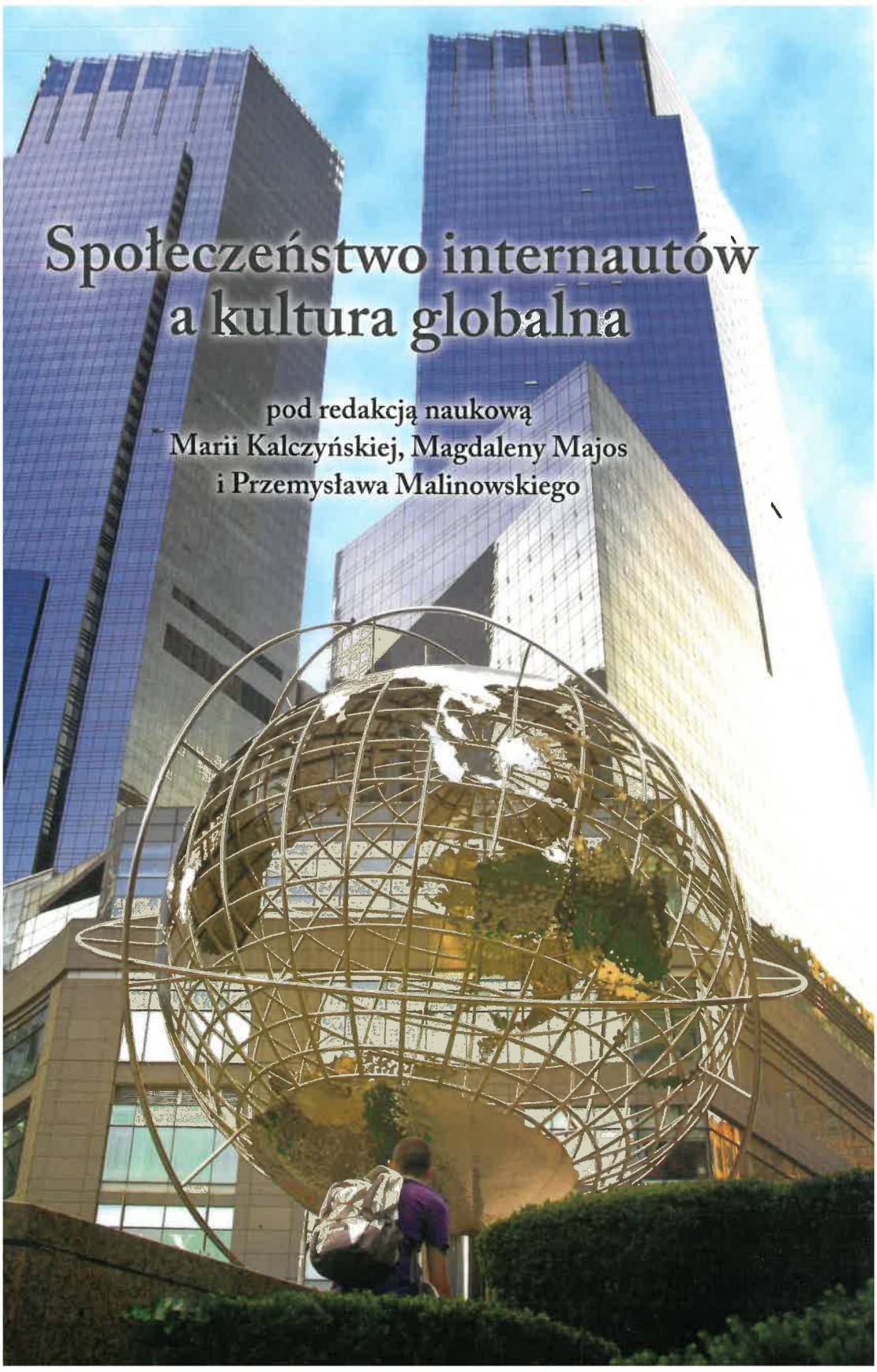
Społeczeństwo internautów a kultura globalna

pod redakcją naukową
Marii Kalczyńskiej, Magdaleny Majos
i Przemysława Malinowskiego



Społeczeństwo internautów a kultura globalna

Prawno-kulturowe aspekty funkcjonowania człowieka w wirtualnej rzeczywistości

pod redakcją naukową
Marii Kalczyńskiej, Magdaleny Majos
i Przemysława Malinowskiego

POLITECHNIKA OPOLSKA
OFICYNA WYDAWNICZA
Opole 2013 ISBN 978-83-64056-06-2

POLITECHNIKA OPOLSKA

Recenzenci:
prof. dr hab. Stanisław Malarski
prof. nadzw. dr hab. Anna Śliz
dr inż. Ewelina Piotrowska

