Małgorzata WRÓBEL

CYBERPRZESTĘPCZOŚĆ W POLSKIM SYSTEMIE PRAWNYM

Słowa kluczowe: cyberprzestępczość, cyberterroryzm, ochrona cyberprzestrzeni, bezpieczeństwo cybernetyczne, system prawny.

STRESZCZENIE

W artykule zostały poruszone kwestie uregulowania zjawiska cyberprzestępczości w polskim systemie prawnym. Autorka ukazała aktualne problemy związane z uporządkowaniem legislacyjnym dotyczącym czynów zabronionych w cyberprzestrzeni oraz propozycje ich rozwiązania.

Zagrożenia bezpieczeństwa cybernetycznego

XX i XXI wiek to okres ogromnego postępu cywilizacyjnego, który jest szczególnie dostrzegalny w rozwoju nowoczesnych technologii, służących człowiekowi do ułatwienia wielu życiowych procesów i działań. Jednakże narzędzia takie jak Internet, komputer czy telefon komórkowy, stały się niebezpieczną bronią w rękach przestępców. W obliczu globalizacji zapewnienie bezpieczeństwa cyberprzestrzeni to jeden z podstawowych celów każdego podmiotu międzynarodowego. Priorytetowym zadaniem dla państw jest stworzenie mechanizmów pozwalających na skuteczne przeciwdziałanie cyberprzestępczości. Aktualne uregulowanie prawne kwestii cyberprzestępczości w Polsce jest niewystarczające. Wprowadzenie odpowiednich zmian legislacyjnych, zaproponowanych w poniższym artykule spowodowałoby usprawnienie zapobiegania, reagowania i ścigania przestępczości w cyberprzestrzeni.

Zgodnie z prognozami współcześnie wzrasta poziom zagrożenia cyberprzestępczością, w tym cyberterroryzmem. Rzeczywiste rozmiary przestępczości w cyberprzestrzeni są trudne do określenia. Podejmowane próby oszacowania obejmują jedynie straty materialne poniesione w krótkim czasie. Sprawcy tych przestępstw zazwyczaj działają długoterminowo, a ich aktywność powoduje również znaczne szkody niematerialne.

Według Białej Księgi Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[1] opublikowanej 24 maja 2013 roku w przyszłości zagrożenie cyberprzestępczością będzie się nieustannie zwiększać. Ataki cybernetyczne mogą zostać przeprowadzone zarówno przez władze i służby państw wrogich, gotowych wypowiedzieć wojnę informacyjną, jak też przez wielkie koncerny, organizacje o charakterze pozarządowym i ponadnarodowym, w tym przestępcze, grupy aktywistów, nieformalne grupy użytkowników Internetu, a nawet indywidualnych użytkowników. Cyberprzestępczość może mieć podłoże ideologiczne, polityczne, religijne oraz biznesowe. Potencjalnym zagrożeniem w najbliższej przyszłości mogą być ataki cybernetyczne, wymierzone przede wszystkim w elementy infrastruktury krytycznej, które posłużą jako narzędzie szantażu dla przestępczości zorganizowanej. Duża trudność w udowodnieniu takich ataków sprzyja wykorzystaniu ich do osiągnięcia swoich celów. Dynamiczny rozwój technologiczny przyczyni się do powstawania i rozpowszechniania nowych technik oraz metod ataków, a tradycyjne zagrożenia przeniosą się do cyberprzestrzeni (jak np. cyberprotesty czy cyberdemonstracje)[2].

Na podstawie statystyk prowadzonych przez polską Policję można dojść do wniosku, iż z roku na rok rośnie w naszym kraju liczba przestępstw popełnianych w sieci, w szczególności dotyczy to różnych rodzajów oszustw. Coraz większa liczba użytkowników komputerów i podmiotów oferujących w sieci towary i usługi, ma odzwierciedlenie w zwiększającej się liczbie cyberprzestępstw. Poniższa tabela ukazuje te zależności.

Tabela 1. Przestępstwa popełniane w sieci w latach 2005-2010

Rok	Wszystkie przestępstwa ogółem	– w tym oszustwa
2005	3 445	2 804
2006	3 922	3 597
2007	7 467	5 787

[1] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (BKBN RP) – opublikowana 24. 05. 2013 roku, dokument prezentujący prace Strategicznego Przeglądu Bezpieczeństwa Narodowego, utworzony głównie na podstawie Raportu Komisji SPBN oceniającego stan bezpieczeństwa narodowego oraz ukazujący strategiczne wnioski dotyczące kierunków i sposobów prowadzenia polityki bezpieczeństwa RP. Celem Białej Księgi jest pogłębienie wiedzy i świadomości społecznej dotyczącej bezpieczeństwa Polski i jej obywateli. Źródło: http://www.spbn.gov.pl/ (dostęp 05.06.2013).

[2] Tamże, s. 116-117.

cd. tabeli 1

Rok	Wszystkie przestępstwa ogółem	– w tym oszustwa
2008	4 015	2 848
2009	6 124	4 915
2010	7 733	6 260

Źródło: http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html (dostęp 05.06.2013).

