Mariusz Czyżak

Cyberprzestępczość a rozwój społeczeństwa informacyjnego

Ekonomiczne Problemy Usług nr 117, 665-673

2015

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

MARIUSZ CZYŻAK
Urząd Komunikacji Elektronicznej

CYBERPRZESTĘPCZOŚĆ A ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO

Streszczenie

Cyberprzestępczość obejmuje „tradycyjne" czyny zabronione podejmowane w cyberprzestrzeni oraz przestępstwa, których istotą jest wykorzystanie technologii informatycznych. Poziom rozwoju społeczeństwa informacyjnego mierzony jest m.in. wzrostem liczby użytkowników Internetu i użytkowanych urządzeń informatycznych. Naturalną konsekwencją tego rozwoju jest zatem wzrost skali zjawiska przestępczości mającej miejsce w cyberprzestrzeni.
Słowa kluczowe: cyberprzestrzeń, cyberprzestępczość, społeczeństwo informacyjne.

Wprowadzenie

Pojęciu „cyberprzestrzeni" przypisuje się wiele znaczeń. W myśl definicji opracowanej w Departamencie Obrony USA jest to „Globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery" (cyt. za: Wasilewski 2013, s. 227). Francuska Agencja Bezpieczeństwa Sieci oraz Informacji definiuje ją z kolei jako „Przestrzeń komunikacyjną utworzoną przez globalne połączenie sprzętu służącego do automatycznego przetwarzania danych cyfrowych" (cyt. za: Wasilewski 2013, s. 230). Zdaniem Komisji Europejskiej stanowi ona „wirtualną przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery całego świata" (cyt. za: Rajnovic, http://blogs.cisco.com). W Polsce pojęcie to doczekało się definicji legalnej na gruncie przepisów dotyczących stanów nadzwyczajnych – m.in. ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił

Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (DzU nr 156, poz. 1301, ze zm.), gdzie określono ją jako „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (…), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Natura cyberprzestrzeni, niezależnie od podejścia do jej definicji, pozwala zatem stwierdzić, iż stanowi ona nieodłączny element współczesnego rozwoju, będąc nie tylko środowiskiem wymiany informacji czy też obrotu gospodarczego, ale i wymiarem, w którym może być naruszony porządek prawny. Celem niniejszej pracy jest ukazanie pewnych współzależności zachodzących pomiędzy zjawiskiem „cyberprzestępczości" a rozwojem społeczeństwa w takim kształcie, któremu przypisuje się obecnie przymiot „informacyjnego".

1. Wyznaczniki rozwoju społeczeństwa informacyjnego

J.S. Nowak przywołuje w swoim artykule pt. *Społeczeństwo informacyjne – geneza i definicje* trzydzieści definicji społeczeństwa informacyjnego, kwitując to wyliczenie, skłaniającym skądinąd do refleksji, sformułowaniem autorstwa E. Bendyka: „Co to jest społeczeństwo informacyjne? Ideologiczny twór państwowych biurokratów czy precyzyjna etykieta opisująca stan społeczeństwa wskutek rozwoju zaawansowanych technologii? Ani jedno, ani drugie. Społeczeństwo informacyjne to puste stwierdzenie, które w warstwie ideologicznej się wyczerpało, jego wartość opisowa zaś jest równie mała" (cyt. za: Nowak 2008, s. 34–35). Abstrahując od wątpliwości towarzyszących wypracowaniu najbardziej adekwatnego znaczenia idei „społeczeństwa informacyjnego", nie sposób zaprzeczyć, iż termin ten wszedł na trwałe do świadomości społecznej oraz na grunt wielu dziedzin nauki (socjologia, ekonomia, psychologia itp.).