Fotografie i oprawa edytorska:
M.J. Kalczyńska

Tłumaczenie na język angielski:
M. Majos

Komitet Redakcyjny Wydawnictw Politechniki Opolskiej
ul. Prószkowska 76

Skład: Oficyna Wydawnicza Politechniki Opolskiej
Nakład: 100 egz. Ark. wyd. 17,1. Ark. druk. 17,0.
Druk i oprawa: Sekcja Poligrafii Politechniki Opolskiej

Spis treści

Część III
Informatyczne aspekty funkcjonowania człowieka w wirtualnej rzeczywistości

Katarzyna Lechowicz
Uniwersytet Rzeszowski

Kontrowersje wokół zwalczania cyberprzestępczości

Wstęp

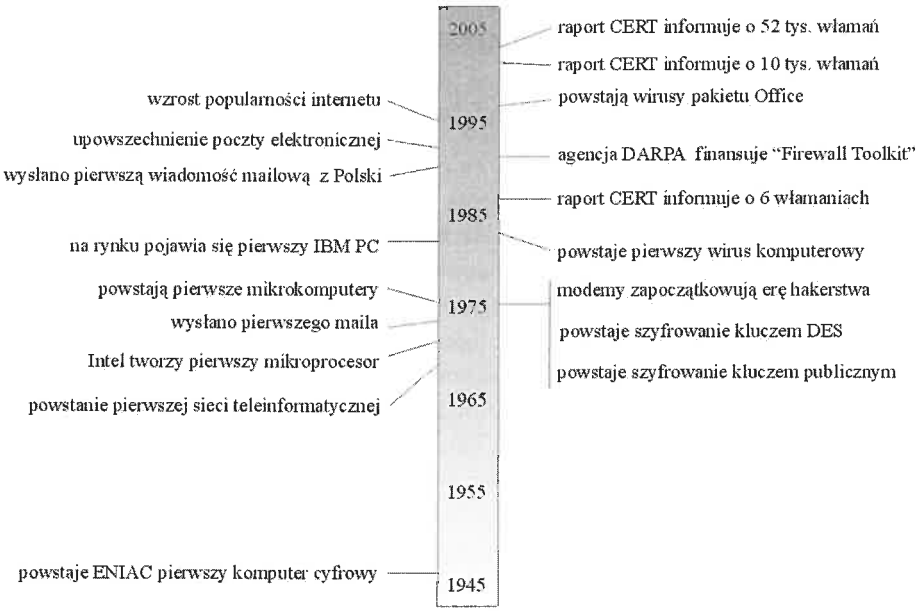
W XX wieku technologia informacyjna wkroczyła niemal do wszystkich dziedzin życia człowieka. Gwałtowny spadek kosztów gromadzenia, przechowywania i transferu informacji, jak również stosunkowo niski koszt produkcji elektroniki okazał się przełomowy. Dostęp do systemów ICT (Information and Communication Technologies) zyskał charakter globalny i masowy. Zmianie uległa także forma popełniania przestępstw. Przestępczość zorganizowana rozszerzyła działalność na cyberprzestrzeń. Ataków na systemy informatyczne jest każdego roku coraz więcej. Wykorzystywane są w tym celu coraz bardziej zaawansowane technologie. Nadużycia popełniane przy pomocy nowoczesnych technologii teleinformatycznych tworzą konkretne zagrożenia, które godzą w interesy zarówno jednostkowe, jak i zbiorowe. W konsekwencji prowadzić mogą do poważnych zakłóceń związanych z funkcjonowaniem całych społeczeństw.

Założeniem przedmiotowego opracowania jest próba charakterystyki współczesnych nadużyć związanych z technologią informacyjną. Analiza dostępnych statystyk umożliwia ocenę skali i specyfikę występujących zjawisk. Autor przedstawia wybrane inicjatywy zmierzające do złagodzenia zjawiska przestępczości komputerowej. Wielowymiarowość oraz złożoność zagadnienia wymaga również omówienia pojawiających się kontrowersji wokół zwalczania cyberprzestępczości[1].

