

ROZDZIAŁ XXI

Zbigniew Ciekanowski

Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej

OGRANICZENIE SKUTKÓW ATAKÓW Z CYBERPRZESTRZENI

Wstęp

Cyberprzestrzeń – przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową¹. Pojęcie cyberprzestrzeni pojawiło się po raz pierwszy ponad 30 lat temu. Wówczas William Gibson – amerykański pisarz science fiction, określany mianem ojca cyberpunku – napisał opowiadanie „Wypalić Chrom” (org. Burning Chrome, 1982), w którym przedstawił światu nowe pojęcie, będące wg autora rzeczywistością wirtualną, w której znajdowali się jego bohaterowie². Najbardziej znanymi przykładami prac reprezentujących ten nurt współczesnej kultury są filmy: trylogia „Matrix” oraz wcześniejszy „Johnny Mnemonic”. Wizja cyberprzestrzeni została przedstawiona w filmach jako przestrzeń zobrazowana za pomocą grafiki komputerowej – funkcjonująca niczym obraz w grze komputerowej, pełna trójwymiarowych, interaktywnych obiektów poruszających się we wspólnym środowisku z zachowaniem perspektywy i znanych nam z rzeczywistości takich zjawisk fizycznych, jak grawitacja czy kolizja obiektów. Wizualizacja ta pozwalała przypisywać cyberprzestrzeni cechy właściwe realnej, postrzegalnej zmysłami rzeczywistości, którą można nie tylko zobaczyć, ale również dotknąć i kształtować za pośrednictwem odpowiednio przygotowanego interfejsu³.

1. Cyberprzestrzeń

Z uwagi na rosnące znaczenie systemów teleinformatycznych wykorzystywanych obecnie przez społeczeństwa na całym świecie, a także wchodzących w skład państwowej infrastruktury krytycznej, współczesna doktryna prawna zaczęła interesować się legalnym definiowaniem cyberprzestrzeni. Było to spowodowane ilością specyficznych działań podejmowanych przez ludzi za pośrednictwem komputerów oraz sieci. Konieczne było rozpoznanie nowego

¹ www.sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (dostęp: 11.07.2016 r.).

² L. Krakowiak, *Neuromancer – 25 lat później. Spełnione przepowiednie*, www.idg.pl (dostęp: 11.07.2016 r.).

³ K. Loska, *Encyklopedia filmu science fiction*, wyd. Rabid, Kraków 2004, s. 30.

cyfrowego środowiska, które nadało zupełnie nowy kształt zawieraniu umów cywilnoprawnych, dokonywaniu czynności administracyjnych, ale i popełnianiu nowoczesnych form przestępczości. Wiele spośród znanych dotychczas czynności prawnych wyraźnie zmieniło się w cyberprzestrzeni, podczas gdy inne dopiero dzięki niej powstały. Poniżej zaprezentowano krótki przegląd definicji cyberprzestrzeni przyjętych na gruncie rządowych dokumentów różnych krajów, w tym definicję cyberprzestrzeni zapisaną w polskiej ustawie, a dalej omówiono, w jaki sposób przyjęcie określonego sposobu charakteryzowania cyberprzestrzeni wpływa na rozumienie tego, czym jest „bezpieczeństwo cyberprzestrzeni”. Jedną z najbardziej znanych i powszechnie cytowanych jest definicja cyberprzestrzeni sformułowana przez Departament Obrony USA na potrzeby powołania jednolitego słownika terminologii wojskowej oraz powiązanej, według której cyberprzestrzeń to: „Globalna domena środowiska informacyjnego składająca się z 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”⁴.

Charakterystyczną cechą tej definicji jest brak odwoływania się w niej do jakichkolwiek elementów społecznych, czy w ogóle do ludzi będących użytkownikami cyberprzestrzeni, pomimo że elementy te były istotną częścią oryginalnego rozumienia cyberprzestrzeni. Definicja Departamentu Obrony USA skupia całą uwagę na technologicznych fundamentach cyberprzestrzeni, wskazując przede wszystkim Internet. Jak słusznie zauważono w literaturze przedmiotu, ów aspekt technologiczny został jednak w definicji poruszony w ograniczonym zakresie: definicja *expressis verbis* wskazuje jedynie na sprzętową stronę infrastruktury tworzącej cyberprzestrzeń, pomijając jej warstwę programową. W przyjętej w 2003 r. Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni zapisano: „Nasza Krajowa infrastruktura krytyczna jest budowana przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych, a także pocztowym oraz dostawczym. Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju. Cyberprzestrzeń jest zbudowana z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej. Stąd też zdrowe funkcjonowanie cyberprzestrzeni jest kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego”⁵.

⁴ Cyt. Za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” nr 9, www.abw.gov.pl. (dostęp: 11.07.2016 r.).

⁵ Tamże.

Zawarty w strategii bezpieczeństwa szeroki zakres definicji cyberprzestrzeni wskazuje nie tylko na wielość oraz rozległość elementów infrastrukturalnych wraz z ich powiązaniem z krajową infrastrukturą krytyczną (której poprawne funkcjonowanie jest fundamentem realizowanych zadań państwa), lecz także na aspekt społeczno-ekonomiczny funkcjonowania cyberprzestrzeni. Nazywanie cyberprzestrzeni układem nerwowym wszelkich sektorów gospodarczych oraz administracyjnych to wyraz znaczenia, jakie przywiązuje się w Stanach Zjednoczonych do zagadnień informatyzacji kraju oraz roli tego procesu w budowaniu nowoczesnego państwa. To właśnie cyberprzestrzeń – będąca nowoczesnym, w dużej mierze zautomatyzowanym obszarem natychmiastowej wymiany ogromnych ilości informacji – jest prezentowana w przytoczonej definicji jako główny ośrodek krajowej działalności gospodarczej. I rzeczywiście, niefunkcjonowanie na przykład w Internecie, będącym, zgodnie z definicją, jednym z podstawowych elementów cyberprzestrzeni, oznacza w wysoko rozwiniętych krajach poważne ograniczenie udziału w nowoczesnej wymianie rynkowej⁶.

Przechodząc na grunt europejski, można znaleźć liczne rozważania na temat istoty cyberprzestrzeni. Analizę pojęcia warto rozpocząć od omówienia definicji przedstawionej na szczycie Unii Europejskiej. W oficjalnym, elektronicznym słowniku pojęć z zakresu społeczeństwa informacyjnego można przeczytać następującą, zaproponowaną przez Komisję Europejską, definicję cyberprzestrzeni: „Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata”⁷.

Socjologicznym rozwinięciem koncepcji cyberprzestrzeni jako obszaru komunikacji o światowym zasięgu jest nazwanie jej Nową Wieżą Babel. Cyberprzestrzeń nie tylko zbliża, ale wręcz powoduje mieszanie się kultur, gromadząc idee oraz informacje pochodzące z całego świata. Stwierdzenie, że wyłączenie się z niej spowoduje izolację jednostek, spadek konkurencyjności przedsiębiorstw oraz podrzędność krajów, wskazuje na ogromne znaczenie tego obszaru, służącego uczestniczeniu w nowoczesnej, globalnej społeczności. Innym, ale tak samo interesującym określeniem użytym w strategii francuskiej jest nazwanie cyberprzestrzeni Nowymi Termopilami, gdzie na co dzień dochodzi do niewidocznych w materialnym świecie starć, nie tylko zaburzających poprawne funkcjonowanie systemów czy naruszających dobra prawne ich użytkowników, lecz także mogących zagrazić ludzkiemu życiu. Może się tak zdarzyć, jeśli na przykład zostaną zaatakowane systemy odpowiedzialne za szeroko rozumiane bezpieczeństwo publiczne.

Również w Polsce do porządku prawnego wprowadzono definicję cyberprzestrzeni, zapisując ją w ustawie, a nie w dokumencie o charakterze

⁶ Tamże.

⁷ www.ec.europa.eu. (dostęp: 11.07.2016)

wyłącznie rządowym, jak w przypadku wcześniej omawianych krajów. W dniu 2 listopada 2011 r. weszła w życie ustawa nowelizująca regulacje prawne stanów nadzwyczajnych. Implementując do polskiego porządku prawnego kwestię ochrony cyberprzestrzeni, wprowadzała również definicję omawianego pojęcia. Na podstawie założeń projektu Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011-2016 (dokumentu przyjętego ostatecznie w połowie 2013 r. pod nazwą *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* – o którym jest mowa dalej), zawarta w noweli definicja pojęcia cyberprzestrzeń przyjęła następujące brzmienie: „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, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”⁸.