Ogromną wagę problemu potwierdzają również ataki na zasoby instytucji administracji państwowej z 21-25 stycznia 2012 roku w ramach akcji protestacyjnych przeciw podpisaniu przez Polskę porozumienia ACTA. Ataki te ukazały, iż państwo nie zapewniło odpowiedniej ochrony cyberprzestrzeni oraz nie wypracowało właściwych narzędzi, dzięki którym można zapobiegać takim incydentom. Wydarzenia te potwierdziły również nieprzewidywalność współczesnych zagrożeń związanych z cyberprzestępczością oraz konieczność utworzenia efektywnego systemu zapobiegania przestępstwom komputerowym.

Poniższa tabela ukazuje stan bezpieczeństwa stron internetowych administracji państwowej w 2012 roku. Jak wynika z badania przeprowadzonego przez Zespół CERT Polska[3] przeważająca część witryn nie posiada wystarczających zabezpieczeń.

Tabela 2. Stan bezpieczeństwa witryn administracji publicznej

Stan bezpieczeństwa przebadanych witryn	Ilość stron
Bardzo dobry poziom bezpieczeństwa	24
Średni poziom bezpieczeństwa	24
Niski poziom bezpieczeństwa	19

Źródło: Raport o stanie cyberprzestrzeni RP w 2012 roku, Warszawa 2013, s. 15, źródło: http://www.cert.gov.pl/ (dostęp 31.05.2013).

[3] Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL – funkcjonuje od 1 lutego 2008 roku. Podstawowym zadaniem zespołu jest wsparcie jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej w zakresie ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

Na podstawie przedstawionych powyżej statystyk można stwierdzić, iż aktualny stan bezpieczeństwa cybernetycznego Polski znajduje się na niskim poziomie.

Uregulowanie prawne cyberprzestępczości w polskim systemie prawnym

Jednym z głównych działań, jakie należy podjąć w celu budowy skutecznej ochrony cyberprzestrzeni naszego kraju jest wprowadzenie zmian w systemie prawnym, aby zawierał ogół regulacji, związanych z przestępstwami w cyberprzestrzeni.

W polskim prawie nie opracowano jednoznacznej definicji cyberprzestępczości. Brak sformułowania podstawowego pojęcia może powodować problemy z klasyfikacją danego przestępstwa. Ponadto samo określenie czym jest cyberprzestępczość przynosi wiele trudności ze względu na różnorodność definicji tego zjawiska.

Szczególną uwagę należy zwrócić na definicję cyberprzestępstwa opracowaną przez X Kongres ONZ w sprawie Zapobiegania Przestępczości i Traktowania Przestępców. Stwierdzono, iż cyberprzestępstwo to:

- w wąskim sensie (przestępstwo komputerowe) – wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub poddawanych procesom przez te systemy danych.
- w szerokim sensie (przestępstwo dotyczące komputerów) – wszelkie nielegalne działanie, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to m.in. nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[4].

Natomiast Komisja Wspólnot Europejskich w 2007 roku w komunikacie „W kierunku ogólnej strategii zwalczania cyberprzestępczości" określiła, iż pojęcie cyberprzestępczości obejmuje trzy rodzaje przestępstw. Pierwszy to tradycyjne formy przestępstw, takie jak oszustwo czy fałszerstwo, jednakże popełnione przy użyciu elektronicznych sieci informatycznych i systemów informatycznych (zwanych dalej sieciami łączności elektronicznej). Drugi rodzaj to publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci oraz nawoływaniem do nienawiści rasowej). Trzeci rodzaj odnosi

[4] Projekt wymiany doświadczeń pomiędzy: Komendą Wojewódzką Policji we Wrocławiu a Inspektoratem Głównym Policji Rumuńskiej w Bukareszcie, Wymiana doświadczeń w zakresie przestępczości w obiegu elektronicznymi środkami płatniczymi, źródło: http://www.kujawsko-pomorska.policja.gov.pl (dostęp 31.05.2013).

się do przestępstw typowych dla sieci łączności elektronicznej, takich jak ataki przeciwko systemom informatycznym, ataki typu denial of service oraz hakerstwo[5].

Powyższe definicje wskazują na to, że cyberprzestępczość będzie związana jedynie z systemem komputerowym i dokonana przy użyciu komputera.

Program Rządowej Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 rozszerza pojęcie cyberprzestępstwa, uwzględniając, iż przestępstwa tego typu mogą być popełnione za pomocą systemów i sieci teleinformatycznych[6].

Klasyfikacja cyberprzestępstw również jest kwestią problematyczną ze względu na dynamiczny rozwój nowoczesnych technologii. Wraz z postępem lista przestępstw ulega ciągłym zmianom.

Według P. Neumanna i D. Pakera do cyberprzestępczości zaliczamy takie działania jak:

- External Information Theft – przeglądanie oraz kradzież informacji przez osobę spoza systemu,
- External Abuse of Resources – zniszczenie twardego dysku,
- Pest Programs – zainstalowanie złośliwego programu,
- Bypassins Authentication or Authority – złamanie haseł,
- Authority Abuse – fałszowanie danych,
- Abuse Through Inaction – celowe prowadzenie złego zarządzania,
- Indirect Abuse – używanie innych systemów do stworzenia „złośliwych" programów[7].