[1] Wobec braku legalnej definicji, w literaturze występują zamiennie terminy cyberprzestępczość, przestępczość komputerowa, przestępczość związana z komputerami lub przestępczość przy użyciu zaawansowanych technologii. Tymczasem cyberprzestępczość odnosi się do przestępstw popełnianych przy użyciu technologii teleinformacyjnych takich jak telefonia komórkowa, komputer, internet. Cyberprzestępczość określana jest niekiedy jako „nowoczesny rodzaj broni masowego rażenia" lub „broń masowych zakłóceń". D. Zarębski, *Współczesne organizacje*

Wpływ internetu na bezpieczeństwo systemów komputerowych

Wzrost znaczenia technologii informacyjnych oraz telekomunikacyjnych związany jest z trzecią rewolucją przemysłową, a także rozwojem mikroelektroniki i telekomunikacji[2]. Trudno precyzyjnie wyznaczyć moment, w którym rozpoczęła się rewolucja informatyczna. W literaturze wskazuje się na 1946 rok, tj. datę skonstruowania maszyny cyfrowej ENIAC. Ważnymi krokami w kierunku rozwoju ICT było również zaprojektowanie układu scalonego w 1958 roku, mikroprocesora w1971 roku, komputera osobistego w 1981 roku oraz powstanie internetu w 1983 roku (por. rys. 1)[3].



Rys. 1. Historia rozwoju komputeryzacji i bezpieczeństwa w sieci

Źródło: opracowanie własne na podstawie M. Strebe, Podstawy bezpieczeństwa sieci, Warszawa 2005, s. 21.

terrorystyczne, Tarnów 2006, s. 115. Z kolei za przestępczość komputerową należy uznać każde bezprawne działanie, nieetyczne lub nieupoważnione zachowanie odnoszące się do procesu przetwarzania, przekazywania danych w systemach komputerowych lub sieciach teleinformatycznych oraz odnosi się do przestępstw popełnianych wyłącznie przy użyciu komputera. *Informatyka ekonomiczna. Podręcznik akademicki*, red. S. Wrycz, Warszawa 2010, s. 596. Na potrzeby niniejszej pracy, termin cyberprzestępczość oraz przestępczość komputerowa będą traktowane zamiennie.

[2] Ł. Arendyt, E. Krynska, I. Kukulak-Dolata, *Przeciwdziałanie wykluczeniu cyfrowemu na Mazowszu. Priorytety strategiczne*, Warszawa 2011, s. 21 i n.

[3] A. Norberg, J.E. o'Neill, *Transforming Computer Technology: Information Processing for the Pentagon, 1962-1982*, Baltimore 1996, s. 153 i n.

Proces upowszechnienia technologii informacyjnej spowodował głębokie przeobrażenia w życiu i aktywności społecznej. Wywarł także znaczący wpływ na zmianę sposobu wykorzystania czasu, pojawienie się nowego modelu społeczeństwa i nowych więzi oraz „sieci społecznych"[4]. Rozwój technologii informacyjnej wpłynął również znacząco na zmianę jakościową w funkcjonowaniu społeczeństw, szczególnie krajów wysoko rozwiniętych.

Użytkownicy internetu na świecie

Obecnie głównym zasobem jest wiedza i informacja, a stopa życiowa oraz bezpieczeństwo są zależne od zastosowania nowoczesnych rozwiązań technologicznych[5]. Kluczowe znaczenie odgrywa również umiejętność korzystania z technologii. Zdolność wykorzystania technologii wpływa na możliwość sprostania wymogom pojawiającym się na rynku pracy, w życiu społecznym, kulturalnym i wielu innych sferach. Efektywne wykorzystywanie technologii teleinformatycznych jest jednym z czynników przewagi konkurencyjnej. Z kolei brak umiejętności stanowi źródło wykluczenia cyfrowego.

Szczególną rolę we współczesnym świecie zyskał internet, który jest nie tylko jednym z podstawowych narzędzi pracy oraz źródłem komunikacji, ale wspomaga tworzenie informacji medialnych i procesy produkcyjne. W ostatniej dekadzie zauważyć należy nienotowany dotąd, dynamiczny wzrost liczby użytkowników globalnej sieci komputerowej. O ile w 2000 roku odnotowano na świecie 361 mln użytkowników internetu, o tyle w 2011 roku liczba ta zwiększyła się ponad sześciokrotnie i wyniosła 2,3 mld użytkowników, przy ogólnej liczbie 6,9 mld mieszkańców ziemi[6].

Najwięcej użytkowników internetu występuje w Azji, gdzie jeszcze w 2000 roku korzystało z sieci tylko 114,3 mln osób, natomiast w 2011 roku liczba użytkowników internetu zwiększyła się prawie dziewięciokrotnie i wyniosła 1016,8 mln. Drugim kontynentem pod względem ilości użytkowników jest Europa. W 2000 roku odnotowano 105,1 mln użytkowników internetu, natomiast do 2011 roku było już ich 500,7 mln[7].