Z pewnością cechą wspólną wszelkich definicji opisujących ten stan rozwoju społeczności ludzkiej jest ich powiązanie z przemianami dotyczącymi trzech obszarów – świadomości i zachowań ludzkich, technologii i edukacji oraz gospodarki. W tym pierwszym mowa jest o przeobrażeniu postrzegania człowieka przez pryzmat informacji i zmian dotyczących charakteru relacji interpersonalnych. Drugi dotyczy nasycenia różnych sfer życia jednostki i społeczeństwa urządzeniami informatycznymi i telekomunikacyjnymi oraz poziomu wykształcenia. Trzeci zaś wskazuje na zorientowanie obrotu gospodarczego na media elektroniczne, prowadzące do e-gospodarki. Zagrożenie wspomnianą już cyberprzestępczością wywiera w oczywisty sposób wpływ na te trzy wymiary przemian, prowadzących do nadania społeczeństwu miana „społeczeństwa informacyjnego".

Przywołać wypada w tym miejscu niektóre spośród wskaźników mających zobrazować stopień rozwoju społeczeństwa informacyjnego, takie chociażby jak: przygotowany przez Międzynarodowy Związek Telekomunikacyjny – Digital Ac-

cess Index (dalej: DAI), Information Society Index (dalej: ISI) oraz zestaw wskaźników opracowanych w ramach World Summit of Information Society 2013 (Luterek 2010, s. 17–29). Wskaźnik DAI obejmuje takie elementy, jak infrastruktura (liczba abonentów telefonii na 100 mieszkańców), kosztochłonność (koszt dostępu do Internetu względem poziomu PKB na 1 mieszkańca), wiedza (wykształcenie dorosłych oraz liczba uczniów i studentów), jakość (mierzona m.in. liczbą abonentów Internetu szerokopasmowego na 100 mieszkańców) oraz wykorzystanie (liczba użytkowników Internetu na 100 mieszkańców). ISI dotyczy natomiast czterech obszarów – aspektów społecznych (odsetek osób pobierających naukę w szkolnictwie średnim i wyższym, wolności obywatelskie, poziom korupcji w administracji), Internetu (liczba użytkowników Internetu w ogóle, Internetu w domu, Internetu mobilnego, poziom wydatków w e-handlu), komputerów (liczba gospodarstw domowych z komputerem osobistym, poziom wydatków w sektorze IT względem PKB, poziom usług sektora IT względem PKB, poziom wydatków na oprogramowanie) oraz telekomunikacji (liczba gospodarstw domowych z Internetem szerokopasmowym, liczba abonentów Internetu szerokopasmowego, liczba sprzedanych urządzeń mobilnych). W trakcie WSIS 2013 zdefiniowano z kolei aż 42 wskaźniki odnoszące się kolejno do: poziomu rozwoju infrastruktury telekomunikacyjnej i jej dostępności, poziomu dostępności technologii informacyjnych i komunikacyjnych oraz ich wykorzystania przez gospodarstwa domowe i indywidualnych użytkowników, poziomu dostępności technologii informacyjnych i komunikacyjnych oraz ich wykorzystania przez przedsiębiorstwa, a także poziomu rozwoju sektora technologii informacyjnych i komunikacyjnych.

2. Dostęp do Internetu a rozwój społeczeństwa informacyjnego

Już pobieżny przegląd struktury przywołanych powyżej wskaźników pozwala stwierdzić, iż jednym z najistotniejszych determinantów rozwoju społeczeństwa informacyjnego jest z pewnością poziom dostępu do Internetu i korzystania z portali społecznościowych, jak również innych kategorii usług telekomunikacyjnych. Wg raportu Global Digital Statistics 2014 ze stycznia 2014 r. dostęp do Internetu posiadało niemal 2485 mln ludzi, tj. 35% ogółu populacji na świecie, przy czym prawie 1857 mln było aktywnymi użytkownikami sieci społecznościowych (1184 mln – Facebook, 816 mln – QQ, Qzone – 632 mln, Whatsapp – 400 mln, 300 mln – Google+, WeChat – 272 mln, LinkedIn – 259 mln, Twitter – 252 mln, Tumblr – 230 mln, Tencent Weibo – 220 mln). Penetracja sieci telefonii komórkowej sięgała aż 93% ogółu ludzkości. Dodać wypada, iż w Polsce niemal 31% użytkowników Internetu to aktywni uczestnicy największych portali społecznościowych. (Global Digital Statistics 2014, s. 5, 11, 34). Raport sporządzony dla Urzędu Komunikacji Elektronicznej w 2014 r. wskazuje na wysoki poziom nasycenia usługami teleko-

