Mariusz Czyżak

Cyberprzestępczość i jej wpływ na rozwój gospodarki elektronicznej

Ekonomiczne Problemy Usług nr 88, 732-740

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 703 EKONOMICZNE PROBLEMY USŁUG NR 88 2012

MARIUSZ CZYŻAK
Urząd Komunikacji Elektronicznej
Wyższa Szkoła Kadr Menedżerskich w Koninie

CYBERPRZESTĘPCZOŚĆ I JEJ WPŁYW NA ROZWÓJ GOSPODARKI ELEKTRONICZNEJ

Wprowadzenie

Nie budzi wątpliwości twierdzenie, że wszechobecny i postępujący rozwój technologiczny wpływa nie tylko na życie jednostki, ale przede wszystkim na funkcjonowanie szeroko rozumianej gospodarki, nadając jej częstokroć wymiar elektroniczny. Nie można jednakże utożsamiać tzw. gospodarki elektronicznej z zupełnie odrębną gałęzią aktywności ekonomicznej człowieka. Przymiotnik „elektroniczny" rozciąga się bowiem tutaj na szereg, niekiedy odległych, dziedzin życia gospodarczego, odnosząc się do swego rodzaju płaszczyzny świadczenia usług we współczesnej dobie. Pod pojęciem gospodarki elektronicznej rozumieć należy zatem tę jej część (ale nie autonomiczną gałąź), gdzie technologia teleinformatyczna stanowi specyficzny nośnik świadczenia różnego rodzaju usług, wpływając przy tym na ich zakres, dostępność, różnorodność, możliwość bieżącej adaptacji do potrzeb klienta, itp. Z tego też względu obejmować ona będzie zatem zarówno typowe – z uwagi na nieodłączne zastosowanie na ich gruncie technologii teleinformatycznych – sektory, tj. telekomunikacyjny, medialny i IT, ale również takie obszary gospodarki kraju, jak np. bankowość czy też handel detaliczny. Udział w działalności gospodarczej szeroko rozumianych usług informacyjnych, czy to w postaci tzw. pośredniego handlu internetowego, gdzie drogą elektroniczną dokonywane są jedynie zamówienia towarów i usług, świadczonych następnie przy wykorzystaniu kanałów tradycyjnych (np. pocztą), czy to w postaci bezpośredniego handlu internetowego, polegającego na wykorzystaniu drogi elektronicznej w trakcie całej transakcji, stanowi przy tym wyznacznik rozwoju społeczeństwa informacyjnego. Nieskrępowany

i prawidłowy rozwój e-gospodarki uzależniony jest – analogicznie jak w przypadku innych obszarów aktywności ekonomicznej człowieka – od wielu czynników zewnętrznych, w tym i występowania różnorakich zjawisk patologicznych godzących w prawidłowość obrotu gospodarczego, tak z punktu widzenia interesów klientów, jak i przedsiębiorców. Jednym z nich jest problem zagrożenia cyberprzestępczością. W świetle powyższego należy zatem dokonać analizy treści i skali zjawiska tzw. cyberprzestępczości, a także charakteru i rozmiarów jej wpływu na rozwój gospodarki elektronicznej.

1. Pojęcia „cyberprzestrzeni" i „cyberprzestępczości"

Poddając analizie zagadnienie stanowiące przedmiot niniejszych rozważań, wypada rozpocząć od przywołania terminu 'cyberprzestrzeń'. Jako pierwszy posłużył się nim William Gibson w swojej książce z 1984 r. zatytułowanej *Neuromancer*, uznając ją za swego rodzaju wirtualną pozaczasową przestrzeń istniejącą dzięki technologii teleinformatycznej. Określił on ją w sposób następujący: „To jest cyberprzestrzeń. Konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych… Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność (…)"[1].

Termin ten doczekał się jednakże również definicji oficjalnej, żeby nie rzec legalnej. I tak np. na gruncie *Założeń Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011* cyberprzestrzeń uznawana jest za przestrzeń komunikacyjną tworzoną przez system powiązań internetowych, zaś „cyberprzestrzeń państwa" to przestrzeń komunikacyjna tworzona przez „system wszystkich powiązań internetowych znajdujących się w obrębie państwa". Obejmuje ona w konsekwencji m.in. „systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne"[2].