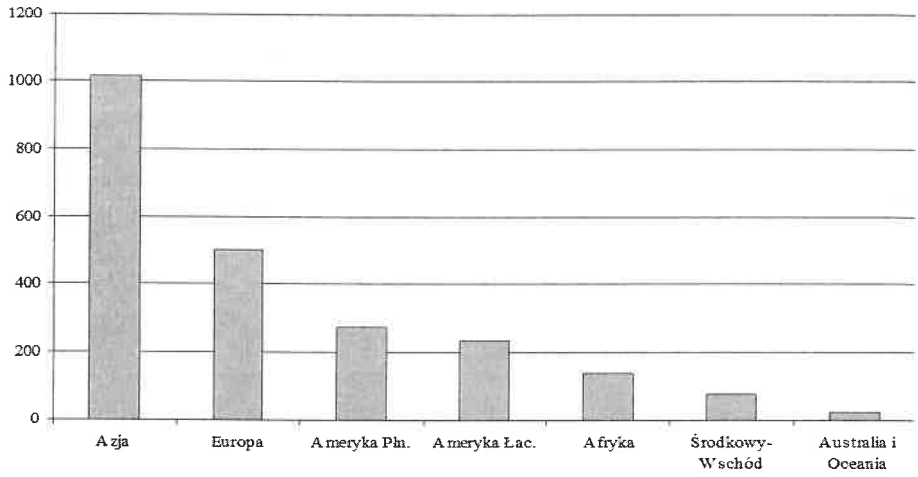
Warto odnotować, że co piąty użytkownik internetu pochodzi z Europy. Ponad połowa osób (56%) zamieszkujących w Unii Europejskiej korzystała w 2011 roku

[4] D. Lombard, *Globalna wioska cyfrowa. Drugie życie sieci*, Warszawa 2009, s. 99–102; D. de Kerckhove, *Inteligencja otwarta. narodziny społeczeństwa sieciowego*, Warszawa 2001, s. 153 i n.

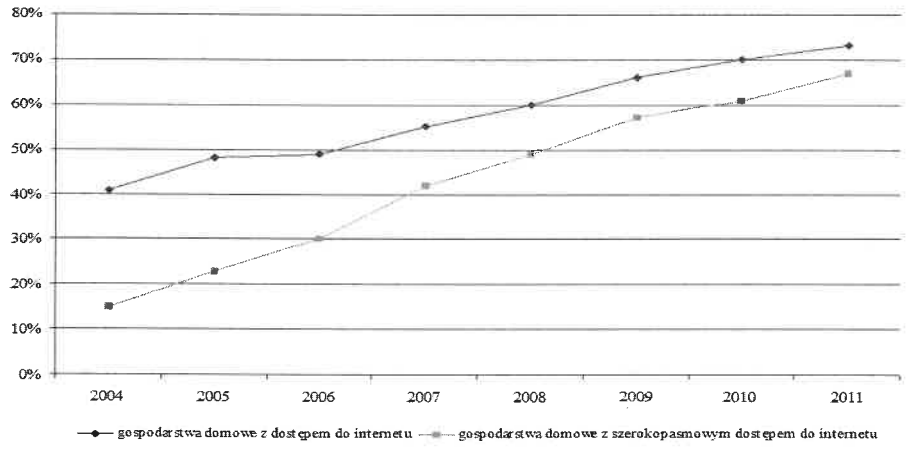
[5] M. Łuszczyk, *Uwarunkowania rozwoju edukacji w zrównoważonej gospodarce opartej na wiedzy*, „Edukacja. Studia, Badania, Innowacje", nr 2 (110), 2010, s. 102-103.

[6] Internet Usage Statistics, Internet World Stats. [Online]. Protokół dostępu: http://www.internetworldstats.com/ [6 lipca 2012].

[7] Ibidem.



Wykres 1. Liczba użytkowników internetu na świecie (w mln) w 2011roku
Źródło: Internet Usage Statistics.



Wykres 2. Skala użytkowników internetu w Europie w latach 2004–2011
Źródło: Internet Usage Statistics.

z internetu codziennie, natomiast dwie spośród trzech osób korzystało co najmniej raz w tygodniu (68%)[8].

Gwałtowny przyrost liczby użytkowników internetu jest tendencją postępującą. Można sądzić, że w najbliższych latach, za przyczyną mobilnych urządzeń telekomunikacyjnych rozwój internetu nadal będzie utrzymywał trend wzrostowy.

[8] H. Seybert, *Internet use in households and by individuals in 2011*, "Statistics in focus" nr 66/2011, s. 1.

Nadużycia związane z technologią teleinformatyczną

Nadużycia popełniane przy pomocy nowoczesnych technologii teleinformatycznych prowadzą do nasilenia obaw związanych z ochroną bezpieczeństwa w wymiarze jednostkowym, lokalnym i globalnym. Celami cyberterrorystów mogą być systemy ICT należące zarówno do użytkowników indywidualnych, administracji państwowej, służb państwa lub podmiotów gospodarczych. Skutkiem cyberataku może być pogwałcenie prywatności, nieuprawnione wykorzystanie informacji, a nawet danych państwowych o istotnym znaczeniu.