Analizując najistotniejsze cechy definicji cyberprzestrzeni pochodzącej z ustawy krajowej, należy wskazać na fakt, że definicja ta wprowadza ideę jednej cyberprzestrzeni, będącej wydzielonym logicznie obszarem – cyfrową domeną przetwarzania oraz wymiany informacji. Przestrzeń ta, mająca charakter ponadnarodowy, jest tworzona przez systemy teleinformatyczne połączone za pośrednictwem sieci telekomunikacyjnych, w tym sieci, których elementy infrastrukturalne są zlokalizowane na terenie innych państw. Działanie w cyberprzestrzeni nie ogranicza się wyłącznie do wymiany informacji. Może ono również polegać na samym ich wytwarzaniu, modyfikowaniu czy po prostu odczytywaniu. Tak więc i te operacje są dokonywane na gruncie domeny cyfrowej. W definicji, wskazując także na wzajemne relacje systemów z użytkownikami, podkreślono swojego rodzaju dwustronne powiązanie działań w cyberprzestrzeni z działaniami w „fizycznej” rzeczywistości (rzeczywistym świecie) oraz ich wzajemne konsekwencje.

2. Bezpieczeństwo teleinformatyczne

Pojęcie bezpieczeństwa teleinformatycznego określa ochronę informacji przetwarzanej, przechowywanej i przesyłanej za pomocą systemów teleinformatycznych, przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania.

⁸ Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Dz.U. z 2011 r. Nr 222, poz. 1323.

Podstawowe atrybuty informacji związane z jej bezpieczeństwem to⁹:

- tajność – termin ten oznacza, że dostęp do określonych danych i informacji posiadają wyłącznie uprawnione osoby;
- integralność – termin ten oznacza, że dane i informacji są poprawne, nienaruszone i nie zostały poddane manipulacji;
- dostępność – termin ten charakteryzuje się systemem informatycznym i oznacza dostępność do danych, procesów i aplikacji zgodnie z wymaganiami użytkownika.

W zależności od typu organizacji chroniącej informację, będą preferowane różne typy wyżej wymienionych atrybutów, np. w organizacji typu militarnego główny nacisk będzie położony zwykle na tajność, w organizacji typu finansowego na integralność i dostępność. W zależności od przeznaczenia i konstrukcji systemu teleinformatycznego rozróżnia się tzw. bezpieczeństwo na zewnątrz oraz bezpieczeństwo do wewnątrz. Termin „bezpieczeństwo na zewnątrz” określa ochronę przed zagrożeniami dla środowiska, w którym pracuje system komputerowy, spowodowane jego nieprawidłowym działaniem. Dotyczy to głównie systemów czasu rzeczywistego, takich jak systemy monitorujące stan pacjenta w szpitalu, systemy kontroli działania elektrowni jądrowej, systemy nadzoru ruchu kolejowego czy też systemy pokładowe współczesnych samolotów, w tym także bojowych. Należy zwrócić uwagę, że wspomniane zagrożenia nie są stwarzane przez oprogramowanie jako takie lecz przez nieprawidłową interakcję pomiędzy oprogramowaniem, a jakimś urządzeniem wykonawczym systemu. Z tego względu problem realizacji bezpiecznego oprogramowania dla systemów tego typu związany jest z problemem bezpiecznej konstrukcji całego systemu. Termin „bezpieczeństwo do wewnątrz” określa ochronę przed zagrożeniami dla informacji przechowywanej, przetwarzanej i przesyłanej w systemie teleinformatycznym. Dotyczy to głównie sieci teleinformatycznych, banków, firm, organizacji naukowych, itp.

Z bezpieczeństwem informatycznym jest związanych szereg pojęć, które definiuje się najczęściej następująco¹⁰:

- zapewnienie bezpieczeństwa informacji, polega na jej ochronie przed przypadkowym lub umyślnym zniszczeniu, ujawnieniem lub modyfikacją;
- środki bezpieczeństwa w systemach teleinformatycznych, to wszelkie zabezpieczenia technologiczne i środki administracyjne, które można stosować do danych, programów i komputerów dla zapewnienia ochrony interesów przedsiębiorstw i indywidualnej poufności;
- poufność, jest to prawo jednostki do decydowania o tym, jakimi informacjami chce się podzielić i jakie jest skłonna przyjąć;

⁹ K. Liderman, *Bezpieczeństwo teleinformatyczne*, Wyd. Naukowe PWN, Warszawa 2013, s. 15

¹⁰Tamże, s. 16.

- tajność, jest to atrybut opisujący stopień ochrony, jakiej informacja ma podlegać. Jest on uzgadniany przez osoby lub organizacje dostarczające i otrzymujące informację;
- nienaruszalność, dane są nienaruszone gdy nie różnią się od danych źródłowych i nie zostały przypadkowo bądź złośliwie zmienione, ujawnione lub zniszczone.

Na podstawie praktycznych doświadczeń zostały sformułowane pewne ogólne zasady bezpieczeństwa teleinformatycznego w systemach projektowania zabezpieczeń. Należą do nich¹¹:

- domniemana odmowa udzielenia dostępu do informacji, jeżeli sytuacją domniemaną jest brak dostępu, można zmusić użytkownika do uzasadnienia potrzeby uzyskania dostępu do określonej informacji przed jego udzieleniem;
- kontrola projektu systemu zabezpieczeń – ukazanie słabych stron projektu jeszcze w toku planowania, ułatwi wprowadzenie poprawek przed wdrożeniem go, zanim inne systemy zaczną polegać na jego błędnym działaniu;
- akceptowalność systemu zabezpieczeń – system zabezpieczeń musi być akceptowany przez użytkownika, gdyż w przeciwnym przypadku nie będzie on z niego korzystał. W szczególności dotyczy to zachowania w maksymalnym stopniu funkcji systemu, do których jest przyzwyczajony użytkownik;
- kontrola upoważnienia dostępu do informacji – upoważnienie musi być badane przy każdym żądaniu dostępu do informacji, a jego wartość określana przy każdej zmianie;
- zasada najmniejszego uprzywilejowania – każdy użytkownik powinien korzystać tylko z tych przywilejów, które są niezbędne do wykonania zadania;
- ekonomiczność systemu ochrony – system ochrony informacji powinien być tak prosty jak tylko możliwe, a jego koszt powinien być adekwatny do wartości chronionej informacji;
- oddzielenie przywilejów – realizowane według reguły, że dwa oddzielne zamki stanowią znacznie lepszą elastyczniejszą ochronę niż jeden, szczególnie wtedy, gdy klucze do nich mogą być fizycznie rozdzielone;
- minimalizacja współużytkowanych mechanizmów ochrony – każdy wspólny mechanizm jest potencjalną ścieżką przepływu informacji między użytkownikami.

¹¹Tamże, s. 17.

3. Cyberterroryzm

Nieustanny postęp technologiczny, będący imperatywem o sile nieomal równej postępowi biologicznemu codziennie zmienia otaczającą nas rzeczywistość, kreując nie tylko nowe możliwości, lecz także wyzwania. Nowoczesne techniki komputerowe, lub szerzej – teleinformatyczne, które zaledwie kilkanaście lat temu były przedmiotem powieści science fiction, są obecnie powszechnie wykorzystywanymi rozwiązaniami. Takie zjawiska, jak ogólnościowa wymiana informacji, stosowanie elektronicznego podpisu, korzystanie z e-bankowości czy niezwykle popularne portale społecznościowe oraz rozrywkowe, prowadzą do wirtualizacji rzeczywistości i „cyfryzacji” ludzkiego życia. Znakiem czasów stało się przetwarzanie jak największych ilości danych o poszczególnych osobach oraz o ich działaniach w przeróżnych systemach teleinformatycznych. Aby uzmysłowić rozmiary poruszonego zjawiska, posłużono się kilkoma liczbami¹²:

- liczba mieszkańców na świecie wynosi ponad 7 mld, ponad 2 mld z nich korzysta z Internetu;
- na świecie jest aktywnych ponad 5 mld numerów telefonów komórkowych;
- liczba użytkowników Internetu w Polsce wynosi około 24 mln;
- statystyczny użytkownik Internetu spędza w sieci 16 godzin miesięcznie, co w skali światowej daje około 35 mld godzin w ciągu miesiąca (czyli, w przybliżeniu, 4 tys. lat online na każdy miesiąc kalendarzowy);
- wartość sprzedaży online w USA w pierwszym kwartale 2012 r. osiągnęła 50 mld dolarów;
- wyszukiwarka Google otrzymuje dziennie ponad miliard pytań;
- liczba kont na portalu Facebook przekracza miliard, w tym ponad 10 mln to konta użytkowników z Polski;
- co sekundę w serwisie Youtube pojawia się kolejna godzina materiału filmowego;
- każdego dnia w grze Farmville (wchodzącej w skład portalu Facebook) sprzedaje się około 500 tys. traktorów. W realnym świecie firma John Deere sprzedaje 5 tys. maszyn rolniczych rocznie.