Inny podział zaproponował U. Sieber, który uznał, że cyberprzestępstwa to:

- przestępstwa w dziedzinie ochrony danych (naruszenie praw jednostki),
- przestępstwa gospodarcze z użyciem komputerów,
- manipulacje komputerowe: operacje rozrachunkowe, manipulacje bilansowe, manipulowanie stanem kont bankowych, nadużycia kart do bankomatów oraz innych środków płatniczych, nadużycia telekomunikacyjne,
- sabotaż i szantaż komputerowy,
- hacking komputerowy,
- szpiegostwo komputerowe,

---

[5] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, *W kierunku ogólnej strategii zwalczania cyberprzestępczości*, Bruksela 2007, źródło: http://eur-lex.europa.eu/ (dostęp 31.05.2013).

[6] *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, Warszawa 2010, s. 6, źródło: http://bip.msw.gov.pl/portal/bip/6/19057 (dostęp 05.06.2013).

[7] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1(160), s. 181-182.

- kradzieże software oraz inne formy piractwa dotyczące produktów przemysłu komputerowego.

Inne rodzaje przestępstw:

a) rozpowszechnianie za pomocą komputerów informacji pochwalających użycie przemocy, rasistowskich i pornograficznych,
b) użycie techniki komputerowej w tradycyjnych rodzajach przestępstw[8].

Na stronie internetowej polskiej Policji znajdziemy natomiast następującą klasyfikację:

1. Przestępstwa komputerowe:
   - Hacking komputerowy,
   - Podsłuch komputerowy,
   - Sabotaż komputerowy,
   - Szpiegostwo komputerowe,
   - Bezprawne niszczenie informacji,
   - Zakłócenie automatycznego przetwarzania informacji związane za sprowadzeniem niebezpieczeństwa powszechnego,
   - Fałszerstwo komputerowe,
   - Oszustwo komputerowe,
   - Kradzież programu komputerowego.

2. Przestępstwa telekomunikacyjne:
   - Oszustwo telekomunikacyjne,
   - Klonowanie numerów IMEI telefonów komórkowych,
   - Kradzież impulsów telefonicznych,
   - Nielegalne współdzielenie łączy,
   - Doładowanie kart telefonicznych (magnetycznych i chipowych) i kart pre-paid,
   - Przełamania centrali telefonicznych.

3. Przestępstwa internetowe
   - Podmiana zawartości stron WWW,
   - Nieuprawniony dostęp do zawartości skrzynek pocztowych i późniejszym wykorzystaniu w działaniach przestępczych,

[8] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8, s. 242.

- Blokowanie usług sieciowych oraz komputerów poprzez przesyłanie setek tysięcy pakietów IP lub listów e-mail,
- Nielegalne rozpowszechnianie i sprzedaż za pośrednictwem Internetu utworów muzycznych, filmów oraz oprogramowania (www, ftp, p2p, p2m),
- Nielegalny handel lekami, anabolikami i sterydami,
- Gry losowe i zakłady wzajemne prowadzone za pośrednictwem Internetu,
- Handel przedmiotami, których posiadanie jest zabronione lub pochodzącymi z przestępstwa,
- Internetowe oszustwa aukcyjne[9].

W polskim systemie prawnym nie wypracowano jednego aktu prawnego określającego jakie przestępstwa zaliczamy do cyberprzestępczości i w jaki sposób będą one sankcjonowane. Do podstawowych aktów prawnych, które zawierają regulacje odnoszące się do cyberprzestępczości należą:

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 nr 78 poz. 483).
- Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. 1997 nr 88 poz. 553).
- Ustawa z dnia 23 kwietnia 1964 r. *Kodeks postępowania cywilnego* (Dz. U. 1964 nr 43 poz. 296).
- Ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz. U. 2004 nr 171 poz. 1800).
- Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz. U. 1994 nr 24 poz. 83).
- Ustawa z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu* (Dz. U. 2002 nr 74 poz. 676).
- Ustawa z dnia 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego* (Dz. U. 2006 nr 104 poz. 709).
- Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. 2007 nr 89 poz. 590).
- Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. 2005 nr 64 poz. 565).
- Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. 2010 nr 182 poz. 1228).
- Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. 1997 nr 133 poz. 883).

[9] Źródło: http://www.policja.pl/portal/pol/1218/2960/Cyberprzestepczosc.html (dostęp 31.01.2013).

- Ustawa z dnia 27 lipca 2001 r. *o ochronie baz danych* (Dz. U. 2001 nr 128 poz. 1402).
- Ustawa z dnia 29 sierpnia 1997 r. *Prawo bankowe* (Dz. U. 1997 nr 140 poz. 939).
- Ustawa z dnia 5 lipca 2002 r. *o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym* (Dz. U. 2002 nr 126 poz. 1068).
- Ustawa z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* (Dz. U. 2002 nr 144 poz. 1204).
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego* (Dz. U. 2005 nr 171 poz. 1433).
- Rozporządzenie Rady Ministrów z dnia 28 marca 2007 r. *w sprawie Planu Informatyzacji Państwa na lata 2007-2010* (Dz. U. 2007 nr 61 poz. 415).
- Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. *w sprawie minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. 2005 nr 212 poz. 1766).
- Decyzja Ministra Obrony Narodowej nr 357/MON z dnia 29 lipca 2008 roku *w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony narodowej* (Dz. Urz. MON Nr 16, poz. 205)[10].