Zjawisko cyberterroryzmu zostało dostrzeżone już podczas wojny w Zatoce Perskiej. Komputer rządowy został wówczas zaatakowany przez holenderskich hakerów. Usiłowali oni sprzedać Saddamowi Husajnowi rządowe informacje zawarte w komputerze, co niewątpliwie utrudniłoby Ameryce wojnę z Irakiem[9].

Pierwszy atak, którego bezpośrednim celem była sieć teleinformatyczna odnotowano w 1996 roku. Wówczas sieci komputerowe misji dyplomatycznych Sri Lanki oraz sieci pociągów podmiejskich zostały zablokowane przez organizację o nazwie Tygrysy Wyzwolenia Tamilskiego Islamu[10].

Atak przeprowadzony 11 września 2001 roku na World Trade Center także uznano za formę cyberterroryzmu, ze względu na wykorzystane ICT. Istnieje także uzasadnione przypuszczenie, że terroryści otrzymywali dyspozycje dotyczące zamachu, drogą mailową[11]. Wieże WTC stanowiły ponadto istotny ośrodek sieci teleinformatycznej, a ich zburzenie spowodowało istotne zakłócenie łączności. Powstał ogólny chaos, zawieszono kursowanie metra, kolei, samolotów. W wyniku ataku zginęło 2973 osób.

Jeszcze tego samego roku wirus Nimda w Sydney zaatakował Narodowy Bank Australijski oraz sieć pięciu szpitali. W efekcie oddziały patologii zmuszone zostały do uruchomienia procedur awaryjnego zarządzania[12].

W 2003 roku odnotowano kolejny atak, który można uznać za formę cyberterroryzmu. Jego celem była sieć elektrowni jądrowej Oak Harbor w Ohio. Wówczas wirus SQL Slammer zablokował system monitorujący bezpieczeństwo i nastąpiła kilkugodzinna przerwa w pracy systemu. Tego samego roku pojawiły się dwa groźne wirusy: Blaster, który po trzech dniach aktywności pozbawił pięćdziesiąt milionów osób energii elektrycznej oraz Welchia, odpowiedzialny za paraliż systemu lotniczego Air Canada[13].

---

[9] A. Bartnicki, H. Dalewska-Gren, M. Dehnel-Szyc, i in., *Konflikty współczesnego świata*, Warszawa 2008, s. 58.

[10] D. Zarębski, *Współczesne* ... op. cit., s. 79-80.

[11] A. Bartnicki, H. Dalewska-Gren, M. Dehnel-Szyc, i in., *Konflikty* ... op. cit., s. 59.

[12] P. Dawidziuk, B. Łącki, M. Stolarski, *Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red., M. Madej, M.Terlikowski, Warszawa 2009, s. 57.

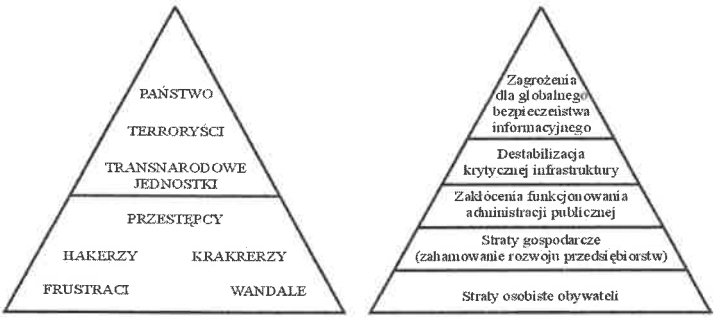
[13] P. Dawidziuk, B. Łącki, M. Stolarski, *Sieć Internet* ... op. cit., s. 57.

W 2007 roku w Estonii miał miejsce cyberterrorystyczny atak, który przeprowadzono na masową skalę. Zablokowaniu uległy wówczas sieci komputerowe w instytucjach publicznych, komputery w kancelarii prezydenta, rządu, policji, banków oraz niektórych gazet. Wyłączono łącza z Unią Europejską i NATO. Ataki były odpowiedzią na decyzję władz dotyczącą przeniesienia pomnika żołnierzy Armii Czerwonej z centrum miasta na cmentarz[14].