Można zatem uznać, iż stanowi on swoisty technosystem ogólnodostępnej komunikacji społecznej, powstały w następstwie zaistnienia trojakiego rodzaju procesów. Po pierwsze, integracji form przekazu i prezentacji informacji, która

---

[1] W. Gibson, *Neuromancer*, Wydawnictwo Książnica, Katowice 2011, s. 59.

[2] *Założenia Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011*, http:// cert.gov.pl, s. 4.

doprowadziła do ucyfrowienia tzw. infosfery. Po drugie, konwergencji systemów teleinformatycznych i telekomunikacyjnych, jak również mediów elektronicznych. Po trzecie, powstania globalnej zintegrowanej platformy teleinformatycznej[3].

Samo pojęcie „cyberprzestępczości", używane niekiedy zamiennie, nie zawsze zresztą słusznie, z terminami „przestępczość komputerowa", „przestępczość internetowa" itp., obejmować powinno, w kryminologicznym i szerokim tego słowa znaczeniu, wszelkie zachowania patologiczne podlegające odpowiedzialności prawnej (karnej, wykroczeniowej, karnoadministracyjnej), dokonywane z wykorzystaniem sieci teleinformatycznych w tzw. cyberprzestrzeni, niezależnie od tego, czy stanowią one przestępstwo, czyn nieuczciwej konkurencji będący wykroczeniem, czy też delikt karnoadministracyjny. Istotna jest bowiem tutaj nie kwalifikacja prawna określonego zachowania godzącego w dobra podmiotów będących użytkownikami Internetu, ale natura przestrzeni, w której do niego dochodzi, jak również rodzaj użytej technologii.

2. Zjawisko cyberprzestępczości – aspekty prawnokarne i kryminologiczne

Dotychczas zidentyfikowano szereg rozmaitych form zjawisk patologicznych zachodzących w Internecie, mających w wielu przypadkach związek z tzw. nielegalnym biznesem w sieci. Mowa tutaj m.in. o usługach finansowych on-line (np. „cyberlaundering" brudnych pieniędzy), naruszeniach praw autorskich, nieuczciwej konkurencji i szpiegostwie gospodarczym, nielegalnym handlu medykamentami, antykami, bronią i materiałami wybuchowymi, itp.[4]

Z prawnego punktu widzenia w grę będą tutaj wchodzić zatem m.in. przestępstwa znane ustawie z dnia 6 czerwca 1997 r. Kodeks karny (DzU 1997, nr 88, poz. 553, ze zm.; dalej: K.k.), takie jak np. udaremnianie lub znaczne utrudnianie dostępu do informacji osobie do tego uprawnionej, dotyczącego zapisu na komputerowym nośniku informacji (art. 268 § 2 K.k.) oraz przestępstwo sabotażu komputerowego (art. 269 K.k.). Analogicznie karalności podlega ponadto niszczenie albo dokonanie wymiany nośnika informacji oraz niszczenie albo uszkadzanie urządzenia służącego automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji (art. 269 § 2 K.k.)[5]. „Cyberprzestępstwo" może przybierać także rozmaite postaci oszustwa (art. 286 K.k.), które będąc dokonywanymi w sieci stanowią postać nieporównywalnie bardziej szkodliwą aniżeli klasyczny typ tego przestępstwa.

---

[3] P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm – nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Warszawa 2009, s. 195.

[4] J.W. Wójcik, *Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne*, w: *Cyberterroryzm…*, *op. cit.*, s. 310–311.

[5] M. Czyżak, *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1–2, s. 50–51.