Powyższe akty prawne regulują poszczególne aspekty związane z funkcjonowaniem danego sektora. Ponadto Polska jest stroną konwencji międzynarodowych, które również mają istotne wpływ na bezpieczeństwo cybernetyczne naszego kraju. Można wymieć takie jak:

- Konwencja Rady Europy *o zwalczaniu terroryzmu* z dnia 27 stycznia 1977 r.,
- Konwencja *o zwalczaniu cyberprzestępczości RE* z dnia 23 listopada 2001 r.,
- Konwencja Rady Europy *o zapobieganiu terroryzmowi*, sporządzoną w dniu 16 maja 2005 r.,
- Program Sztokholmski,
- Strategia i Plan działania w dziedzinie zwalczania terroryzmu,
- Europejska Agenda Cyfrowa Rady Europejskiej[11].

Do prawnie wyznaczonych podmiotów, które są odpowiedzialne za bezpieczeństwo cyberprzestrzeni należą:

- Kancelaria Prezesa Rady Ministrów,
- Ministerstwo Spraw Wewnętrznych,
- Ministerstwo Obrony Narodowej,

[10] *Rządowy Program Ochrony…*, dz. cyt., s. 9-10.

[11] Tamże, s. 10-11.

- Ministerstwo Administracji i Cyfryzacji,
- Ministerstwo Edukacji Narodowej,
- Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej,
- Ministerstwo Nauki i Szkolnictwa Wyższego,
- Rządowe Centrum Bezpieczeństwa,
- Agencja Bezpieczeństwa Wewnętrznego,
- Służba Kontrwywiadu Wojskowego,
- Komenda Główna Policji,
- Komenda Główna Straży Granicznej,
- Komenda Główna Państwowej Straży Pożarnej,
- Naukowa i Akademicka Sieć Komputerowa – Zespół CERT Polska,
- Przedsiębiorcy telekomunikacyjni, posiadający własną infrastrukturę telekomunikacyjną[12].

W najszerszym zakresie kwestie cyberprzestępczości reguluje ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. 1997 nr 88 poz. 553). Na jego podstawie można wyodrębnić czyny zabronione w cyberprzestrzeni.

W art. 130 § 3 kk zawarta jest regulacja dotycząca szpiegostwa przy pomocy systemu informatycznego. Zgodnie z tym artykułem *Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2, gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8*[13]." Przepis ten reguluje kwestie związane z działalnością szpiegowską odnoszącą się do bezpieczeństwa całego kraju.

Istotnym przestępstwem związanym z użyciem systemu informatycznego jest spowodowanie powszechnego zagrożenia na skutek zakłócenia procesów przetwarzania danych. Czyn ten określa art. 165 § 1 kk *Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach:*

1) *powodując zagrożenie epidemiologiczne lub szerzenie się choroby zakaźnej albo zarazy zwierzęcej lub roślinnej,*
2) *wyrabiając lub wprowadzając do obrotu szkodliwe dla zdrowia substancje, środki spożywcze lub inne artykuły powszechnego użytku lub też środki farmaceutyczne nie odpowiadające obowiązującym warunkom jakości,*
3) *powodując uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności urządzenia dostarczającego wodę, światło, ciepło, gaz, ener-*

[12] Tamże, s. 12.

[13] Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*…, art. 130.

gię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia,

4) *zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych,*
5) *działając w inny sposób w okolicznościach szczególnie niebezpiecznych*[14].

Zgodnie z tym przepisem, karze podlega przede wszystkim zakłócenie funkcjonowania urządzeń użyteczności publicznej lub urządzeń ochronnych, których nieprawidłowe działanie może spowodować niebezpieczeństwo dla społeczeństwa. Czyn uregulowany w art. 165 dotyczy również ataków cyberterrorystycznych, wymierzonych zazwyczaj w bezbronnych obywateli.

Na podstawie Rozdziału XXXIII Kodeksu karnego, który dotyczy przestępstw przeciw ochronie informacji można wymienić takie czyny zabronione w cyberprzestrzeni jak:

- Hacking rozumiany jako bezprawne wejście do systemu komputera w celu kradzieży jego czasu pracy i informacji. Jest regulowany przez art. 267 kk i zgodnie z jego treścią *[…] karze podlega, kto bez uprawienia uzyskuje dostęp do całości lub części systemu informatycznego*[15]. Za pomocą tego przepisu ustanowiono karalność czynu polegającego na zdobyciu bez uprawnienia dostępu do systemu informatycznego lub jego części, nawet bez złamania jakichkolwiek zabezpieczeń.
- Podsłuch lub inwigilacja określone jako nieuprawnione przechwytywanie informacji przy użyciu urządzeń podsłuchowych oraz wizualnych oraz innych urządzeń lub oprogramowania-uregulowane również przez art. 267 kk[16]. Właściwym rozwiązaniem jest szerokie ujęcie urządzeń, za pomocą których można dokonać podsłuchu lub inwigilacji, gdyż w przyszłości prawdopodobnie pojawią się nieznane aktualnie możliwości techniczne podsłuchiwania.
- Sabotaż komputerowy rozumiany jako naruszenie integralności komputerowego zapisu informacji poprzez zniszczenie, uszkodzenie, usunięcie lub zmianę zapisu informacji, utrudnianie zapoznania się z informacją, zakłócanie lub uniemożliwianie przetwarzania, gromadzenia i przekazywania informacji, zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej lub urządzenia służącego automatycznemu przetwarzaniu, gromadzeniu oraz przesyłaniu informacji, zniszczenie lub wymianę nośnika informacji i urządzenia do przechowywania informacji. Przestępstwo to określone zostało w art.