Z kolei w 2008 roku za sprawą ataku cyberterrorystycznego przestały działać litewskie rządowe strony internetowe. Atak był odpowiedzią na podpisaną ustawę dotyczącą zakazu publicznego posługiwania się symboliką radziecką. Tego samego roku odnotowano atak cyberterrorystów na strony rządu, prezydenta oraz Narodowego Banku Gruzji[15]. Również w 2008 roku cyberterroryści zablokowali systemy sterujące pracę nuklearnych bloków energetycznych w USA[16].

Rozbudowa infrastruktury i urządzeń połączonych z internetem nieuchronnie prowadzi do rozszerzenia pola działalności cyberprzestępców. Według danych Norton Cybercrime Report 2011, ofiarą cyberprzestępczości było ponad 50 tys. osób na godzinę. Ponad milion osób na świecie stało się każdego dnia ofiarą przestępczości komputerowej. Najczęściej atakowani byli przedstawiciele pokolenia Y oraz dorośli zamieszkujący w krajach rozwijających się.

Łączne straty będące skutkiem cyberprzestępczości wyniosły w 2011 roku 388 mld USD, w tym koszty bezpośrednie zwalczania przestępczości komputerowej wyniosły 114 mld USD, a koszt alternatywny czasu 274 mld USD[17]. Ofiarami cy-



Rys. 2. Hierarchia zagrożeń internetowych i ich skutków

Źródło: P. Sienkiewicz, H. Świeboda, Analiza systemowa zjawiska cyberterroryzmu, „Zeszyty Naukowe AON" 2006, nr 2 (63), s. 10.

[14] A. Bartnicki, H. Dalewska-Gren, M. Dehnel-Szyc, i in., *Konflikty* ... op. cit., s. 60.

[15] Ibidem.

[16] P. Dawidziuk, B. Łącki, M. Stolarski, *Sieć Internet* ... op. cit., s. 59.

[17] Raport został opracowany na podstawie ankiety przeprowadzonej w wybranych krajach Australii, Brazylii, Kanadzie, Chinach, Francji, Niemczech, Indiach, Włoszech, Japonii, Nowej Zelandii, Hiszpanii, Szwecji, Wielkiej Brytanii, USA, Belgii, Danii, Holandii, Hongkongu, Meksyku, RPA, Singapurze, Polsce, Szwajcarii i Zjednoczonych Emiratach Arabskich.

berprzestępczości było w 2011 roku 9% wszystkich mieszkańców świata, a nakład finansowy na przeciwdziałanie przestępczości komputerowej przekraczał ponad stukrotnie wydatki organizacji UNICEF. Przedstawiona wartość jest wyższa niż ogólnoświatowy czarny rynek handlu marihuaną, kokainą i heroiną (295 mld USD). Środki przeznaczone w ciągu jednego roku na przeciwdziałanie cyberprzestępczości wystarczyłyby na zwalczanie malarii przez okres 90 lat lub na trzydzieści osiem lat podwojonych nakładów na edukację w Afryce[18].

Wybrane inicjatywy z zakresu zwalczania cyberprzestępczości

Prace dotyczące zwalczania cyberprzestępczości podjęto na płaszczyźnie europejskiej dwutorowo przez: Unię Europejską oraz Radę Europy. Pierwszą wielostronną umową międzynarodową dotyczącą zwalczania przestępstw komputerowych jest Konwencja o cyberprzestępczości[19], która weszła w życie 1 lipca 2004 roku. Konwencja jest umową bezterminową, ma charakter półotwarty i uzupełnia inne umowy wielostronne oraz dwustronne zawarte między państwami, w szczególności postanowienia:

– Europejskiej Konwencji o ekstradycji podpisanej w Paryżu dnia 13 grudnia 1957 roku (ETS nr 24)[20],

– Europejskiej Konwencji o wzajemnej pomocy prawnej w sprawach karnych podpisanej w Strasburgu dnia 20 kwietnia 1959 roku (ETS nr 30)[21],

– Protokołu dodatkowego do Europejskiej Konwencji o wzajemnej pomocy prawnej w sprawach karnych podpisanej w Strasburgu dnia 17 marca 1978 roku (ETS nr 99)[22].

Celem utworzenia konwencji było powstrzymanie działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, a także uznanie za przestępstwo nieprawidłowe wykorzystywanie tych systemów. Impulsem do utworzenia Konwencji była także chęć przyjęcia skutecznych środków zarówno na szczeblu krajowym, jak i międzynarodowym, które umożliwią zwalczanie, wykrywanie, dochodzenie oraz ściganie cyberprzestępczości.

Konwencja o cyberprzestępczości w preambule akcentuje digitalizację, konwergencję i globalizację sieci informatycznych oraz ryzyko wykorzystywania sieci informatycznych i informacji elektronicznych w celu popełniania przestępstw. Ponadto zauważona została potrzeba ochrony technologii informatycznych, jak

[18] Norton Cybercrime Report 2011. [Online]. Protokół dostępu: http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport// [6 lipca 2012].