Warto wspomnieć o kilku z nich. Mowa tutaj w szczególności o tzw. phishingu (ang. *password harvesting fishing* – łowienie haseł). Polega on na oszukańczym pozyskiwaniu informacji poufnej od indywidualnego użytkownika (np. loginu lub hasła konta internetowego, PIN-u do bankomatu, numeru karty kredytowej itp.), poprzez podszywanie się pod godną zaufania osobę (np. pracownika banku), której informacje te są pilnie potrzebne np. z uwagi na konieczność weryfikacji danych personalnych. W następstwie wyłudzenia hasła „napastnik" uzyskuje dostęp do konta osoby pokrzywdzonej i wykorzystuje je w celu przestępczym, np. dla uzyskania korzyści finansowej. Odmiany tego zjawiska to również tzw. SMiShing (ang. *SMS phishing* – phishing SMS-owy) oraz tzw. pharming. Ten pierwszy sprowadza się do przesyłania SMS-ów mających nakłonić „ofiarę ataku" do wykonania na stronie internetowej wskazanej czynności, która skutkuje w konsekwencji zainstalowaniem na komputerze tegoż użytkownika szkodliwego oprogramowania. Pharming, jako bardziej skomplikowana forma phishingu, polega z kolei na przekierowywaniu użytkownika Internetu do spreparowanej strony internetowej, która łudząco przypomina lub jest, z uwagi na wygląd, identyczna z witryną serwisu aukcyjnego, banku internetowego, sklepu internetowego czy też innego podmiotu tego rodzaju, a następnie pozyskaniu danych niezbędnych „napastnikowi" do zdobycia korzyści finansowych, np. poprzez kradzież z konta bankowego[6].

W celu zobrazowania skali ilościowej zjawiska przestępczości związanej z nowoczesnymi technologiami, w tym z Internetem, której rozmiary rzutują na rozwój e-gospodarki, wskazać należy chociażby kilka policyjnych danych statystycznych z ostatnich lat. I tak, jak podają wspomniane statystyki, tylko w I półroczu 2011 w wyniku oszustw dokonanych przy wykorzystaniu mediów pokrzywdzono łącznie 8044 osoby, zaś telefon komórkowy stał się głównym przedmiotem przestępstwa w 22 672 zdarzeniach. W roku 2010 o nielegalne zakładanie podsłuchu podejrzanych było 190 osób. Nadal pokaźna, aczkolwiek odbiega od najwyższych wskaźników tego rodzaju przestępczości, jest skala naruszeń praw własności intelektualnej w dziedzinie programów komputerowych. W roku 2010 wszczęto w tym zakresie 401 postępowań (przy 1500 w roku 2006, 1483 w roku 2007, 1436 w roku 2008 i 986 w roku 2009), przy czym zabezpieczono ponad 22 tysiące nośników (przy 143 995 w roku 2007, 98 282 w roku 2008 i 28 925 w roku 2009). Co więcej, w związku z rosnącą liczbą użytkowników Internetu oraz podmiotów świadczących usługi za pośrednictwem tego medium, rośnie również liczba przestępstw popełnianych w sieci. I tak, o ile w latach 2009 i 2010 odnotowano odpowiednio 6124 i 7733 przestępstwa popełnione w sieci (w tym odpowiednio 4915

[6] M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary – Automatyka – Kontrola" 2009, nr 7, s. 549.

i 6260 oszustw), to w I półroczu roku 2011 ich liczba osiągnęła poziom 7590 (w tym 6727 oszustw)[7].

3. Wpływ cyberprzestępczości na e-gospodarkę

Rozmiary i zakres wpływu cyberprzestępczości na funkcjonowanie gospodarki narodowej są nieporównywalnie poważniejsze i trudniejsze do zdefiniowania aniżeli rozmiary i wpływ jakiejkolwiek znanej dotychczas innej formy przestępczości na określoną dziedzinę działalności gospodarczej. Powodów takiego stanu rzeczy jest wiele. Wymienić wśród nich należy m.in.: szeroki krąg podmiotów narażonych na atak cyberprzestępczy, wyrafinowane metody działania cyberprzestępców, trudny do oszacowania poziom szkód wyrządzonych w następstwie cyberprzestępstw, a wreszcie chociażby znikome możliwości wykrycia sprawców zachowań patologicznych związanych z wykorzystaniem sieci Internet.