munikacyjnymi. Jedynie 3% Polaków w wieku 15 lat lub starszych nie posiadało żadnej usługi (telefonu komórkowego, telefonu stacjonarnego ani dostępu do Internetu). Aż 88% badanych posiada telefon komórkowy, 23% gospodarstw domowych – telefon stacjonarny, a z dostępu do Internetu (niezależnie od rodzaju łącza) korzysta 58% Polaków w wieku 15 lat i więcej. Większość robi to codziennie bądź kilka razy w tygodniu, najczęściej sprawdzając pocztę elektroniczną, odwiedzając portale internetowe i serwisy społecznościowe, słuchając muzyki przez Internet oraz używając komunikatorów (*Rynek usług telekomunikacyjnych…* 2014, s. 11, 14). Co istotne, prowadzone badania wskazują, iż należy do nich znaczący odsetek nieletnich. Aż 90% dzieci w wieku 13–15 lat deklaruje korzystanie z Facebooka. 17% spośród nieletnich w wielu 10–15 lat spędza w dni szkolne co najmniej 2 godziny w Internecie, a w dni wolne poświęca taką ilość czasu 40% (*Bezpieczeństwo dzieci…* 2013, s. 11, 16). Wzrostowi liczby użytkowników Internetu towarzyszy również z oczywistych powodów wzrost liczby wykorzystywanych przez nich urządzeń. Według ostatnich prognoz Cisco Systems do roku 2020 do Internetu podłączonych będzie na świecie około 50 mld urządzeń (Mikołajczyk, http://www.biznes.newseria.pl).

3. Pojęcie cyberprzestępczości

Cyberprzestępstwo określane jest jako „czyn zabroniony popełniony w obszarze cyberprzestrzeni" (*Polityka ochrony…* 2013, s. 5). Do przestępstw tego rodzaju, mając na względzie aspekty prawnokarne i kryminologiczne, należy zatem dosyć szeroki krąg czynów zabronionych. Po pierwsze, klasyczne typy przestępstw popełniane nie w sposób „tradycyjny", ale w przestrzeni teleinformatycznej, np. oszustwa popełniane z wykorzystaniem technologii informatycznych w ramach bankowości elektronicznej. Po drugie, takie czyny zabronione, których istotą jest wykorzystanie technologii informatycznych, np. tzw. sabotaż komputerowy. Różnorodność rodzajową zjawiska cyberprzestępczości potwierdzają regulacje prawa międzynarodowego, a także dane analityczne i statystyczne.

W świetle danych policyjnych wyróżnić można trzy kategorie przestępstw zaliczanych do tzw. cyberprzestępczości – przestępstwa komputerowe (np. hacking komputerowy, podsłuch komputerowy, sabotaż komputerowy), przestępstwa telekomunikacyjne (np. klonowanie numerów IMEI telefonów komórkowych) i przestępstwa internetowe (np. podmiana zawartości stron WWW, nielegalne gry hazardowe w Internecie, nieuprawniony dostęp do skrzynek e-mail) (*Cyberprzestępczość*, http://www.policja.pl). Niezależnie od formy działalności cyberprzestępczej poza dyskusją pozostaje fakt, iż jej istnienie nie jest możliwe bez wykorzystania Internetu jako medium komunikacyjnego.

Ten „internetowy" charakter znacznej części form cyberprzestępczości potwierdzają niejako postanowienia Konwencji Rady Europy o cyberprzestępczości przyjętej w Budapeszcie 23 listopada 2001 r., ratyfikowanej przez Sejm RP 12 września 2014 r. (http://orka.sejm.gov.pl). Co prawda nie zawiera ona definicji „cyberprzestępczości", ale wskazuje na takie kategorie czynów, które powinny zostać poddane penalizacji na gruncie ustawodawstwa krajowego, tj. przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (nielegalny dostęp, nielegalne przechwytywanie danych, naruszenie integralności danych, naruszenie integralności systemu, niewłaściwe używanie urządzeń); przestępstwa komputerowe (fałszerstwa komputerowe, oszustwa komputerowe); przestępstwa ze względu na charakter zawartych informacji (związane z pornografią dziecięcą) oraz przestępstwa dotyczące naruszenia praw autorskich i praw pokrewnych. A zatem znowu mowa jest o takich czynach zabronionych, których częstokroć nie sposób popełnić bez wykorzystania Internetu.