Powyższe liczby to jedynie czubek góry lodowej całego zjawiska. Uzmysławiają, jak dużą część życia spędza się obecnie online przed komputerem, tabletem czy smartfonem. Dla wielu osób wykładnikiem statusu społecznego stała się liczba osób zaproszonych do grona znajomych na ich profilu, znajdującym się na portalach społecznościowych. Dla innych zakup wirtualnego przedmiotu, dostępnego choćby tylko w sieciowej grze kompu-

¹²www.internetworldstats.com/stats.htm (dostęp: 11.07.2016 r.).

terowej, może być wart nawet kilka tysięcy dolarów. Dla wszystkich Internet stał się najszybszym źródłem informacji oraz wygodną przestrzenią wykorzystywaną do świadczenia wielu usług. Tak narodziła się wcześniej opisywana cyberprzestrzeń. Tak też w konsekwencji wraz z rozwojem techniki komputerowej zaczął się cyberterroryzm. Cyberterroryzm to politycznie umotywowany atak lub groźba ataku na komputery, sieci lub system informatyczne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów. W szerszym rozumowaniu tego słowa jest to także użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne¹³. Cyberterroryzm nie jest odrębnym lub specyficznym rodzajem terroryzmu ze względu na ideologię. Służy dokładnie tym samym celom co zamachy bombowe, porwania czy branie zakładników, z tą tylko różnicą, że jest niewidoczny podczas ataku. Cyberterroryzm ma zatem dla terrorystów wiele zalet, które czynią go doskonałym narzędziem godzenia w cel przy bardzo niskich kosztach (w porównaniu z innymi zamachami) i niewielkich możliwościach wykrycia. Jest bezpieczny ponieważ nie wymaga wykorzystywania zabronionych środków zagrażających życiu i zdrowiu, takich jak: broń palna, materiały wybuchowe, substancje chemiczne i radioaktywne. Jeszcze jedną z zalet jest możliwość długotrwałego działania bez wykrycia, wielokrotnego przełamывania systemów ochronnych bez alarmowania odpowiednich służb. Niektóre operacje, np. włamania do systemów bankowych mogą nie zostać nigdy wykryte. Rozróżniamy 3 zasadnicze formy cyberterroryzmu¹⁴:

- włamania (włącznie z nielegalnym pozyskaniem, usuwaniem lub zmianom danych) i blokada serwerów – może to przybrać formę zmieniania lub uszkodzania systemów operacyjnych i doprowadzania do wielokrotnych połączeń atakowanego serwera jak i innych serwerów. Prowadzi to do stopniowego spowolnienia jego pracy, a następnie do zawieszenia (zwanego efektem DOS – denial of service);
- wirusy – programy działające wbrew woli użytkownika systemu na jego szkodę. Mogą wywołać różne efekty. Najczęściej przeznaczone są do uszkodzania baz danych i systemów operacyjnych. Mogą także paraliżować systemy zabezpieczające lub modyfikować zachowanie systemu. Zgodnie z powszechną nazwą, wirusy mogą mieć zdolność atakowania systemów połączonych z zaatakowaną jednostką przenoszącą się wraz z pocztą elektroniczną. Mogą także być umieszczane w systemie podczas włamania, albo atakować go po innym połączeniu z zainfekowanym serwerem (np. przez wejście na stronę internetową);

¹³A. Bógdał-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Wyd. Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 326.

¹⁴Z. Ciekanowski, *Zwalczanie terroryzmu w Polsce*, wyd. PWST-E, Jarosław 2015, s. 120.

- atak konwencjonalny – polega na fizycznym uszkodzeniu elementów systemu komputerowego, serwerów, infrastruktury telekomunikacyjnej, energetycznej, komunikacji (lotniska, koleje, itp.). Atak tego typu może, zależnie od sposobu prowadzenia, prowadzić do czasowego paraliżu systemu lub nieodwracalnej utraty danych.

Za narodziny cyberterroryzmu na świecie uważa się moment powstania politycznej koncepcji „autostrad informatycznych”, w czasie kampanii prezydenta Billa Clintona w 1992 roku. Koncepcja ta zakładała, że wszelkiego typu informacje zawierające tekst, dźwięk i obraz będą mogły być przekazywane na duże odległości szybko i bez przeszkód. Jednak pierwsze wzmianki na temat zamachów terrorystycznych przy użyciu komputerów pojawiły się dużo wcześniej, bo w 1979 roku, w raporcie rządu szwedzkiego na temat zagrożeń społecznych związanych z komputeryzacją. Słowo cyberterroryzm zaś było używane już w latach 80. w wypowiedziach amerykańskich specjalistów w wydziale wywiadu wojskowego¹⁵. Od tego czasu o cyberterroryzmie mówiło się coraz częściej. W latach 90. XX wieku zawiśło nad Stanami Zjednoczonymi widmo „elektronicznego Pearl Harbour”. W prasie zaczęły pojawiać się bowiem nagłówki informujące o atakach cyberterrorystów. W roku 1995 cybernetyczny świat obiegła makabryczna wieść, że rząd meksykański zbombardował pewne miasto: „korytarze szpitala w Comitán były pełne trupów, a żołnierze gwałcili kobiety i mordowali dzieci”. Później okazało się, że doniesienia były sfałszowane¹⁶. Przykłady niestety można mnożyć. Najbardziej spektakularny i dramatyczny przykład działania cyberterrorystów to przeprowadzenie 11 września 2001 roku uszkodzenia przez zespół Al.-Kaidy systemów identyfikacji samolotów porwanych i wykorzystanych podczas zamachów, co skutkowało zamachem na World Trade Center. Cyberataki nie są już więc tylko wytworem wyobraźni autorów książek o tematyce fantastyki naukowej, ale realnym zagrożeniem, którego skutki mogą być odczuwalne dla każdego z nas. Najbardziej prawdopodobne są bowiem ataki przeciw systemom informacyjnym użytkowanym w sferze cywilnej. Poziom ich zabezpieczenia jest bowiem z reguły niższy niż systemów wojskowych.

4. Europejski obszar wolności, sprawiedliwości oraz bezpieczeństwa

Jednym z podstawowych celów stworzenia Unii Europejskiej było zapewnienie na jej terenie swobodnego przepływu ludzi, towarów, usług i kapitału. Swobodny przepływ usług i towarów umożliwił utworzony na terytorium UE Jednolity Rynek Europejski, natomiast swobodny przepływ

¹⁵A. Adamski, *Cyberterroryzm*, [w:] *Materiały z konferencji nt. Terroryzmu*, Wyd. Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2002, s. 113-114.

¹⁶www.tecfa.unige.ch/etu/E71b/99/deian/terrorisme.html (dostęp: 11.07.2016 r.).

osób warunkuje Układ z Schengen z 1985 r., podpisany przez państwa które wchodziły w skład Wspólnoty z wyłączeniem Wielkiej Brytanii i Irlandii. Trzeba tutaj także zaznaczyć, że państwa włączone do UE w 2004 r. nie spełniały jeszcze wszystkich wymagań warunkujących przystąpienie do obszaru Schengen. Porozumienie z Schengen – oprócz zniesienia kontroli dla osób przekraczających wewnętrzne granice Unii – wzmacnia współpracę państw członkowskich w zakresie bezpieczeństwa, a także polityki azylowej. Koncepcja zniesienia kontroli paszportowych na wewnętrznych granicach Unii spowodowała, że zaczęto zastanawiać się nad koniecznością wprowadzenia dodatkowych środków mających nie tylko wzmocnić zewnętrzne granice UE, ale także podjęcie innych działań na poziomie europejskim w celu zapewnienia bezpieczeństwa obywatelom.

