyczący osobowości przestępców działających w sieci. Do najpowszechniejszych z nich należy za pewne przekonanie, iż wszyscy oni mają nadzwyczajnie wysoki iloraz inteligencji i szeroką wiedzę techniczno – komputerową, że są błyskotliwi i po-

mysłowi, lecz nieprzystosowani do życia w społeczeństwie. Ponadto, wszyscy z nich to młodzi mężczyźni, a czasem nawet nastoletni chłopcy, których przestępczym działaniom, z uwagi na „nierzeczywistość świata", w którym się poruszają, nigdy nie towarzyszy brutalność ani przemoc.

Pierwszym krokiem przy budowaniu sylwetki przestępcy internetowego jest na pewno jednak zastanowienie się nad kilkoma cechami, które zazwyczaj dotyczą wszystkich cyberprzestępców, ze szczególnym uwzględnieniem hackerów – należy tylko pamiętać, by wystąpienie tych cech uważać wyłącznie za zjawisko prawdopodobne, a nie bezsporne i oczywiste, bowiem w każdym przypadku mogą nastąpić wyjątki. S. Gold, autor historycznego już poradnika *The Hacker's Handbook,* sugeruje, że osobowość osób naruszających prawo w Internecie jest bardzo skomplikowana. Zwykle jest to człowiek o przeciętnej inteligencji, któremu praca zawodowa nie daje satysfakcji, ani nie zaspokaja jego ambicji, przez co zaczyna on poszukiwać nowych wyzwań. Jak twierdzą zaś amerykańscy socjologowie, wspólną cechą większości włamywaczy internetowych jest dodatkowo brak akceptacji społecznej i silne osamotnienie. Co więcej, osoby te są często nieśmiałe i pełne kompleksów, mają wiele wewnętrznych obaw i duże trudności sprawia im radzenie sobie ze zwykłymi stosunkami międzyludzkimi. Towarzystwo rodziny bądź rówieśników wolą zastąpić ekranem monitora[11]. W rezultacie, zgodnie z teorią społecznego uczenia się, stają się szczególnie podatni na wszelkiego rodzaju negatywne i kryminogenne wpływy, na które natknąwszy się w sieci, zaczynają naśladować[12].

Do najczęściej wymienianych cech przestępców internetowych należy przede wszystkim jednak sprawność techniczna. Typowy przestępca nie jest osobą, która właśnie pierwszy raz zalogowała się w Internecie. Musi on posiadać wiedzę na temat poruszania się w sieci, oferowanych przez nią możliwości i rozwiązań, co wcale jednak nie oznacza, że musi być geniuszem komputerowym. Wzorcowy przestępca charakteryzuje się również lekceważeniem prawa; często jest również przekonany, że stoi ponad nim lub poza jego zasięgiem, a łamiąc przepisy, usprawiedliwia swoje działanie twierdząc, że prawo jest złe bądź nieobiektywne. Co więcej, posiada on aktywną wyobraźnię, a dzięki dostępowi do Internetu, swobodnie realizuje swoje fantazje. Zjawisko to może dotyczyć tak przestępców działających na tle seksualnym, którzy korzystają z dziecięcej pornografii, jaki oszustów, którzy chcąc ukryć swoją prawdziwą tożsamość, budują skomplikowane gry oraz schematy, celem „omamienia" swojej ofiary. Przestępców internetowych cechuje również chęć podporządkowania sobie innych i skłonność do podejmowania ryzyka.

---

[11] D. Doroziński, *Hakerzy. Technoanarchiści cyberprzestrzeni,* Helion, Gliwice 2001, s. 25.

[12] P. Rice, *The Adolescent: Development, Relationships, and Culture,* Allyn and Bacon, Boston1999, s. 43.

2.4. Profil psychologiczny hackera

W roku 2003 grupa naukowców z *University of Georgia* w USA opublikowała wyniki badań, których celem było stworzenie profilu psychologicznego internetowego włamywacza. Naukowcy chcieli m. in. uzyskać odpowiedź na pytania, w jaki sposób osobowość hackerów wpływa na ich zachowania przestępcze w sieci, jakie pobudki skłaniają ich do prowadzania nielegalnych działań w Internecie, a także jak sami reagują w sytuacji, gdy to ich prywatność i poczucie bezpieczeństwa zostają zagrożone. W badaniu, które polegało na wypełnieniu ankiety on-line, wzięło udział 1385 hackerów z 30 krajów świata.

Z uwagi na fakt, iż anonimowość w środowisku hackerskim jest sprawą oczywistą, grupa badawcza została pozyskana przy współpracy z koreańską firmą *Hackerslab*, twórcą *Free Hacking Zone*, która jako specjalista ds. zabezpieczeń systemów komputerowych, co rok organizuje konkurs dla internetowych włamywaczy na testowanie oprogramowania.