Taką diagnozę obrazu tego zjawiska potwierdza również treść Komunikatu Komisji Europejskiej do Parlamentu Europejskiego, Rady oraz Komitetu Regionów KOM(2007) 267 wydanego w Brukseli w dniu 22 maja 2007 r. (http://eur-lex.europa.eu) dotyczącego ogólnej strategii zwalczania cyberprzestępczości. Stwierdza się w nim, iż przy użyciu środków komunikacji elektronicznej popełniona może być większość tradycyjnych przestępstw, jakkolwiek zwykle są to różnego rodzaju oszustwa. Rosnącym problemem staje się przy tym nielegalny handel internetowy, tak krajowy, jak i międzynarodowy, obejmujący m.in. handel narkotykami, bronią, czy też zagrożonymi gatunkami zwierząt. W krajach europejskich zaobserwować można również istnienie coraz liczniejszych stron internetowych zawierających takie nielegalne treści, jak materiały związane z pedofilią, podżeganiem do aktów o charakterze terrorystycznym i ich pochwałą, terroryzmem, rasizmem i ksenofobią. Coraz częściej dokonuje się masowych ataków, skierowanych przeciwko systemom informatycznym, instytucjom, jak i osobom prywatnym. Zaobserwowano także przypadki bezpośrednich, skoordynowanych, systematycznych i masowych ataków na teleinformatyczną infrastrukturę krytyczną niektórych państw. Sytuację pogarsza równoczesne zastosowanie różnych technologii i istnienie powiązań pomiędzy systemami informatycznymi, co sprawia, że są one bardziej na nie podatne. Przedsięwzięcia tego rodzaju są częstokroć bardzo dobrze przygotowane, a ich celem jest wymuszenie. Zdaniem autorów komunikatu przypuszczać można, iż liczba zgłoszonych ataków jest zaniżona, przede wszystkim ze względu na straty, jakie mogłoby przynieść przedsiębiorstwom upublicznienie informacji o problemach z bezpieczeństwem. Jednocześnie daje się zauważyć stały wzrost liczby przestępstw o charakterze informatycznym, a przy tym transgranicznych, popełnianych w coraz bardziej wyrafinowany sposób oraz powiązanych z przestępczością zorganizowaną.

4. Skala i skutki przestępczości w sieci Internet

Dla potwierdzenia tezy o wzroście liczby przestępstw popełnianych z wykorzystaniem Internetu posłużyć można się chociażby wynikami raportu przygotowanego przez Norton dla Symantec, opartego na badaniach przeprowadzonych wśród 13 022 osób w wieku od 18 do 64 lat pochodzących z 24 krajów (m.in. Stanów Zjednoczonych, Rosji, Polski, Brazylii, Indii, Szwecji, Turcji, Zjednoczonych Emiratów Arabskich, Japonii, Włoch). Wskazuje on, iż do cyberprzestępstw zaliczyć można takie czyny jak: kradzieże tożsamości, włamania na konta e-mailowe i profile w sieciach społecznościowych i podszywanie się pod ich posiadaczy, oszustwa z wykorzystaniem kart kredytowych dokonane drogą elektroniczną, kradzież i wykorzystanie smartfonu bez zgody posiadacza, przy czym ofiarą cyberprzestępców pada dziennie 1 mln osób. Szacuje się, iż same koszty ponoszone z tytułu cyberprzestępczości w krajach poddanych badaniu osiągnęły w roku 2013 poziom 113 mld USD (w USA 38 mld, w Europie – 12 mld USD). Aż 38% spośród nich to następstwo oszustw. Co więcej, aż 50% dorosłych użytkowników Internetu zadeklarowało, iż w ciągu ostatniego roku padło ofiarą bądź to cyberprzestępstw, bądź to innych negatywnych zjawisk w Internecie, np. stalkingu, przy czym 41% stało się obiektem takich ataków jak hacking, oprogramowanie złośliwe, wirusy komputerowe, kradzieże i oszustwa. W badaniu prowadzonym w roku 2013 zaobserwowano również 50-procentowy wzrost do kwoty 298 USD, w porównaniu do roku 2012, kosztów cyberprzestępczości w przeliczeniu na 1 pokrzywdzonego (*Norton Cybercrime Report* 2013). Zdaniem polskiej Policji przewidywany jest dalszy wzrost rozmiarów cyberprzestępczości. Związane jest to przede wszystkim ze stale rosnącą liczbą użytkowników Internetu, jak również coraz częstszym wykorzystywaniem przez cyberprzestępców urządzeń mobilnych korzystających z punktów dostępowych do sieci Internet (*Cyberprzestępczość*, http://www.policja.pl), czego nie sposób nie wiązać z determinantami rozwoju społeczeństwa informacyjnego.