W 1999 r. podczas szczytu w Tampere w Finlandii władze UE postanowiły utworzyć na swoim terytorium jednolity obszar bezpieczeństwa, sprawiedliwości i wolności. Podkreślano, że wolność, bezpieczeństwo i sprawiedliwość to koncepcje wzajemnie się uzupełniające, ponieważ jedynie w bezpiecznym państwie ludzie mogą czuć się prawdziwie wolni. Na szczycie w Tampere omawiano między innymi kwestię wspólnej polityki azylowej i migracyjnej, zwalczanie przestępczości i problemy związane z ujednoliceniem systemu prawnego. W konsekwencji przyjęto 5-letni plan działania, którego realizację powierzono Komisji Europejskiej. Realizacja przebiegała początkowo powoli i dość pasywnie, zajmowano się raczej uzgodnieniami niż praktyczną realizacją zadań. Jednakże po zamachach terrorystycznych przez Al-Kaidę we wrześniu 2001 r. i marcu 2004 r. zaobserwowano gwałtowne przyspieszenie prac legislacyjnych i organizacyjnych, w szczególności w sferze bezpieczeństwa. Podczas pierwszych lat realizacji planu stworzono podstawy prawne mające na celu poprawę skuteczności zwalczania zorganizowanej przestępczości i terroryzmu. Przygotowano ramy prawne działania Europejskiego Nakazu Aresztowania, stworzono europejską listę organizacji terrorystycznych oraz dopracowano samą definicję terroryzmu. Opublikowano szereg decyzji ramowych, a także decyzję na temat zasad walki z praniem brudnych pieniędzy¹⁷. W komunikacie z dnia 2 czerwca 2004 r. Komisja podsumowała realizację planu Tampere, i tym samym zainicjowała konsultacje nad opracowaniem nowego, dalszego programu działań. Jako główne osiągnięcie programu Tampere wymieniono widoczny, ogromny postęp w obszarze sprawiedliwości i spraw wewnętrznych UE. Dotarło do wniosku, że działania w tej dziedzinie traktowane są przez Unię jako działania priorytetowe. Podkreślono, że wprowadzanie zmian odbywało się przy pełnej akceptacji europejskiej opinii publicznej. Podkreślono także, że coraz większość obywateli UE dostrzega korzyści płynące z ży-

¹⁷ A. Podolski, *Program Haski (Bezpieczeństwo wewnętrzne i sprawiedliwość w latach 2005 – 2006) – Polska perspektywa*, Centrum Stosunków Międzynarodowych, *Raporty i Analizy* 2004, nr 14, s. 2.

cia w jednolitym obszarze bezpieczeństwa, sprawiedliwości i wolności. Stwierdzono, że rozszerzenie EU o nowe państwo powinno być traktowane jak ogromne wyzwanie, wymagające położenia coraz większego nacisku na wzmocnienie bezpieczeństwa wewnątrz europejskiego. Apelowano także o wzmocnienie zewnętrznych granic EU, rozwój Systemu Informacji Schengen drugiej generacji, oraz dobrego przygotowania nowych państw członkowskich do pełnej z nią integracji. Zapewnienie skuteczniejszej ochrony praw podstawowych jednostki uznano za jeden z podstawowych priorytetów. Zostanie ona przede wszystkim wzmocniona poprzez włączenie Karty Praw Podstawowych do Traktatu Konstytucyjnego oraz przystąpienie do europejskiej konwencji w sprawie ochrony praw człowieka i podstawowych wolności¹⁸.

We wprowadzeniu podkreślono dorobek wcześniejszych lat oraz zwrócono uwagę, że w świetle ataków terrorystycznych zaistniała silna potrzeba wypracowania bardziej skutecznego, wspólnego podejścia przede wszystkim do problemów transgranicznych, w szczególności związanych z zapobieganiem terroryzmowi i jego powstrzymywaniem.

W obszarze wzmacniania wolności zaakcentowano, iż należy jak najszybciej umożliwić wszystkim obywatelom Unii swobodne przemieszczanie się i przebywanie na obszarze dowolnego państwa członkowskiego¹⁹. Sporo miejsca poświęcono także zagadnieniom związanym ze wzmacnianiem bezpieczeństwa. Stwierdzono między innymi, że poprawa informacji transgranicznych między organami ścigania jest jednym z najważniejszych zadań. Metody wymiany informacji powinny wykorzystywać nowoczesną technologię, umożliwiającą łatwy i bezpośredni dostęp do nowych, jak i istniejących już baz danych. Koncepcja rozwoju Europejskiego Obszaru Bezpieczeństwa, Wolności i Sprawiedliwości zawarta w Programie Haskim promuje „międzyrządowy sposób organizacji działań i wymiany informacji w kwestii bezpieczeństwa”²⁰. Podsumowując działania podejmowane w ramach Programu Haskiego za sukces uznano przyjęcie w lutym 2006 r. dyrektywy w sprawie przechowywania danych generowanych lub przetwarzanych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej, zmieniając dyrektywę 2002/58/WE.

Powstaniu bardziej sprawiedliwego, bezpieczniejszego i zjednoczonego obszaru europejskiego miała sprzyjać także przyjęta na spotkaniu

¹⁸Komunikat Komisji dla Rady i Parlamentu Europejskiego, *Obszar Wolności, Bezpieczeństwa i Sprawiedliwości: bilans programu Tampere i przyszłe kierunki działania z dnia 2 czerwca 2004 r.*, COM (2004) 401.

¹⁹Dyrektywa Parlamentu Europejskiego i Rady 2004/38/WE z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium państw członkowskich.

²⁰A. Podolski, *Program Haski...* s. 5.

Rady Europejskiej w Brukseli 11-12 grudnia 2003 r. Europejska Strategia Bezpieczeństwa (ESS), będąca potwierdzeniem wywiązywania się EU z obowiązku zagwarantowania bezpiecznej Europy w lepszym świecie. Przedstawiono ją w zwięzłym dokumencie zatytułowanym Bezpieczna Europa w Lepszym Świecie (ang. A Secure Europe in a Better World). Na wstępie dokumentu podkreślano, iż Europa licząca ponad 450 mln mieszkańców i wytwarzająca ponad jedną czwartą światowego produktu brutto powinna przyjąć współodpowiedzialność za globalne bezpieczeństwo i budowę lepszego świata. Dokument został więc podzielony na trzy części. Pierwszą z nich poświęcono analizie międzynarodowego środowiska bezpieczeństwa. Po raz pierwszy w unijnym dokumencie precyzyjnie zdefiniowano i wyodrębniono pięć zagrożeń w obliczu których stoi Europa: terroryzm, proliferacja broni masowego rażenia, konflikty regionalne, upadek państwa oraz zorganizowana przestępczość. Drugim strategicznym celem UE powinno być tworzenie porządku międzynarodowego, opartego na skutecznym multilateralizmie. W trzeciej części dokumentu zawarto praktyczne implikacje politycznych założeń Europy. Podkreślono, że podejmując działania w celu zwiększenia bezpieczeństwa światowego, UE powinna być bardziej aktywna, spójna i dysponować lepszymi zdolnościami działania. Bycie aktywnym w tym wypadku oznacza „większe zdecydowanie w stosowaniu szerokiego spektrum instrumentów, które Unia ma do dyspozycji w celu rozwiązywania kryzysów i zapobiegania konfliktom: politycznym, dyplomatycznym oraz militarnym oraz wykorzystywaniu instrumentów z zakresu handlu i pomocy rozwojowej”²¹.

Dodatkowo warto zaznaczyć, że w dokumencie odnotowano także zadowolenie przyjęcia europejskiego nakazu aresztowania, wzmocnienia działań w celu zwalczania finansowania terroryzmu, a także zawarcia umowy ze Stanami Zjednoczonymi o wzajemnej pomocy prawnej. W grudniu 2008 r. Rada Europejska przyjęła sprawozdanie o realizacji *Europejskiej Strategii Bezpieczeństwa Sprawozdanie na temat wdrażania europejskiej strategii bezpieczeństwa – utrzymanie bezpieczeństwa w zmieniającym się świecie*. We wstępie do raportu podkreślono, że Europejska Strategia Bezpieczeństwa z 2003 r. jest cały czas aktualna, żadne z przedstawionych w niej zagrożeń nie zniknęło, niektóre zyskały na znaczeniu, a wszystkie stały się bardziej złożone. Jako globalne wyzwanie i główne zagrożenia wymieniono: rozprzestrzenianie się broni masowego rażenia, terroryzm i przestępczość zorganizowaną, cyberbezpieczeństwo, bezpieczeństwo energetyczne oraz zmiany klimatyczne które uznano za czynniki zwielokrotniające zagrożenia. Autorzy zwrócili także uwagę na problem piractwa. Mówiąc o cyberbezpieczeństwie, podkreślono, że nowoczesne gospodarki

²¹R. Kuźniar, *Europejska Strategia Bezpieczeństwa*, „Polska w Europie” 2004, nr 2, s. 24.

w dużym stopniu zależą od krytycznej infrastruktury, w tym transportu, łączności i dostaw energii, ale również od Internetu. Ataki kierowane na prywatne lub rządowe systemy informatyczne w państwach członkowski EU można uznać za nową potencjalną broń ekonomiczną, polityczną a nawet wojskową. W związku z tym w obszarze cyberbezpieczeństwa konieczne są dalsze prace w celu przeanalizowania możliwości przyjęcia kompleksowego podejścia unijnego, podniesienie poziomu świadomości zacieśnienia współpracy międzynarodowej. Instrumentem ściśle powiązanym z walką z szeroko pojętym terroryzmem jest obowiązek gromadzenia i archiwizowania danych o ruchu w sieciach telekomunikacyjnych dla potrzeb organów ścigania i służb specjalnych. Retencja danych obliuguje operatorów i dostawców telekomunikacyjnych – w tym dostawców Internetu – do zapisywania i archiwizowania przez pewien określony czas wszystkich danych o ruchu generowanym podczas normalnej pracy przez systemy teleinformatyczne, w tym serwery. Dostęp do zgromadzonych przez operatorów i dostawców usług danych ma zapewnić organom ścigania możliwości dotarcia do elektronicznych śladów popełniania przestępstw, które w przypadku braku obowiązku zapisu szybko są usuwane z pamięci komputerów. Ogólne zasady dotyczące przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej zostały zebrane w 2002 r. w dyrektywie 2002/58/WE o prywatności i łączności²². Zgodnie z art. 6 i 9 tej dyrektywy dane o ruchu i lokalizacji powstałe w wyniku korzystania z usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, ponieważ generalnie nie są już potrzebne. Wyjątek stanowią dane niezbędne w celu naliczania opłat i rozliczeń międzyoperatorów. Za zgodą abonenta pewne dane mogą być też przetwarzane w celach marketingowych.