[14] Art. 165 kk, s. 50.
[15] Art. 267 kk, s. 79.
[16] Tamże.

268-269b kk[17]. Dodatkowo art. 269 b kk odnosi się do urządzeń oraz oprogramowania, za pomocą których dokonuje się sabotażu komputerowego. Karze podlega osoba wytwarzająca, pozyskująca, sprzedająca lub udostępniająca tego typu narzędzia. Szczególnie istotnym dla bezpieczeństwa całego państwa jest art. 269 § 1 kk zgodnie z którym *Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych*[18]. Zgodnie z propozycją D. Habrata właściwe wydaje się uzupełnienie tego artykułu o przestępstwa związane z naruszeniem integralności systemu finansowego, gdyż współczesne bezpieczeństwo ekonomiczne kraju jest w znacznym stopniu zależne od systemów oraz sieci komputerowych i atak na nie może skutkować dużymi stratami finansowymi[19].

W Rozdziale XXXV Kodeksu karnego uregulowano przestępstwa przeciwko mieniu, również te, które związane są z cyberprzestępczością. Wymienione zostały takie przestępstwa jak:

- kradzież programu komputerowego,
- kradzież karty bankomatowej,
- oszustwo telekomunikacyjne,
- oszustwo komputerowe,
- paserstwo programu komputerowego[20].

Art. 278 kk reguluje kwestie kradzieży programu komputerowego oraz karty bankomatowej. Zgodnie z treścią przepisu karze podlega *[…] kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej (…) § 5. Przepisy § 1, 3 i 4 stosuje się odpowiednio do kradzieży energii lub karty uprawniającej do podjęcia pieniędzy z automatu bankowego*[21].

Oszustwo telekomunikacyjne określono w art. 285 kk, zgodnie z którym czyn ten popełnia ten kto włącza się do urządzenia telekomunikacyjnego i uruchamia na cudzy rachunek impulsy telefoniczne[22].

---

[17] *Projekt wymiany doświadczeń…*, dz. cyt., s. 16-17.

[18] Art. 269 kk, s. 80.

[19] A. Sucharzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 227-228.

[20] Projekt wymiany doświadczeń…, dz. cyt., s. 17-18.

[21] Art. 278 kk, s. 82.

[22] Art. 285 kk, s. 83.

Oszustwa komputerowego dopuszcza się natomiast ten *Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych*[23].

Powyższe czyny powszechnie nazywają się piractwem komputerowym. Piractwo w Polsce jest nadal znaczącym problemem ze względu na powszechne przyzwolenie oraz brak świadomości prawnej w społeczeństwie.

W Kodeksie karnym uregulowano także kwestie podszywania się pod inną osobę oraz tworzenia fałszywych profili. Według art. 190 a kk § 2 *Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej*[24].

Do cyberprzestępstw zalicza się również rozpowszechnianie treści faszystowskich oraz propagujących inny totalitarny system. Zgodnie z art. 256 kk karze podlega osoba, która nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych lub ze względu na bezwyznaniowość oraz w tym celu rozpowszechniania produkuje, utrwala lub sprowadza, nabywa, przechowuje, posiada, prezentuje, przewozi lub przesyła druk, nagranie lub inny przedmiot[25]. Aktualnie wiele grup terrorystycznych wykorzystuje sieci i systemy teleinformatyczne do popularyzowania swoich poglądów oraz prezentowania sposobów walki z wrogiem, jak też do werbowania nowych członków. Internet wykorzystany w taki sposób staje się niebezpiecznym narzędziem w rękach terrorystów. W polskim prawie nie uregulowano problematyki rozpowszechniania taktyki walki i pozyskiwania nowych działaczy przez takie ugrupowania. Słusznym wydaje się uzupełnienie art. 256 kk o tego typu przestępstwa.

W Kodeksie karnym uregulowano również kwestie związane z materiałami pornograficznymi. W myśl art. 202 § 1 i § 2 *Kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jednocześnie, kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*[26]. Artykuł 202 reguluje także kwestię pornografii dziecięcej. Według Kodeksu karnego karze podlega *ten kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub publicznie prezentuje treści pornograficzne z udziałem mało-*

[23] Art. 287 kk, s. 84.
[24] Art. 190 kk, s. 57.
[25] Art. 256 kk, s. 76.
[26] Art. 202 kk, s. 60.

letniego[27]. Istotną zmianą jaka powinna zostać wprowadzona do tego przepisu jest podwyższenie granicy wieku ochrony małoletnich do 18 lat[28]. W prawie polskim nie określono również czy samo wyświetlanie pornografii dziecięcej lub usunięcie pliku o takiej treści oznacza jej posiadanie. W momencie wyświetlenia danego pliku za pomocą sieci na komputerze zapisywane są pliki tymczasowe, które mogą świadczyć o posiadaniu danego pliku. Natomiast usunięty wcześniej plik można w prosty sposób przywrócić.