Rzeczywista skala zjawiska cyberprzestępczości jest niezwykle trudna do określenia, tak z uwagi na różnorodność form działalności przestępczej, jak i „wirtualny" charakter tej działalności, jakkolwiek jej koszty społeczne i ekonomiczne są znaczące wobec skali wykorzystania Internetu w gospodarce i życiu społecznym. Straty gospodarcze poniesione na świecie w roku 2013 spowodowane działalnością o charakterze cyberprzestępczym szacowane są na 445 mld dolarów, zaś ich konsekwencją jest również spadek PKB o 0,9% w krajach rozwiniętych, a także utrata 200 tysięcy miejsc w pracy i 150 tysięcy w krajach Unii Europejskiej. Pośrednie koszty cyberprzestępczości to m.in. również koszty utraty zaufania klientów do e-usług, koszty poprawy stanu bezpieczeństwa infrastruktury teleinformatycznej, utrata części klientów przez przedsiębiorców (*445 mld dolarów strat z powodu cyberprzestępczości*, http://www.ekonomia.rp.pl). Podkreślić należy, że na działania nielegalne w znacznym stopniu narażone są również struktury teleinformatyczne

sektora publicznego. Warto zatem przy tym odnotować, iż z *Raportu o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2013* sporządzonego przez CERT.GOV.PL wynika, że w roku 2013 zarejestrowanych zostało aż 8817 zgłoszeń, spośród których 5670 zakwalifikowano jako incydenty, zaś 4270 z nich to tzw. „botnety", dotyczące złośliwego oprogramowania działającego na stacjach roboczych podłączonych do sieci teleinformatycznej jednostek organizacyjnych wchodzących w skład administracji publicznej (*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2013*, www.cert.gov.pl, s. 5, 7).