5. Cyberterroryzm wyzwaniem dla Rady Europy

Praca nad doskonaleniem przepisów prawnych do zmieniających się warunków wynikających z szybkiego postępu technologicznego przebiegała na obszarze europejskim dwutorowo. Walkę z przestępczością komputerową podjęła nie tylko EU, ale również Rada Europy – instytucja częstokroć mylona z instytucjami Unii: Radą Europejską i Radą Unii Europejskiej. Pierwsze prace będące uregulowaniem zagadnień związanych z prędko rozprzestrzeniającą się cyberprzestępczością zostały podjęte właśnie przez Radę Europy.

²²Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

23 listopada 2001 r. Rada Europy przyjęła konwencję o cyberprzestępczości (ang. Convention on Cybercrime²³), dokument uznawany później za jedno z największych osiągnięć rady w obszarze ochrony społeczeństwa przed cyberprzestępczością. Jego uchwalenie uzasadniano silną potrzebą podjęcia zdecydowanych działań w celu uogólnienia zasad zwalczania i ścigania cyberprzestępców oraz procedur ich ekstradycji z krajów o bardzo restrykcyjnej, jak również liberalnej polityce. Jak napisano w preambule, nowe regulacje były reakcją na głębokie zmiany dokonujące się na skutek digitalizacji, konwergencji i trwającej globalizacji sieci informatycznych. Postępujący rozwój technologii informatycznych wywołał znaczny wzrost działań skierowanych przeciwko poufności, integralności i dostępności danych, sieci i systemów informatycznych. Jednym z narzędzi wspierających ten cel miało być przyjęcie właściwych przepisów prawnych. Konwencję podpisało wiele państw członkowskich, w tym również Stany Zjednoczone, Japonia, Kanada, RPA, jak również Polska. Sejm uchwalił ustawę 12 września 2014 r. Prezydent Bronisław Komorowski podpisał ją 28 października 2014 roku. Ustawa weszła w życie 19 listopada 2014 roku. Konwencja – zdaniem kancelarii prezydenckiej – w przyszłości będzie najefektywniejszym narzędziem międzynarodowej ochrony przed przestępstwami dokonywanymi z pomocą komputera.

Celem konwencji o cyberprzestępczości jest stworzenie jednolitych rozwiązań prawnych dla przeciwdziałania przestępczości w cyberprzestrzeni. Ustala ona katalog przestępstw komputerowych, wprowadza procedury dotyczące wykrywania i ścigania przestępczości komputerowej, określa też zasady współpracy międzynarodowej.

Pierwsza część konwencji poświęcona została środkom, jakie powinny zostać podjęte na szczeblu krajowym w obszarze prawa karnego i materialnego oraz procesowego. Zdefiniowano przestępstwa przeciwko poufności, integralności, i dostępności danych informatycznych oraz systemów. Zgodnie z przepisami omawianej konwencji państwa członkowskie powinny uznać za przestępstwa działania polegające na: umyślnym i bezprawnym dostępie do całości lub części systemu informatycznego (nielegalny dostęp), przechwytywaniu (z nieuczciwym zamiarem) za pomocą urządzeń technicznych niepublicznej transmisji danych informatycznych (nielegalne przechwytywanie danych), naruszeniu integralności danych (niszczeniu, wykasowywaniu, uszkodzaniu, dokonywaniu zmian), skutkującemu poważną szkodą oraz wprowadzaniu, transmisji, niszczeniu, wykasowaniu, lub dokonywaniu zmian w danych, które w rezultacie powodują poważne uszkodzenia funkcjonowania systemu informatycznego (naruszenie integralności systemu), jak i użyciu urządzeń, udostępnianiu haseł, programów

²³www.conventions.coe.int (dostęp: 11.07.2016).

komputerowych, czy też innych informacji, w celu popełnienia wyżej wspomnianych przestępstw (niewłaściwe użycie).

Za cyberprzestępstwo należy uznać także oszustwa i fałszerstwa komputerowe, przestępstwa powiązane z pornografią dziecięcą, naruszeniem praw autorskich i praw pokrewnych. Konwencja mówi, że pornografia dziecięca obejmuje materiał pornograficzny, który w sposób widoczny przedstawia: osobę małoletnią w trakcie czynności wyraźnie seksualnej; osobę, która wydaje się być nieletnią, w trakcie czynności wyraźnie seksualnej; realistyczny obraz przedstawiający osobę małoletnią w trakcie czynności wyraźnie seksualnej. Zakłada także, że karane ma być umyślne pomocnictwo lub podżeganie do popełnienia któregośkolwiek z przestępstw wymienionych powyżej.

Konwencja z listopada 2001 r. o cyberprzestępczości nie określa jednak dokładnie, jakie kary i środki powinny zostać zastosowane w razie popełnienia zdefiniowanych przestępstw komputerowych. Stwierdzono tylko, że każda ze stron konwencji powinna zagwarantować, aby były one karane za pomocą skutecznych, proporcjonalnych i zniechęających sankcji, obejmujących również pozbawionych wolności i sankcje pieniężne w przypadku osób prawnych. Część druga konwencji została poświęcona prawu procesowemu. Zobowiązano jej Strony do przyjęcia środków prawnych, umożliwiających nakazanie lub też uzyskanie niezwłocznego zabezpieczenia danych informatycznych, w tym także danych dotyczących ruchu, w szczególności gdy istnieje ryzyko ich utraty lub modyfikacji. Dane dotyczące ruchu oznaczają przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny²⁴. Stwierdzono, że dla realizacji wyżej wymienionego celu Strony konwencji powinny nadać właściwym organom wewnętrznym uprawnienia pozwalające na skuteczne nakazanie osobie przebywającej na terytorium Strony przekazania danych informatycznych, które są w jej posiadaniu w tym także pod jej kontrolą. Podobnie powinno być z nakazaniem dostawcy usług przekazania informacji odnoszących się do abonenta usług. Według samej konwencji, dane informatyczne odnoszące się do abonenta to wszelkie informacje w postaci danych informatycznych lub w dowolnej innej postaci, znajdujące się w posiadaniu dostawcy usług i odnoszące się do użytkowników tych usług, inne niż dane dotyczące ruchu lub treści, które pozwalają na ustalenie rodzaju usług komunikacyjnych, tożsamości użytkownika, adresu pocztowego oraz wszelkich innych informacji związanych z miejscem zainstalowania sprzętu komunikacyjnego, dostępnych na podstawie

²⁴Art. 1 *Konwencji o cyberprzestępczości*, bip.ms.gov.pl/Data/Files/_public/bip/prawo_eu/ue3/ue3in32.doc (dostęp: 11.07.2016).

umowy lub ustaleń dotyczących usług²⁵. Zamieszczono także wytyczne dotyczące uzyskania dostępu, jak i przeszukania oraz zajęcia przechowywanych danych w systemach informatycznych, w ich częściach, jak i na innych nośnikach służących do przechowywania danych. Podkreślono, że przyjęte środki prawne powinny obejmować także uprawnienia do zajęcia i zabezpieczenia systemu informatycznego lub jego części, wykonania i zachowania kopii całości lub części danych, uczynienia danych niedostępnymi lub usunięcia z systemu. Uprawnione organy powinny dodatkowo posiadać prawo do szybkiego rozszerzenia poszukiwań na inny system, jeżeli istnieje uzasadnione przypuszczenie, że poszukiwane dane są przechowywane w innym, niż założono początkowo, systemie informatycznym. Dużo uwagi przywiązano także do umożliwienia rejestrowania danych dotyczących ruchu oraz treści konkretnych przekazów w czasie rzeczywistym oraz zasad współpracy z dostawcami usług. Sporo miejsca poświęcono zagadnieniom związanym ze współpracą międzynarodową podejmowaną w celu ścigania i prowadzenia postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi lub dla celów zbierania dowodów w postaci elektronicznej, odnoszących się do przestępstw. W części ogólnej zdefiniowano między innymi zasady dotyczące ekstradycji, przekazywania informacji między Stronami konwencji z własnej inicjatywy oraz na podstawie wniosku o udzielenie wzajemnej pomocy prawnej. Przyjęcie rozwiązania polegającego na zobowiązaniu organów jednego państwa do wykonania określonych czynności procesowych na wniosek państwa drugiego jest wynikiem braku porozumienia co do przyjęcia środków „pozwalających na bezpośrednie działania organów procesowych jednego państwa na terytorium innego państwa, w tym przede wszystkim sprawdzenia zwartości danych zgromadzonych na znajdujących się tam systemach komputerowych przez użycie sieci komputerowej²⁶”.