W Rozdziale XXXIV zostały przedstawione przestępstwa przeciwko wiarygodności dokumentów. Artykuł 270 § 1 kk reguluje kwestie fałszerstwa dokumentów[29]. Zgodnie z przepisem karze podlega każda ingerencja w treść dokumentu, w tym dokumentu elektronicznego, obejmująca jego podrobienie lub przerobienie przez osobę do tego nieuprawnioną i działającą w zamiarze bezpośrednim posłużenia się tym dokumentem. Niestety ustawodawca nie określa z pomocą jakich narzędzi dokumenty mogą zostać sfałszowane, a w obliczu ogromnego postępu technologicznego służą do tego przede wszystkim komputery.

W obliczu zagrożeń związanych z cyberprzestępczością priorytetową kwestią jest ochrona ważnych dla państwa informacji, które mogą zostać użyte przez osoby do tego nieuprawnione. Ochrona informacji niejawnych należy do najistotniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa. Obecnie rośnie znaczenie bezpieczeństwa informacyjnego. Szczególną jego dziedziną jest ochrona informacji niejawnych, których nieuprawnione ujawnienie mogłoby doprowadzić do szkody dla Polski lub byłoby niekorzystne dla jej interesów[30]. Ustawa o ochronie informacji niejawnych reguluje kto i na jakich zasadach posiada dostęp do istotnych informacji państwowych. Rozwój nowoczesnych technologii oraz rozpowszechnienie komunikacji elektronicznej spowodowały, iż tajne informacje są coraz częściej wytwarzane, przechowywane, przetwarzane i przekazywane za pomocą systemów oraz sieci teleinformatycznych. W konsekwencji doprowadziło to do znacznego zagrożenia dla tych informacji, w szczególności cyberprzestępczością. Zgodnie z art. 48 ustawy z dnia 5 sierpnia 2010 r. *o informacjach niejawnych* (Dz. U. 2010 nr 182 poz. 1228) systemy, które wykorzystywane są do wytwarzania, przechowywania, przetwarzania i przekazywania informacji niejawnych, muszą posiadać akredytację bezpieczeństwa teleinformatycznego przez służby ochrony państwa. Dostęp do tych systemów i odpowiedzialność za ich bezpieczeństwo posiadają również

[27] Tamże.

[28] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, s. 53.

[29] Art. 270 kk, s. 80-81.

[30] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, dz. cyt., s. 171.

jedynie wyznaczone do tego odpowiednio przeszkolone osoby[31]. Z punktu widzenia bezpieczeństwa obywatela ważną rolę spełnia ochrona danych osobowych. We współczesnym społeczeństwie to właśnie informacja jest najcenniejszym zasobem i osoba nieuprawniona do posiadania danej informacji może nieodpowiednio ją wykorzystać, np. do dokonania przestępstwa. W rozdziale 5 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. 1997 nr 133 poz. 883) uregulowano kwestie związane z zabezpieczeniem danych osobowych w systemach i sieciach teleinformatycznych. Odpowiednia ochrona danych ma polegać na wdrożeniu i eksploatacji stosownych środków technicznych i organizacyjnych, pozwalających na zapobieganie nieuprawnionemu przetwarzaniu danych. Za zabezpieczenie danych odpowiada administrator. Zadania, które są na niego nałożone ujęto dość szeroko i ogólnie. Zgodnie z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem*[32]. Właściwym wydaje się ogólne określenie zasad zabezpieczania sieci i systemów teleinformatycznych w ustawie, gdyż pozwala to na dostosowanie się do aktualnego stanu wiedzy i rozwoju technologicznego.

W polskim systemie prawnym uregulowano także problematykę ochrony praw autorskich. Według art. 116. ustawy z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz. U. 1994 nr 24 poz. 83), karze podlega ten Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie[33]. W art. 117 powyższej ustawy za przestępstwo uznano również utrwalanie oraz zwielokrotnianie cudzego utworu bez uprawnienia lub wbrew jego warunkom. Natomiast zgodnie z art. 118 karze podlega ten *Kto w celu osiągnięcia korzyści majątkowej przedmiot będący nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnionego bez uprawnienia albo wbrew jego warunkom nabywa lub pomaga w jego zbyciu albo przedmiot ten przyjmuje lub pomaga w jego ukryciu*[34].

---

[31] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 nr 182 poz. 1228), art. 48, s. 34-36, źródło: http://isap.sejm.gov.pl/ (dostęp 05.06.2013).

[32] Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych…*, art. 36.

[33] Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych…*, art. 116.

[34] Tamże, art. 118.