Wyniki przeprowadzonej ankiety pozwoliły wyciągnąć następujące wnioski dla zbudowania modelowej sylwetki hackera:

1. Demografia
   96% ankietowanych hackerów stanowią mężczyźni, spośród których 98% jest w wieku poniżej 35 lat.
2. Religia
   40% badanych nie deklaruje wyznawania żadnej religii, natomiast wśród 60% deklarujących największy odsetek (24%) wskazuje na religię chrześcijańską.
3. Pochodzenie etniczne
   Ponad 60% respondentów określa się mianem Azjatów, 19% definiuje swoje pochodzenie etniczne jako kaukaskie/europejskie.
4. Wykształcenie
   65% ankietowanych określiło swoje wykształcenie jako minimum średnie, z czego ponad 40% deklaruje ukończenie 2- lub 4-letniego college'u.
5. Obiekty hackerskich ataków
   70% badanych hackerów przyznało się do atakowania stron WWW osób prywatnych, blisko 50% strony małych przedsiębiorstw, a 22% witryn bankowych.
6. Poziom narcyzmu a agresja w sieci
   Zgodnie z wynikami badań, hackerzy wykazujący wysoki poziom narcyzmu są bardziej agresywni w swoich przestępczych działaniach w cyberprzestrzeni, niż ci, u których poziom autofilii jest niższy.
7. Ofensywność charakteru a determinacja do działania
   Jak wykazała analiza badań, hackerzy, u których zdiagnozowano wysoki poziom ofensywności charakteru bardziej konsekwentni w swoich przestępczych działaniach w cyberprzestrzeni, niż ci, u których poziom ten jest niższy.

8. Radykalizm a aktywność hackerska
   Powołując się na wyniki ankiety, hackerzy, którzy wykazali skrajne poglądy na podłożu narodowym bądź religijnym, okazali się być bardziej zmotywowani w swoich działaniach przestępczych w sieci[13].

Podsumowanie

Pojawienie się Internetu otworzyło nowe perspektywy dla nauki, biznesu i kultury. Zaczęły rozwijać się elektroniczne dziedziny handlu, jak sklepy internetowe i portale aukcyjne, powstały fora internetowe, czaty, w końcu narodziły się media społecznościowe. Niestety, wraz z rosnącym potencjałem sieci, powstały też nowe rodzaje przestępstw i choć wiele z nich zostało jedynie przeniesionych do Internetu z życia codziennego, jak na przykład wyłudzenia, czy działalność pedofilii, to powstały też nowe, w tym hacking czy podsłuch komputerowy.

W celu skutecznego zwalczania przestępczości w Internecie, koniecznie jest zrozumienie motywów, jakie kierują działalnością przestępców w cyberprzestrzeni. Dzięki analizie ich psychologii, czynników emocjonalno – behawioralnych oraz metod postępowania, możliwe jest zarysowanie ich profilu psychologicznego. Prawidłowo opracowana zaś sylwetka psychologiczna przestępcy ma zaś ma kluczowe znaczenie dla ujęcia sprawcy czy jego potencjalnych naśladowców, jak też może istotnie pomóc w prewencji przyszłych, podobnych działań.

Bibliografia

Castells M., *Galaktyka Internetu*, Dom Wydawniczy Rebis, Poznań2003.

Cornawall H., *New Hacker's Handbook By Hugo Cornwall & Steve Gold*, Ebury Press, Londyn 1992.

Doroziński D., *Hakerzy. Technoanarchiści cyberprzestrzeni*, Helion, Gliwice 2001.

Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Dom Wydawniczy Zakamycze, Kraków 2000.

Internet World Stats, *Usage and Population Statistics*, www.internetworldstats.com.

Jakubki K.J., *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" 1996, nr 12.

Raport Internet Crime Complaint Center IC3.

Rice P., *The Adolescent: Development, Relationships, and Culture*, Allyn and Bacon, Boston 1999.

Shinder D.L., *Cybeprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Helion, Gliwice 2004.

Sowa M., *Ogólna charakterystyka przestępczości internetowej*, „Palestra" 2001, nr 5–6.

[13] H.J. Woo, *The hacker mentality: exploring the relationship between psychological variables and hacking activities,* Dissertation Abstracts International, The University of Georgia, Athens 2003, s. 63.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks Karny (Dz.U. z dnia 2 sierpnia 1997 r. Nr 88, poz. 533.

Woo H.J, *The hacker mentality: exploring the relationship between psychological variables and hacking activities, Dissertation Abstracts International*, The University of Georgia, Athens 2003.

www.business2community.com/tech-gadgets/cyber-crime-causes-445-billion-loss-annually-global-economy-0923809

www.hackerslab.org

www.ic3.gov/media/annualreport/2011_ic3report.pdf

Streszczenie

Pojawienie się Internetu stworzyło wiele nowych możliwości dla rozwoju nauki, kultury i biznesu. Niemniej, wraz z upowszechnieniem się globalnej sieci, pojawiło się także wiele nowych form przestępstw. Celem skutecznej walki z tym zjawiskiem, jednym z kluczowych zadań dla organów ścigania stało się zbudowanie rysu psychologicznego ich sprawców. Artykuł przybliża problematykę przestępczości w Internecie i podejmuje próbę stworzenia portretu psychologicznego przestępców działających w cyberprzestrzeni.

Słowa kluczowe: cyberprzestrzeń, haker, Internet, przestępca, psychologia

PATHOLOGIES IN CYBERSPACE. PSYCHOLOGY OF INTERNET CRIMES PERPETRATORS

Summary

The evolution of Internet has created great opportunities for the development of science, culture, trade and business. Unfortunately, the expansion of global network has also brought many new forms of crime. In order to fight the phenomenon, one of the key tasks for the enforcement has become to create a psychological trait of their perpetrators. The paper introduces the problem of Internet crime and provides an attempt to sketch a psychological profile of criminals operating in cyberspace.