W części zawierającej postanowienia szczegółowe zawarto wytyczne dotyczące niezwłocznego zabezpieczenia oraz ujawnienia przechowywanych w systemie informatycznym danych, znajdujących się na terytorium innego państwa będącego Stroną konwencji. Między innymi wskazano, jakie elementy powinien zawierać wniosek o zabezpieczenie dowodu oraz omówiono warunki odmowy wykonania wniosku. W zakresie pomocy prawnej, odnoszącej się do środków śledczych, w konwencji zawarto wytyczne regulujące wzajemną pomoc w umożliwianiu dostępu do przechowywanych danych, w szczególności gdy są narażone na ryzyko modyfikacji czy utraty całkowitej. Nadmieniono, że Strona konwencji bez zezwolenia drugiej Strony może uzyskać dostęp do danych publicznie ogólnie dostęp-

²⁵Art. 18 *Konwencji o cyberprzestępczości...*

²⁶J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, wyd. LexisNexis, Warszawa 2003, s. 329.

nych, niezależnie od szerokości geograficznej, lub gdy uzyska skuteczną i dobrowolną zgodę do ich ujawnienia od upoważnionej osoby. Dodatkowo zaakcentowano, że Strony powinny świadczyć sobie wzajemną pomoc prawną w gromadzeniu w czasie rzeczywistym danych dotyczących ruchu oraz treści określonych przekazów realizowanych za pomocą systemu informatycznego²⁷. Konwencja nakłada również na Strony obowiązek wyznaczenia punktu kontaktowego dostępnego całodobowo przez cały tydzień, w celu zapewnienia natychmiastowej pomocy międzynarodowej, w razie prowadzenia czynności śledczych lub postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi. Powstanie sieci punktów kontaktowych ma zapewnić wzajemną pomoc techniczną, umożliwić niezwłoczne zabezpieczenie lub ujawnienie przechowywanych danych informatycznych, znajdujących się na obszarze innego państwa, jak umożliwić łatwiejsze i szybsze gromadzenie dowodów, dostarczenie informacji o prawie oraz lokalizowanie podejrzanych²⁸. W Polsce taką rolę ma pełnić Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Służby Kryminalnej Komendy Głównej Policji. W dokumencie zapisano także możliwość dostępu do danych informatycznych znajdujących się na terytorium innego państwa.

6. Unia Europejska wobec cyberprzestępczości

UE jest jedynym w swoim rodzaju partnerstwem gospodarczym i politycznym między 28 krajami europejskimi, które razem zajmują większą część kontynentu. Działalność prawodawcza Unii Europejskiej ograniczała się początkowo do wydania dyrektyw precyzujących wymagania konieczne do harmonizacji innych aniżeli prawnokarne sposobów ochrony danych osobowych i prywatności. Jednym z najważniejszych aktów wydanych w tym celu była dyrektywa o prywatności i łączności, która nie zawierała postanowień odnoszących się do prawa karnego. Już w 1997 r. Parlament Europejski oraz Rada Unii Europejskiej uchwaliły dyrektywę dotyczącą przetwarzania danych osobowych oraz ochrony prywatności w sektorze telekomunikacyjnym²⁹. Szybko poddano ją rewizji i dnia 12 lipca 2002 r. wydano nowy akt który swym zakresem obejmował cały sektor komunikacji elektronicznej zwany dyrektywą o prywatności i łączności elektronicznej³⁰.

²⁷Część II Postanowienia szczegółowe Konwencji o cyberprzestępczości...

²⁸Art. 35 Konwencji o cyberprzestępczości...

²⁹Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. dotycząca przetwarzania danych osobowych oraz ochrony prywatności w sektorze telekomunikacyjnym, Dz. Urz. UE L24 z 30.01.1998, s. 1.

³⁰Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.

Omawiana dyrektywa jest uszczegółowieniem ogólnej dyrektyw 94/46/EU, która została uchwalona w celu stworzenia jedynie generalnych ram ochrony danych osobowych we Wspólnocie Europejskiej. Dyrektywa 2002/58/WE o ochronie danych w sektorze komunikacji elektronicznej ma zapewnić zastosowanie tych zasad w dynamicznie rozwijającym się sektorze komunikacji elektronicznej. Przyjęcie dyrektywy było odpowiedzią EU na poszerzający się zasięg sieci cyfrowej telekomunikacji, prędkie pojawienie się nowych usług telekomunikacyjnych oraz wzrost idącego za tym zagrożeniem prywatności i wolności użytkowników. Możliwość łatwego i systematycznego zapisywania komputerowego oraz przetwarzania danych dotyczących ruchu, czyli wszelkich danych przetwarzanych do celów przekazywania komunikatu online lub naliczania opłat za te usługi, zdaniem Komisji naraża prywatność użytkowników na nowe bezpieczeństwa, czemu więc mają przeciwdziałać przepisy owej dyrektywy³¹.

Poprzez przyjęcie dyrektywy 2002/58/WE ustawodawca zobowiązał dostawców publicznie dostępnych usług łączności elektronicznej do podjęcia właściwych środków technicznych i organizacyjnych, w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług. Dodatkowo, w wypadku pojawienia się ryzyka naruszenia bezpieczeństwa sieci, na dostawcę nałożono permanentny obowiązek poinformowania abonentów o zaistniałym ryzyku³². Ponadto, dyrektywa zobowiązuje wszystkie państwa członkowskie do zapewnienia przez ustawodawstwo krajowe, poufności komunikacji i związanych z nią danych o ruchu wykonywanej za pośrednictwem dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności, w kwestii poufności przekazu, zakazano słuchania, nagrywania oraz przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu przez osoby inne niż użytkownicy, bez uzyskania zgody osób zainteresowanych. Należy wziąć pod uwagę, że poufność nie ma jednakże zastosowania w wypadku przetwarzania danych celem udokumentowania faktu transakcji lub prowadzenia korespondencji handlowej. Dodatkowo dozwolone jest techniczne przechowywanie danych oraz dostęp do nich w celu wykonania lub ułatwienia transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub też w sytuacji, gdy jest to konieczne w celu dostarczenia usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika³³. Istotą tego przepisu stanowi generalna dopuszczalność wykorzystywania rozwiązań technologicznych dających usługodawcy dostęp do niektórych danych użytkowników końcowych. To, na jakich zasadach dostęp ten ma mieć miejsce, zależy już jednak od regulacji szczegółowych. Zgodnie z wolą ustawodawcy

³¹J. Gałczyński (red.), dz. cyt., s. 292.

³²Art. 4 Dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE...

³³Art. 5 ust. 3 Dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE...

państwa członkowskie powinny zapewnić, by sieci łączności elektronicznej mogły być wykorzystywane w celu przechowywania informacji na terminalu abonenta lub użytkownika o celach przetwarzania oraz prawie sprzeciwu wobec niego. Tego typu rozwiązanie to tzw. model opt-out, który z założenia opiera się na domniemaniu zgody na przetwarzanie³⁴.

Należy podkreślić, że dyrektywę 2002/58/WE można w pełnym zakresie stosować do Internetu. Niezamówiona poczta, czyli tzw. spam, to praktyka przekazywania jednostkom, z którymi wysyłającego nie łączą wcześniejsze kontakty, wielu niezamówionych, częstokroć wręcz niechcianych listów elektronicznych, najczęściej w celach handlowych i reklamowych³⁵. Otrzymywanie niechcianej poczty jest uciążliwe dla użytkowników oraz łączy się z naruszaniem ich prywatności. Na mocy omawianej dyrektywy dostarczanie niepożądanego poczty elektronicznej jest zakazane, podobnie jak wykorzystywanie automatycznych systemów wywołujących, bez ludzkiej ingerencji, faksów, lub poczty elektronicznej do celów marketingu bezpośredniego, chyba że na owe działania uzyskana została wcześniejsza zgoda użytkownika. W szczególności zakazano wysyłania poczty elektronicznej do celów marketingu bezpośredniego, gdzie przerobiono lub ukryto tożsamość nadawcy, w imieniu którego wysyłano komunikat, lub bez aktualnego adresu, na który odbiorca może wysłać wniosek o zaprzestanie takich komunikatów³⁶.