Po pierwsze, każdy uczestnik wymiany handlowej, do której dochodzi w obszarze gospodarki określanym mianem „gospodarki elektronicznej", jest potencjalnym obiektem ataku cyberprzestępczego. Mowa tutaj zarówno o przedsiębiorcach, jak i o konsumentach usług świadczonych drogą elektroniczną. Ci pierwsi są bowiem, jako podmioty zaliczane do e-gospodarki, automatycznymi użytkownikami sieci Internet i technologii teleinformatycznych, czy to jako przedsiębiorcy, których istotą jest świadczenie usług wyłącznie drogą elektroniczną, jak to ma miejsce np. w przypadku sklepów internetowych, czy to jako ci, którzy utrzymują stały kontakt z klientem za pośrednictwem łączy internetowych, stając się np. przedmiotem oszustw internetowych lub spammingu. Dotyczy to wreszcie klientów usług internetowych padających ofiarą nieuczciwych praktyk rynkowych (np. dostarczanie produktów o niewłaściwych parametrach jakościowych), wyłudzeń itp.

Po drugie, stale postępujący rozwój technologiczny w dziedzinie teleinformatyki, który już sygnalizowano na wstępie niniejszych rozważań, sprawia, że metody działań stosowane przez przestępców w cyberprzestrzeni stają się coraz to bardziej wyszukane. W konsekwencji użytkownikom Internetu coraz trudniej ustrzec się przed staniem się ofiarą cyberprzestępstwa, a stosowane przez przedsiębiorców systemy zabezpieczeń wymagają stałego doskonalenia, podążającego niejako za przemyślnością ich sprawców.

Po trzecie, wysokość rzeczywistych szkód ponoszonych przez przedsiębiorców i konsumentów jest niezwykle trudna do ustalenia. Z jednej bowiem strony poważnych problemów dostarcza sama próba oszacowania szkodliwości niektórych zjawisk, np. spammingu, jako czynu nieuczciwej konkurencji obniżającego zaufanie konsumenta do usług świadczonych drogą elektroniczną, z drugiej zaś strony

[7] Internet: http://statystyka.policja.pl.

rzeczywista skala zjawiska cyberprzestępczości wydaje się odznaczać wysokim poziomem tzw. ciemnej liczby przestępstw. Wiele osób nie informuje organów ścigania o zaistniałych naruszeniach porządku prawnego, nie łudząc się, że ich sprawcy zostaną ujęci.

Po czwarte, specyfika sieci Internet i wirtualny oraz globalny charakter cyberprzestrzeni sprawiają, że źródło ataku cyberprzestępczego, nie dość, że trudne do uchwycenia w określonym czasie, zlokalizowane może być w miejscu bardzo odległym (nie tylko w innym kraju, ale na innym kontynencie). Stąd też także prawne możliwości ścigania sprawców przestępstw sieciowych są ograniczone, a materiał dowodowy trudny do ustalenia. Sami przestępcy zaś, czując się bezkarni, ponawiając ataki na infrastrukturę informatyczną nie tylko indywidualnych konsumentów, ale również poważnych korporacji międzynarodowych, banków, a nawet całych państw.

Samo zagrożenie cyberprzestępczością wpływa w znaczący sposób na zachowania trojakiego rodzaju podmiotów – przedsiębiorców, klientów usług internetowych oraz podmiotów publicznych zajmujących się stanowieniem prawa oraz ochroną praw konsumentów i zwalczaniem przestępczości (w tym tej mającej miejsce w cyberprzestrzeni), wymuszając podejmowanie przez nich określonych przedsięwzięć. Co istotne, determinuje kierunki rozwoju technologicznego, zmuszając przedsiębiorców, i to nie tylko telekomunikacyjnych, jak również działające na ich rzecz rozmaite ośrodki badawczo-rozwojowe, do innowacyjności i poszukiwania narzędzi organizacyjnych i technicznych umożliwiających skuteczne zabezpieczenie interesów konsumentów i infrastruktury teleinformatycznej przed atakiem cyberprzestępców. Koszty wspomnianych powyżej prac doświadczalnych i wdrażanych mechanizmów ochronnych podnoszą w oczywisty sposób koszty działalności gospodarczej prowadzonej przez przedsiębiorców, a tym samym wpływają na cenę świadczonych przez nich usług. Zjawiska patologiczne w tym obszarze intensyfikują jednocześnie prace legislacyjne i wyznaczają treść ustawodawstwa regulującego ramy prowadzenia działalności gospodarczej z wykorzystaniem elektronicznej drogi świadczenia usług, zwłaszcza w sektorze finansowym, telekomunikacyjnym i medialnym. Wspomnieć tutaj należy m.in. o takich aktach rangi ustawowej jak: ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU 2010, nr 46, poz. 276, ze zm.), ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (DzU 2002, nr 126, poz. 1068, ze zm.), ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (DzU 2002, nr 144, poz. 1204, ze zm.), czy też ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (DzU 2002, nr 169, poz. 1385, ze zm.). Świadczy o tym chociażby treść uzasadnień do przywołanych powyżej aktów normatywnych. I tak np. w uzasadnieniu do *Projektu ustawy o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie*