Znaczącym problemem związanym z uregulowaniem kwestii cyberprzestępczości w polskim systemie prawnym jest niezgodność pomiędzy terminologią prawną a informatyczną. Rzadko możemy spotkać się z nazwami specjalistycznymi, które umożliwiłyby klasyfikację oraz karalność cyberprzestępczości. Ponadto prawo nie jest dostosowane do postępu technologicznego.

W czerwcu 2010 roku został przyjęty *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, w którym przedstawiono plan zmian legislacyjnych. Założono takie działania jak:

- *zdefiniowanie pojęć dotyczących cyberprzestrzeni – cyberprzestępczości, cyberterroryzmu, cyberprzestrzeni RP,*
- *wskazania, że cyberprzestrzeń RP należy traktować, jako dobro ogólne umożliwiające rozwój i niezakłócone funkcjonowanie społeczeństwa informacyjnego, komunikację – wymianę informacji oraz repozytorium wiedzy,*
- *ustalenia odpowiedzialności za ochronę cyberprzestrzeni RP – opisanie zakresów zadań, odpowiedzialności i zmian w strukturach organizacyjnych (Prezes Rady Ministrów, MSWiA, MON w tym służby ochrony cyberprzestrzeni tj. ABW i SKW),*
- *wprowadzenie ścigania z urzędu naruszeń bezpieczeństwa w cyberprzestrzeni, które miały miejsce w odniesieniu do podmiotów administracji publicznej oraz infrastruktury krytycznej ujawnionej w wykazie. Wprowadzenie ścigania na wniosek pokrzywdzonego w przypadku wykrycia incydentu bezpieczeństwa w obszarze cyberprzestrzeni RP,*
- *ustanowienie głównych sektorowych punktów kontaktowych CERT.GOV.PL dla obszaru administracji publicznej, CERT POLSKA dla obszaru cywilnego, MIL CERT dla obszaru wojskowego oraz sektorowych punktów kontaktowych w ministerstwach właściwych dla danych sektorów gospodarki RP,*
- *wprowadzenie roli Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni RP oraz ustalenie sposobów i form współpracy,*
- *wprowadzenia funkcji pełnomocnika kierownika jednostki organizacyjnej ds. ochrony cyberprzestrzeni w podmiotach administracji publicznej i zalecenie utworzenia takiej roli u przedsiębiorców,*
- *umocowania prawnego Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL,*
- *wprowadzenia obowiązku dla podmiotów publicznych i zalecenia dla pozostałych użytkowników cyberprzestrzeni informowania (nie dłużej niż w ciągu jednego dnia od wykrycia zdarzenia przez personel) do właściwego zespołu CERT o wykrytych incydentach bezpieczeństwa związanych z cyberprzestrzenią RP*[35].

[35] *Rządowy Program Ochrony…*, dz. cyt., s. 15-16.

W Białej Księdze Bezpieczeństwa Narodowego RP podkreślono również priorytetowość utworzenia skutecznej ochrony cyberprzestrzeni naszego kraju. Wskazano, iż procedury i regulacje związane z wymianą informacji o sposobach oraz taktyce działania przestępców są niedoskonałe i niewystarczające. Na skutek czego opracowanie jednolitych metod wykrywania oraz monitorowania przestępstw w cyberprzestrzeni i przeciwdziałania im jest problematyczne, co przekłada się na trudność w odpowiednim przygotowaniu organów ścigania. Kolejnym znaczącym problemem jaki wymieniono w Białej Księdze jest rozproszenie odpowiedzialności za bezpieczeństwo teleinformatyczne i niewłaściwy przepływ informacji między podmiotami zobligowanymi do zajmowania się tymi zagadnieniami. Brak trwałego systemu koordynacji, procedur współpracy i wymiany informacji utrudnia, a niekiedy wręcz uniemożliwia skuteczne reagowanie na ataki wymierzone w systemy teleinformatyczne oraz oferowane przez nie usługi[36].

W dokumencie zaznaczono, że istotnym wkładem w zagwarantowanie bezpieczeństwa cyberprzestrzeni była nowelizacja w 2011 roku ustaw o stanach nadzwyczajnych, a w szczególności 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,* (Dz. U. 2002 nr 156 poz. 1301). W art. 2 ust. 1b wymienionej wyżej ustawy zdefiniowano pojęcie cyberprzestrzeni. Zgodnie z treścią artykułu *Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm. 1), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Dzięki wprowadzonym zmianom ujęto w ustawach wydarzenia w cyberprzestrzeni jako możliwe przesłanki do wprowadzania stanów nadzwyczajnych. Przyjęte rozwiązania przełożyły się na system funkcjonowania organów odpowiedzialnych za bezpieczeństwo narodowe i poszczególne jego segmenty. Tworzą one prawną podstawę do działań w zakresie planowania, przygotowywania oraz wdrażania konkretnych przedsięwzięć niezbędnych do eliminowania zagrożeń w cyberprzestrzeni. Ponadto nowelizacja ustaw otworzyła drogę dla kolejnych inicjatyw ustawodawczych[37].

W Białej Księdze przedstawiono również propozycje dokonania przeglądu i ewentualnej nowelizacji istniejących aktów prawnych, co do ich zgodności z unormowaniami innych krajów oraz organizacji międzynarodowych w celu ułatwienia współpracy międzynarodowej w zakresie ochrony cyberprzestrzeni oraz precyzyj-

[36] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, dz. cyt., s. 63-64.