Z punktu widzenia walki z cyberterroryzmem największe znaczenie ma opracowana na początku 2005 r. przez Radę Unii Europejskiej decyzja ramowa w sprawie ataków na systemy informatyczne³⁷. Celem przyjętej 24 lutego 2005 r. decyzji było poprawienie współpracy właściwych organów państw członkowskich w dziedzinie ataków na systemy teleinformatyczne. Stwierdzono, że ataki na systemy, w szczególności te, będące częścią infrastruktury krytycznej państw członkowskich, stanowią ogromne zagrożenie dla osiągnięcia bezpieczniejszego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Ponadto, nowoczesne systemy informatyczne mają obecnie transnarodowy i transgraniczny charakter, co sprawia, że istotne luki i różnice w przepisach prawnych państw członkowskich utrudniają skuteczną walkę z atakami na te systemy. Uznano, że postęp w tej dziedzinie mocno przyczyni się do walki z przestępczością zorganizowaną oraz terroryzmem w szerokim pojęciu.

³⁴D. Adamski, *Europejskie prawo łączności elektronicznej – telefonia, telewizja, Internet*, wyd. Prawo i Praktyka Gospodarcza Sp. z o.o. Warszawa 2005, s. 291.

³⁵Tamże, s. 114.

³⁶Art. 13 Dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE...

³⁷Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne.

Omawiana decyzja zawiera definicje pojęć „system informatyczny”, „dane komputerowe”, jak i „bezprawność”, których zrozumienie jest kluczowe z punktu widzenia poprawnego pojmowania przyjętych rozwiązań. „System informatyczny” oznacza wszelkie urządzenie lub grupę podłączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskiwanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania. Dane komputerowe oznaczają w tym wypadku natomiast wszelkie przedstawienie faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do spowodowania wykonania funkcji przez system. Terminem „bezprawne” określono dostęp lub ingerencję na którą właściciel, nie udzielił zgody lub która nie jest dozwolona na mocy prawa krajowego³⁸.

W celu zbliżenia porządków prawnych uznano, że w każdym państwie członkowskim karany jako przestępstwo powinien być nielegalny dostęp do systemu informatycznego oraz nielegalna ingerencja w system jak również dane. Nielegalny dostęp do systemu informatycznego rozumiany jest jako umyślny, bezprawny dostęp do całości lub części systemu informatycznego. Państwa członkowskie mogą swobodnie zdecydować, czy jest on objęty oskarżeniem zawsze, czy też jedynie w sytuacji, gdy przestępstwo popełnione jest z naruszeniem bezpieczeństwa. Nielegalna ingerencja w system to bezprawne, umyślne, poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego przez wprowadzenie, przekazywanie, uszkodzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych. Natomiast nielegalna ingerencja w dane oznacza umyślne i bezprawne usunięcie, uszkodzenie, pogorszenie, zmianę, zatajenie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym. Karze podlegają także kierowanie, pomaganie, usiłowanie i podżeganie do popełnienia wyżej wymienionych przestępstw. Trzeba zaznaczyć, że każde państwo może decydować, że nie będzie karane jako przestępstwo usiłowanie uzyskania nielegalnego dostępu do systemu informatycznego³⁹. Do odpowiedzialności karnej może zostać pociągnięta nie tylko osoba fizyczna, ale również osoba prawna. Zastosowanie tej sankcji powinno obejmować nie tylko kary grzywny, ale również kary finansowe. Wśród przykładów innych sankcji wymieniono: wyłączenie z uprawiania do przywilejów lub pomocy publicznej, czasowy lub stały zakaz prowadzenia działalności gospodarczej a także umieszczanie pod nadzorem sądowym oraz nakaz likwidacji. Skuteczna walka z prze-

³⁸Art. 1. *Decyzji ramowej Rady 2005/222/WSiSW...*

³⁹Art. 5 *Decyzji ramowej Rady 2005/222/WSiSW...*

stępczością komputerową wymaga ścisłej współpracy, ale także szybkiej wymiany informacji pomiędzy państwami członkowskimi. Stąd też owe państwa powinny korzystać z istniejącej sieci operacyjnych punktów kontaktowych, utrzymanych 24 godziny na dobę w dyżurze, w celu zwalczania omawianej cyberprzestępczości. Wszystkie państwa członkowskie UE zostały zobowiązane do podjęcia niezbędnych środków w celu dostosowania przepisów prawa krajowego do przepisów ujętych w decyzji ramowej do dnia 16 marca 2007 roku. Do tego dnia państwa członkowskie miały przekazać Sekretariatowi Generalnemu Rady oraz Komisji teksty wszelkich przepisów przenoszących do ich prawa krajowego obowiązki nałożone na nie na podstawie omawianej decyzji ramowej. Natomiast do dnia 16 września 2007 roku stopień spełnienia wymagań określonych w opisywanej decyzji powinien zostać oceniony przez Radę.

Sieci łączności oraz systemy informacyjne stały się narzędziami wszechobecnymi, a ich bezpieczeństwo wzbudza coraz większe zainteresowanie społeczeństwa. W celu zapewnienia wysokiego i skutecznego poziomu bezpieczeństwa, Unia Europejska, 10 marca 2004 roku, utworzyła Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), która doradza Komisji oraz państwom UE, a także koordynuje środki podejmowane przez nie w celu zabezpieczenia swoich sieci i systemów informacji⁴⁰.

Agencja ma stać się ośrodkiem ekspertyzy ds. zagadnień związanych z bezpieczeństwem internetowym, ma zapewnić pomoc władzom państw członkowskich, a w szczególności ich zespołom interwencyjnym, w przypadku nadzwyczajnych sytuacji związanych z systemami informatycznymi. Ma opracować ekspertyzy o wysokim poziomie szczegółowości i stosować je do stymulowania szerokiej współpracy między instytucjami sektora publicznego i porywanego. Ponadto ma wspierać Komisję w technicznych pracach przygotowawczych, dotyczących aktualizacji i rozwoju ustawodawstwa Wspólnoty, w dziedzinie bezpieczeństwa sieci informacji. Realizując poszczególne cele, Agencja ma odgrywać pierwszorzędą rolę w zapewnieniu bezpieczeństwa technologii cyfrowej w Europie. Co więcej Agencja ułatwia i rozszerza współpracę między różnymi podmiotami działającymi w sektorze publicznym i prywatnym w celu osiągnięcia odpowiednio wysokiego poziomu bezpieczeństwa w państwach UE.

Agencja ds. Bezpieczeństwa Sieci i Informacji składa się z zarządu obejmującego przedstawicieli państw UE i Komisji oraz przedstawicieli biznesu, ekspertów akademickich i konsumentów bez prawa głosowania, dyrektora naczelnego powoływanego przez zarząd na podstawie listy kandydatów zaproponowanych przez Komisję, a także ze stałej grupy udziałowców powoływanej przez dyrektora naczelnego. Grupa składa się

⁴⁰ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz. Urz. UE L 77 z 13.03.2004, s. 1.

z przedstawicieli przedsiębiorstw działających w przemyśle technologii informacyjnych i łączności, grup konsumenckich oraz ekspertów akademickich. Daje ona Agencji dostęp do najnowszych informacji, aby mogła ona reagować na wyzwania związane z bezpieczeństwem sieci. Agencja powinna wykonywać swoje zadania przy pełnej współpracy z państwami członkowskimi, a także powinna być otwarta na kontakty ze wspólnotą biznesową, przemysłem i innymi właściwymi udziałowcami⁴¹. Ponieważ sieci elektroniczne stanowią w znacznym stopniu własność prywatną, Agencja powinna bazować na danych wejściowych pochodzących z sektora prywatnego oraz na współpracy z tym sektorem. Wśród zadań, jakie postawiono Agencji, wymieniono zbieranie stosownych informacji w celu przeanalizowania ryzyka bieżącego i powstającego, a wyniki przekazać państwom UE oraz Komisji. Stwierdzono, że powinna zajmować się doradztwem Parlamentowi Europejskiemu, Komisji, organom europejskim, a także właściwym organom krajowym wyznaczonym przez państwa członkowskie, oferować na żądanie pomoc, rozszerzać współpracę między różnymi instytucjami działającymi w obszarze bezpieczeństwa sieci i informacji, między innymi poprzez organizowanie różnego rodzaju konsultacji i tworzeniu sieci kontaktów. Agencja ponadto:

- ułatwia współpracę między Komisją a państwami UE w zakresie rozwoju wspólnych metod, w celu zapobiegania problemom dotyczącym bezpieczeństwa;
- przyczynia się do wzrostu świadomości i dostępności aktualnych, celowych i wszechstronnych informacji na temat bezpieczeństwa sieci i informacji w stosunku do wszystkich użytkowników (między innymi poprzez promowanie wymiany najlepszych praktyk, w tym metod ostrzegania użytkowników oraz poszukiwanie współdziałania między inicjatywami w sektorze publicznym i prywatnym);
- wspiera Komisję i państwa UE w ich dialogu z przemysłem, w celu określania problemów dotyczących bezpieczeństwa sprzętu i oprogramowania;
- śledzi rozwój norm bezpieczeństwa w zakresie produktów i usług oraz promuje działania z zakresu oceny ryzyka i zarządzania nim;
- uczestniczy w wysiłkach UE zmierzających do współpracy z krajami trzecimi i organizacjami międzynarodowymi, w celu promowania globalnej propozycji dotyczącej bezpieczeństwa;
- wyraża własne wnioski, wytyczne i porady.