Podsumowanie

Wskaźnikiem rozwoju społeczeństwa informacyjnego, niezależnie od przypisywanej mu definicji, jest z pewnością wzrost stopnia wykorzystywania technologii informatycznych, tak jeśli chodzi o liczbę użytkowanych urządzeń, jak i zakres ich wykorzystywania w gospodarce, nauce, edukacji, itd. Utrzymujący się zatem stały wzrost liczby użytkowników Internetu i zakresu usług świadczonych za jego pośrednictwem, a także liczby samych urządzeń wykorzystywanych w sieci sprawia, że użytkownicy Internetu stają się bardziej podatni na ataki cyberprzestępców. Dzieje się tak ze względu na powszechność korzystania z technologii informatycznych i Internetu, a niekiedy rezygnację z dotychczas form aktywności społecznej i gospodarczej np. na rzecz poczty elektronicznej, portali społecznościowych, czy też sklepów internetowych i bankowości elektronicznej. Tym samym oczywiste jest, że rozwojowi społeczeństwa informacyjnego (zakładając, iż jest to tendencja stała) towarzyszył będzie również stały wzrost rozmiarów takiego zjawiska patologicznego, jakim jest cyberprzestępczość – proceder polegający na wykorzystaniu cyberprzestrzeni i nowych technologii informacyjnych do naruszania porządku prawnego. Nie można oprzeć się wręcz dosyć przekornemu stwierdzeniu, iż bez pozyskania przez społeczeństwo charakteru informacyjnego nie mielibyśmy do czynienia ze zjawiskiem cyberprzestępczości, wobec braku użytkowników Internetu mogących stać się przedmiotem ataku ze strony cyberprzestępców. Pamiętać należy przy tym jednak, że nie ma ona jedynie wymiaru prawnokarnego i kryminologicznego, ale także wymiar społeczny i ekonomiczny. Cyberprzestępstwa powodują bowiem wymierne straty, wpływając na poziom rozwoju gospodarczego, a także na zachowania ludzkie, powodowane chociażby obawą przed staniem się obiektem ataku o charakterze cyberprzestępczym. W pewnym sensie prowadzą zatem równocześnie do spowalniania procesu rozwoju społeczeństwa informacyjnego, podnosząc koszty wykorzystania technologii teleinformatycznych z uwagi na kwestię zachowania należytego poziomu bezpieczeństwa usług świadczonych z ich wykorzystaniem, jak również odstręczając od korzystania z nich jako potencjalnego źródła cyberataku. Mając na względzie rosnący poziom wykorzystania Internetu

oraz wszechobecność zastosowania technologii informatycznych, wydaje się jednakże, że wzrost liczby popełnianych w cyberprzestrzeni przestępstw oraz ich różnorodność nie stanowią realnego zagrożenia dla rozwoju społeczeństwa informacyjnego.

Literatura

1. *Bezpieczeństwo dzieci w Internecie. Raport z badań jakościowych i ilościowych* (2013), Warszawa, http://www.fdn.pl.
2. *Cyberprzestępczość*, http://www.policja.pl.
3. *Global Digital Statistics* 2014, http://wearesocial.net.
4. Hofmokl J. (2009), *Internet jako nowe dobro wspólne*, Warszawa.
5. Kańciak A. (2013), *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 8.
6. Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady oraz Komitetu Regionów KOM(2007)267 wydany w Brukseli w dniu 22 maja 2007 r. dotyczący ogólnej strategii zwalczania cyberprzestępczości, http://eur-lex.europa.eu.
7. Konwencja o cyberprzestępczości, Budapeszt, 23 listopada 2001 r., http://nowetechnologie.umk.pl.
8. Luterek M. (2010), *e-Government. Systemy informacji publicznej*, Warszawa.
9. Mikołajczyk G., *Do 2020 roku 50 mld urządzeń na świecie będzie podłączonych do Internetu. To pole do działań dla cyberprzestępców*, 13 października 2014 r., http://www.biznes.newseria.pl.
10. *Norton Cybercrime Report* (2013).
11. Nowak J.S. (2008), *Społeczeństwo informacyjne – geneza i definicje*, w: P. Sienkiewicz, J.S. Nowak (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, Katowice.
12. *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa, 25 czerwca 2013 r.
13. Rajnovic D., *Cyberspace – what is it?*, http://blogs.cisco.com.
14. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2013*, www.cert.gov.pl
15. *Rynek usług telekomunikacyjnych w Polsce w 2014 roku. Raport z badania klientów indywidualnych*, grudzień 2014, http://www.uke.gov.pl.
16. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (DzU nr 156, poz. 1301, z późn. zm.).
17. Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 9.
18. *445 mld dolarów strat z powodu cyberprzestępczości*, 21 czerwca 2014 r., http://www.ekonomia.rp.pl.

CYBERCRIME AND DEVELOPMENT OF INFORMATION SOCIETY

Summary

A phenomenon called "cybercrime" contains two kinds of crimes – "traditional" crimes committed in the cyberspace and crimes committed with the use of information technology. The level of information society development is particularly connected with growth in the number of Internet users and the number of active IT devices. Because of that, increasing criminality taking place in the cyberspace is a natural consequence of this development.

Keywords: cyberspace, cybercrime, information society.

Translated by Mariusz Czyżak