[37] Tamże, s. 64.

nego określenia: racjonalności struktur, roli, zakresów kompetencji i odpowiedzialności, szczegółowych uprawnień, zasad wzajemnej współpracy i wymiany informacji w odniesieniu do poszczególnych organizacji, instytucji, jednostek organizacyjnych, organów i służb RP w zakresie prowadzenia działań w cyberprzestrzeni.

Konkluzje

Wobec rosnącego w szybkim tempie zagrożenia przestępczością w sieciach i systemach teleinformatycznych, zapewnienie bezpieczeństwa cyberprzestrzeni staje się kluczowym wyzwaniem dla podmiotów międzynarodowych. Do priorytetowych zadań naszego państwa należy natychmiastowe podjęcie kompleksowych działań w celu tworzenia mechanizmów zapobiegania, reagowania i ścigania cyberprzestępczości. Głównym elementem skutecznego systemu ochrony cyberprzestrzeni Polski jest system prawny, który obejmowałby ogół przepisów związanych z przestępstwami w cyberprzestrzeni. Aktualne regulacje dotyczące cyberprzestępczości są niewystarczające i wymagają wprowadzenia kluczowych zmian. Jednym z działań, jakie należy podjąć, jest ujednolicenie prawa w zakresie cyberprzestępczości, co umożliwiłoby ściganie takich przestępstw. Ponadto zdefiniowanie podstawowych pojęć, takich jak: cyberprzestępczość, cyberterroryzm oraz cyberprzestrzeń, umożliwiłoby odpowiednią klasyfikację przestępstw popełnionych w sieci. Kolejnym krokiem, jaki powinien zostać podjęty jest wprowadzenie zakresu zadań, odpowiedzialności i zmian w strukturach organizacyjnych służb, mających zapewnić bezpieczeństwo cybernetyczne.

Ze względu na przenoszenie się tradycyjnych zagrożeń do cyberprzestrzeni, można spodziewać się w najbliższej przyszłości wzrostu działalności ugrupowań terrorystycznych w sieciach i systemach teleinformatycznych. W związku z tym istotną kwestią jest wprowadzenie odpowiednich regulacji odnoszących się do tego typu przestępstw.

Zdaniem autorki zaproponowane w Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej działania legislacyjne w zakresie cyberprzestępczości, są niewystarczające. Brakuje istotnej kwestii dostosowania przepisów prawnych do terminologii informatycznej oraz do postępu technologicznego. Coraz częściej do dokonania cyberprzestępstwa wykorzystuje się urządzenia mobilne, takie jak np. telefony komórkowe, telefony VoIP i inne urządzenia posiadające dostęp do sieci, dlatego istotnym wydaje się uwzględnienie zmian jakie mogą nastąpić w przyszłości.

Właściwym wydaje się rozwiązanie zaproponowane w Białej Księdze Bezpieczeństwa Narodowego polegające na przeanalizowaniu wszystkich aktów prawnych związanych z cyberprzestępczością i dokonanie w nich odpowiednich zmian,

zgodnie z przyjętymi, w innych krajach oraz organizacjach międzynarodowych, regulacjami, co ułatwiłoby współpracę międzynarodową w tworzeniu bezpieczeństwa cyberprzestrzeni.

Należy mieć na uwadze, iż ze względu na ciągły rozwój technologiczny nie jest możliwe stworzenie idealnego systemu prawnego, który jako jeden z elementów systemu ochrony cyberprzestrzeni zapewniłby bezpieczeństwo cybernetyczne państwa. Ze względu na ten fakt, ustawodawca powinien uwzględnić i przewidzieć zmiany, jakie mogą nastąpić wraz z rozwojem nowych form cyberprzestępczości.

*****

Keywords: Cybercrime, cyber-terrorism, cyber protection, cyber security, the legal system.

SUMMARY

The article dealt with the issues of cybercrime legislation in the Polish legal system. The author presents the current problems associated with the ordering of legislation related to criminal acts in cyberspace as well as suggestions for their solution.

Bibliografia

Dokumenty:

1. Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013.
2. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, *W kierunku ogólnej strategii zwalczania cyberprzestępczości*, Bruksela 2007.
3. Projekt wymiany doświadczeń pomiędzy: Komendą Wojewódzką Policji we Wrocławiu a Inspektoratem Głównym Policji Rumuńskiej w Bukareszcie, Wymiana doświadczeń w zakresie przestępczości w obiegu elektronicznymi środkami płatniczymi, 2008.
4. Raport o stanie cyberprzestrzeni RP w 2012 roku, Warszawa 2013.
5. *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, Warszawa 2010.
6. Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz. U. 1994 nr 24 poz. 83).
7. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. 1997 nr 88 poz. 553).
8. Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. 2010 nr 182 poz. 1228).
9. Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. 1997 nr 133 poz. 883).

Monografie i artykuły:
1. Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001.
2. Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8.
3. Sucharzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
4. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1(160).

Źródła internetowe:
1. www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html
2. www.policja.pl/portal/pol/1218/2960/Cyberprzestepczosc.html