[19] Council of Europe Convention on Cybercrime, Budapest 23.11.2001 – ETS 185.

[20] Dz. U. z 1994 r., Nr 70, poz. 307.

[21] Dz. U. z 1999 r., Nr 76, poz. 854.

[22] Dz. U. z 1999 r., Nr 76, poz. 854.

również pogłębienie współpracy między państwami i sektorem prywatnym oraz przyjęcie właściwych przepisów prawnych w kierunku wzmocnienia bezpieczeństwa cybernetycznego.

Postanowienia konwencji gwarantują równowagę pomiędzy krajowymi przepisami prawnymi a prawami człowieka. Zgodnie z art. 15 każda strona ma za zadanie wdrożyć i zastosować procedury stosownie do systemu prawa wewnętrznego oraz zgodne ze zobowiązaniami wynikającymi z Konwencji Rady Europy z 1950 roku o Ochronie Praw Człowieka i Podstawowych Wolności, Międzynarodowego Paktu Narodów Zjednoczonych z 1966 roku o Prawach Obywatelskich i Politycznych i innych międzynarodowych instrumentów z zakresu praw człowieka. Konwencja umożliwia również przyjęcie rozwiązań, które sprzyjają rzetelnej współpracy międzynarodowej, a także harmonizuje prawodawstwa krajowe w zakresie terminologii dotyczącej przestępstw komputerowych oraz gwarantuje bezpieczeństwo sieci i użytkowników. Postanowienia konwencji określają działania, jakie należy podjąć w zakresie prawa karnego materialnego, procesowego i kwestii jurysdykcyjnych dotyczących zwalczania cyberprzestępczości oraz konkretyzuje podstawy funkcjonowania współpracy sądowej między państwami-sygnatariuszami.

Ramy prawne dla ścigania aktów związanych z cyberprzestępczością stanowi nadto protokół dodatkowy dotyczący ścigania aktów rasistowskich i ksenofobicznych popełnionych za pomocą systemów komputerowych[23].

W ramach walki z cyberprzestępczością przyjęto Plan działania Rady i Komisji, który stanowił podstawę kroków Unii Europejskiej podejmowanych w walce z przestępczością komputerową. Realizował on założenia programu haskiego, mającego na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej[24].

Do innych aktów prawnych traktujących o cyberprzestępczości należy:

– decyzja ramowa 2001/413/WSiSW z dnia 28 maja 2001 roku w sprawie walki z oszustwami i fałszerstwami dotyczącymi bezgotówkowych środków płatności[25]. W decyzji zwrócono uwagę na konieczność harmonizacji prawodawstwa poszczególnych krajów w celu zapobiegania oszustwom popełnianym przy wykorzystaniu elektronicznych instrumentów płatniczych oraz zapewnienie skuteczniejszych, proporcjonalnych i zniechęcających sankcji wobec podmiotów popełniających takie przestępstwa.

– dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 roku dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności

[23] Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.01.2003 – ETS 189.

[24] Dz. Urz. UE C 198 z 12 sierpnia 2005 r.

[25] Dz. Urz. UE L 149 z 2 czerwca 2001 r.

elektronicznej)[26]. Dyrektywa uszczegółowia postanowienia dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[27]. Poprzez przyjęcie dyrektywy 2002/58/WE ustawodawca nałożył na dostawców usług komunikacji elektronicznej obowiązek zapewnienia bezpieczeństwa świadczonych przez nich usług. Problematykę tę podejmował również komunikat dotyczący strategii na rzecz bezpiecznego społeczeństwa informacyjnego[28] oraz komunikat w sprawie walki ze spamem, oprogramowaniem szpiegującym i złośliwym[29].

– decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 roku w sprawie ataków na systemy informatyczne[30]. Celem decyzji było podniesienie świadomości odnośnie zagrożeń związanych z bezpieczeństwem systemów informatycznych, które posiadają transnarodowy i transgraniczny charakter. W dokumencie podkreślono konieczność zbliżenia porządków prawnych i współpracy pomiędzy organami państw członkowskich w dziedzinie ataków na systemy informatyczne.

– dyrektywa Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 roku w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[31]. Dyrektywa zastępuje decyzję ramową Rady 2004/68/WSiSW z dnia 22 grudnia 2003 roku dotyczącą zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej[32]. Dyrektywa traktuje o problemie seksualnego wykorzystywania dzieci przy użyciu technologii informatycznych. Celem decyzji było zbliżenie systemów prawnych ustawowych i wykonawczych oraz wspólne odniesienie do przestępstw związanych z wykorzystaniem seksualnym dzieci i pornografii dziecięcej.