warunkowym wyraźnie wskazano, iż „Celem projektowanej ustawy o ochronie niektórych usług świadczonych drogą elektroniczną dostępnych warunkowo oraz usług świadczenia dostępu warunkowego jest zapewnienie ochrony usługodawcom, świadczącym usługi tego rodzaju, przed pozbawianiem ich należnych im wynagrodzeń przez osoby, które wprowadzają, a także używają w obrocie handlowym niedozwolonych urządzeń oraz innych rozwiązań technicznych służących obejściu zabezpieczeń”[8], zaś w uzasadnieniu do *Projektu ustawy o świadczeniu usług drogą elektroniczną* stwierdzono: „Aby zapewnić bezpieczeństwo transakcji elektronicznych, a tym samym zwiększyć wartość rynku e-gospodarki w Polsce, należy zagwarantować tak usługobiorcom, jak i usługodawcom przejrzyste i uregulowane normami prawnymi funkcjonowanie obrotu elektronicznego”[9].

Potrzeba zapewnienia bezpieczeństwa teleinformatycznego, tak instytucji państwowych, jak i komercyjnych, obliguje wreszcie organy ochrony prawnej do podejmowania działań mających na celu zapobieganie, wykrywanie i ściganie przestępczości o charakterze elektronicznym. Mowa tutaj w szczególności o Agencji Bezpieczeństwa Wewnętrznego i Rządowym Zespole Reagowania na Incydenty Komputerowe (CERT.GOV.PL). Funkcjonują one zgodnie z Założeniami Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011 (RPOC), przyjętymi przez Komitet Stały Rady Ministrów w dniu 9 marca 2009 r. Do zadań CERT należy zaś m.in. kreowanie polityki w zakresie ochrony przed cyberzagrożeniami, reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury teleinformatycznej państwa, czy też świadczenie doradztwa w zakresie cyberbezpieczeństwa[10].

Podsumowanie

Nie sposób nie zgodzić się z tezą, iż zjawisko cyberprzestępczości wywiera istotny wpływ na rozwój gospodarki określanej mianem elektronicznej. Samo wykorzystanie Internetu, stanowiącego na jej gruncie podstawową płaszczyznę wymiany handlowej, sprzyja bowiem nie tylko rozwojowi gospodarki narodowej jako takiej, ale umożliwia przy tym przedstawicielom środowisk przestępczych (częstokroć o charakterze międzynarodowym i zorganizowanym) kreowanie szeregu nowych postaci zjawisk patologicznych, dotychczas pozostających jedynie w sferze

---

[8] *Uzasadnienie do projektu ustawy o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym*, Sejm RP IV kadencji, Druk sejmowy nr 353.

[9] *Uzasadnienie do projektu ustawy o świadczeniu usług drogą elektroniczną*, Sejm RP IV kadencji, Druk sejmowy nr 409.

[10] M. Młotek, M. Siedlarz, *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego” 2011, nr 4, s. 158 i n.

fikcji z uwagi na brak możliwości technicznych. Metody oszukańczych praktyk wymierzonych przeciwko konsumentom i przedsiębiorcom stają się w konsekwencji coraz bardziej wyrafinowane i szkodliwe, a przy tym trudne do zwymiarowania, tak w aspekcie prawnym, kryminologicznym, jak i ekonomicznym. Prawdopodobieństwo stania się przedmiotem ataku cyberprzestępczego wydaje się zatem wysoce realne i dostrzegalne zarazem. Dane uzyskane w drodze Światowego Badania Bezpieczeństwa Informacyjnego przeprowadzonego wśród 1700 przedstawicieli kadry zarządzającej wyższego i średniego szczebla w 52 krajach świata wskazują, że aż 72% spośród nich zauważa wzrastający poziom ryzyka spowodowanego zagrożeniami zewnętrznymi. Z drugiej zaś strony np. jedynie co trzeci respondent zdecydował się dostosować własną strategię bezpieczeństwa informacji do technologii teleinformatycznych wdrażanych w ciągu ostatniego roku we własnej organizacji[11]. Aby zasygnalizować, jakie skutki pociągają za sobą tego typu zagrożenia w skali ogólnoświatowej, wystarczy przytoczyć szacunki dokonane przy okazji ostatnich cyberataków na infrastrukturę krytyczną instytucji rządowych w Polsce, które miały miejsce w styczniu 2012 r. w związku z planami ratyfikacji konwencji ACTA, mającej na celu wprowadzenie mechanizmów międzynarodowej ochrony praw autorskich. Wskazują one na konieczność przeznaczenia przez krajowe instytucje państwowe, przedsiębiorców i prywatnych użytkowników sieci aż 50 mld złotych w okresie następnych 5 lat[12]. Świadczy to z pewnością o istnieniu nie tylko jedynie potencjalnie niebezpiecznego, ale i wymiernego ekonomicznie wpływu zjawiska cyberprzestępczości na rozwój gospodarki elektronicznej.

Literatura

1. Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary – Automatyka – Kontrola" 2009, nr 7.
2. Czyżak M., *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010, nr 1-2.
3. Gibson W., *Neuromancer*, Wydawnictwo Książnica, Katowice 2011.
4. Jaślan M., *Raport o zagrożeniach z mediów społecznościowych i cloud computing*, http://www.forumszerokopasmowe.pl.
5. Młotek M., Siedlarz M., *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 4.
6. *Raport Ernst & Young, Eksperci: Polska nie ma strategii na wypadek cyberataku*, „Rzeczpospolita" 28–29.01.2012.

[11] M. Jaślan, *Raport o zagrożeniach z mediów społecznościowych i cloud computing*, http://www.forumszerokopasmowe.pl.

[12] *Raport Ernst & Young, Eksperci: Polska nie ma strategii na wypadek cyberataku*, „Rzeczpospolita" 28–29.01.2012, s. A5.

7. Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm – nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Warszawa 2009.
8. Wójcik J.W., *Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne*, w: *Cyberterroryzm – nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Warszawa 2009.
9. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (DzU 1997, nr 88, poz. 553, ze zm.).
10. Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU 2010, nr 46, poz. 276, ze zm.).
11. Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (DzU 2002, nr 126, poz. 1068, ze zm.).
12. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (DzU 2002, nr 144, poz. 1204, ze zm.).
13. Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (DzU 2002, nr 169, poz. 1385, ze zm.).
14. *Uzasadnienie do projektu ustawy o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym*, Sejm RP IV kadencji, Druk sejmowy nr 353.
15. *Uzasadnienie do projektu ustawy o świadczeniu usług drogą elektroniczną*, Sejm RP IV kadencji, Druk sejmowy nr 409.
16. *Założenia Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011*, http://cert.gov.pl.
17. www.statystyka.policja.pl.

THE CYBERCRIMINALITY PHENOMENON AS THE DETERMINANT OF ELECTRONIC ECONOMY DEVELOPMENT

Summary

The article presents the cybercriminality as a danger for the electronic economy. It presents definition and different forms of this phenomenon. Furthermore, the paper indicates the essential actions undertaken in this area by the entrepreneurs, legislature and different authorities of legal protection. The author concludes, that the influence exerted by this kind of criminality on electronic economy is negative and very difficult to quantify.

Translated by Mariusz Czyżak