Wśród wielu istotnych inicjatyw podejmujących strategię bezpieczeństwa internetu, na uwagę zasługuje:

– Programy Safer Internet oraz Safer Interet plus, ustanowione przez Komisję Europejską od 1999 roku, które promują bezpieczne korzystanie z Internetu przez najmłodszych użytkowników.

– Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), której podstawą prawną działania jest. Rozporządzenie Parlamentu Europejskiego i Rady UE nr 460/2004 z dnia 10 marca 2004 roku w sprawie powołania Europejskiej

[26] Dz. Urz. UE L 201 z 31 lipca 2002 r.

[27] Dz. U. L 281 z 23 listopada 1995 r.

[28] Komunikat dotyczący strategii na rzecz bezpiecznego społeczeństwa informacyjnego (KOM (2006) 261).

[29] Komunikat w sprawie walki ze spamem, oprogramowaniem szpiegującym i złośliwym (KOM (2006) 688).

[30] Dz. Urz. UE L 069 z dnia 16 marca 2005 r.

[31] Dz. Urz. L 355/1 z 17 grudnia 2011 r.

[32] Dz. Urz. UE L 13 z 20 stycznia 2004 r.

Agencji ds. Bezpieczeństwa Sieci i Informacji[33] oraz Dyrektywa Parlamentu Europejskiego i Rady UE nr 2002/21/EC z 7 marca 2002 roku w sprawie ramowych uregulowań dla sieci komunikacji elektronicznej i usług. Głównym celem ENISA jest m.in. sporządzanie ekspertyz dotyczących zagadnień związanych z bezpieczeństwem internetowym, jak również wzmacnianie współpracy Komisji z państwami członkowskimi w zakresie zwalczania cyberprzestępczości.

- Contact Network of Spam Enforcement Authorities (CNSA), który powstał z inicjatywy Komisji Europejskiej. Zadaniem CNSA jest współpraca pomiędzy organizacjami narodowymi w zakresie zwalczania spamu.

Ważnym krokiem w kierunku walki z cyberprzestępczością był także przedstawiony w maju 2007 Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów zatytułowany „W kierunku ogólnej strategii zwalczania cyberprzestępczości"[34]. W dokumencie tym postuluje się wdrożenie strategii zwalczania cyberprzestępczości na szczeblu krajowym, europejskim i międzynarodowym. Zauważono, że cyberataki mogą być skierowane przeciwko najważniejszym strukturom krajów. Uznano za konieczne wzmocnienie współpracy organów ścigania oraz wymianę najlepszych praktyk w zwalczaniu cyberprzestępczości.

Podjęto wiele inicjatyw na poziomie europejskim w kierunku wzmocnienia bezpieczeństwa cybernetycznego. Prace nad niektórymi porozumieniami trwają (np. Canada – EU Trade Agreement), niektóre projekty zostały odrzucone przez Parlament Europejski (np. Anti-Counterfeiting Trade Agreement). Pojawiają się także liczne przeszkody, wśród których należy wymienić niezadowalającą wymianę informacji wywiadowczych, problemy w śledzeniu pochodzenia cyberprzestępców, a także granice jurysdykcji i odmienne możliwości w zakresie dochodzeń oraz ekspertyz sądowych. Wyzwania te przyczyniły się do przedstawienia przez Komisję zamiaru ustanowienia do 2013 roku Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3)[35], którego zadaniem będzie koordynacja działań w zakresie walki z przestępczością komputerową w Europie.

Zakończenie

Prowadzone analizy statystyczne wskazują, że cyberprzestępczość jest obecnie groźniejsza od konwencjonalnych ataków terrorystycznych. Łączne straty będące skutkiem cyberprzestępczości wielokrotnie przewyższają wydatki wielu organizacji humanitarnych, np. UNICEF. Skala dezorganizacji, chaosu oraz destabilizacji

[33] Dz. Urz. UE L 77 z 13 marca 2004 r.

[34] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, W kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r., COM (2007) 267.

[35] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością z dnia 28 marca 2012 r., COM (2012) 140.

życia społecznego, jaką może powodować cyberprzestępczość jest trudna do przewidzenia. Równolegle obserwowana jest również dynamicznie rosnąca zależność społeczeństw i gospodarek od ICT. Oczekuje się przy tym, że rozszerzy się baza użytkowników oraz wzrośnie ilość urządzeń mobilnych połączonych z internetem.

W tak przedstawiających się uwarunkowaniach niezwykle ważne są inicjatywy z zakresu zwalczania cyberprzestępczości, w szczególności podejmowane przez instytucje Unii Europejskiej.