Warto także zwrócić uwagę o zaangażowaniu UE w zwalczaniu spamu. Stwierdzono, że aby skutecznie walczyć z tym zjawiskiem należy podjąć działania na poziomie ponadnarodowym. W tym celu została utworzo-

⁴¹Tamże.

na nieformalna grupa, składająca się z przedstawicieli państw członkowskich UE pod szyldem Contact Network of Spam Enforcement Authorities (CNSA). Jego zadaniem jest wymiana skarg między organizacjami narodowymi, wspólnie ściganie przestępstw oraz budowanie najlepszych praktyk w zakresie zwalczania przesyłanej na dużą skalę niezamówionej informacji handlowej, naruszającej postanowienia art. 13 dyrektywy 2002/58/WE o prywatności i łączności elektronicznej.

Ważnym krokiem podjętym na szczepku unijnym w kierunku efektywnej woli z cyberterroryzmem było przedstawienie przez Komisję w maju 2007 roku komunikatu do Parlamentu Europejskiego, Rady, oraz Komitetu Regionów zatytułowanego „W kierunku ogólnej strategii zwalczania cyberprzestępczości”⁴². Komunikat ten stanowił odpowiedź na stale zwiększającą się liczbę przestępstw informatycznych pełnionych w coraz bardziej wyrafinowany sposób i wykracających poza granice państwowe, jak i europejskie, wyraźnie rosnący udział w cyberprzestępczości zorganizowanych grup przestępczych oraz brak odzwierciedlenia tych trendów w liczbie aktów oskarżenia na podstawie transgranicznej współpracy oddziałów ścigania w Europie. Opracowanie strategii w tym obszarze ma uzupełnić działania UE mające na celu lepsze zwalczanie cyberprzestępczości na poziomie krajowym, unijnym i międzynarodowym. Strategia ma obejmować lepszą współpracę i koordynację polityczną między państwami członkowskimi, współpracę polityczną i prawną z krajami trzecimi, podnoszenie świadomości, szkolenia, konferencje, badania oraz ściślejszy dialog z sektorem przemysłu. Działanie rozpoczęło się od spotkania ekspertów w 2007 r. i jego wynikiem mogło być stworzenie centralnego punktu kontaktowego Unii Europejskiej (UE) w sprawach cyberprzestępczości.

Celem Komunikatu Komisji jest zapewnienie poprawy i ułatwienia koordynacji i współpracy między zespołami do spraw przestępczości internetowej, stworzenie przy współpracy z państwami członkowskimi, właściwymi organizacjami unijnymi i międzynarodowymi, a także innymi zaangażowanymi podmiotami spójnej strategii ramowej UE w sprawie zwalczania cyberprzestępczości oraz zwiększenie wiedzy na temat kosztów i niebezpieczeństw związanych z cyberprzestępczością.

Na wstępie komunikatu *W kierunku ogólnej strategii zwalczania cyberprzestępczości* stwierdzono unijną definicję cyberprzestępczości oraz ogólny podział przestępstw zaliczanych do tej kategorii. Cyberprzestępczość wg wymienionego komunikatu Komisji należy rozumieć jako „czyny przestępcze dokonane przez użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom”⁴³.

⁴² Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, *W kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r.*, COM (2007) 267.

⁴³ Tamże.

Zgodnie z definicją do grupy czynów zabronionych zaliczamy⁴⁴:

- tradycyjne formy przestępstw, takie jak oszustwo, czy fałszerstwo, jednakże popełnione przy użyciu elektronicznych sieci informatycznych i systemów informatycznych;
- publikację nielegalnych treści w mediach elektronicznych takich jak materiałów związanych z seksualnym wykorzystywaniu dzieci, podżeganiem ataków terrorystycznych, nakłanianie do nienawiści rasowej czy przemocy;
- wszystkie przestępstwa typowe dla sieci elektronicznej, tzn. ataki przeciwko systemom informatycznym w tym także hackerstwo.

W dalszej części komunikatu Komisja wspomina o istniejących instrumentach prawnych w walce z cyberprzestępczością na szczeblu unijnym jak i międzynarodowym. Podkreślono, że ze względu na transgraniczność cyberprzestępczości żadna strategia nie będzie do końca skuteczna, jeżeli wysiłki będą podejmowane tylko i wyłącznie w obrębie Unii. Za najbardziej skuteczne instrumenty uznano konwencję Rady Europy o cyberprzestępczości z 2001 r, o której wspomniano w drugim podrozdziale omawianego rozdziału. Komisja zobowiązała się do podejmowania działań celem zachęcenia państw członkowskich jak i krajów trzecich do jej ratyfikacji, a także do nawiązania współpracy ze Wspólnotą Europejską⁴⁵. W omawianym komunikacie Komisja zawarła wykaz szczegółowych działań, jakie zamierza podjąć celem zwalczania cyberprzestępczości. Jest to podjęcie ściślejszej współpracy operacyjnej między organami ścigania i organami sądowymi państw członkowskich, promowanie mocniejszego zaangażowania państw członkowskich i wszystkich organów publicznych w podejmowanie skutecznych działań przeciw cyberprzestępczości oraz przeznaczanie odpowiednich zasobów na zwalczanie tego rodzaju przestępstw ze szczególnym uwzględnieniem identyfikacji ofiar w materiałach związanych z wykorzystywaniem seksualnym rozprowadzanych online, zbadanie wspólnie z państwami członkowskimi zjawiska dobrze zorganizowanych masowych ataków na krytyczne infrastruktury informatyczne państw członkowskich w celu zapobiegania im i ich zwalczania, a także skoordynowanego reagowania na nie i wymiany informacji oraz najlepszych praktyk, rozpoczęcie dogłębnych badań w celu opracowania wniosku w sprawie specjalnego aktu prawnego UE dotyczącego kradzieży tożsamości oraz zawieranie dobrowolnych porozumień i konwencji na szczeblu unijnym między organami publicznymi i podmiotami publicznymi, zwłaszcza dostawcami usług internetowych, w odniesieniu do procedur blokowania i zamykania nielegalnych stron internetowych⁴⁶.

⁴⁴A. Suchorzewska, *Ochrona prawna systemów informatycznych...*, s. 164-165.

⁴⁵*Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów...*

⁴⁶Tamże.

Kolejnym podjętym przez Radę Europejską krokiem w celu zwalczania cyberprzestępczości było uzgodnienie strategii pracy i konkretnych środków służących zwalczaniu cyberprzestępczości. Opracowane przez Radę konkluzje w tym obszarze zostały przyjęte w listopadzie 2008 roku⁴⁷. W owym dokumencie Rada wyraziła opinię, że skuteczną odpowiedzią na cyberprzestępczość będą następujące działania:

- wzmocnienie partnerstwa między organami publicznymi a sektorem prywatnym w celu wykrywania i zapobiegania działalności przestępczej w tym obszarze;
- zwiększenie wiedzy i poprawienie stopnia wyszkolenia podmiotów zaangażowanych w walkę z cyberprzestępczością;
- wzmocnienie technicznej i międzynarodowej współpracy z państwami trzecimi.

Rada wezwała Komisję Europejską oraz jej państwa członkowskie do wprowadzenia środków technicznych w celu zwalczania cyberprzestępczości. Ponadto zobowiązała ją do przeprowadzenia oceny przygotowań do realizacji działań, o których mowa we wspomnianym dokumencie, a także do wprowadzenia w dłuższej perspektywie środków uzupełniających. W ramach kolejnego programu w dziedzinie wolności, bezpieczeństwa i sprawiedliwości, 26-27 czerwca 2014 Rada Europejska określiła strategiczne wytyczne dotyczące planowania ustawodawczego i operacyjnego na nadchodzące lata. Nowe wytyczne stanowią kontynuację programu sztokholmskiego (2010 – 2014). Po debacie na temat priorytetów UE w zakresie wolności, bezpieczeństwa i sprawiedliwości na lata 2015 – 2019, Rada Europejska określiła, że jednym z najważniejszych celów Unii jest stworzenie przestrzeni wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych i z pełnym poszanowaniem praw podstawowych. Rada Europejska zapowiedziała przegląd śródkresowy wytycznych w 2017 roku.

Podsumowanie

Cyberterroryzm to chcąc nie chcąc temat znajdujący się na piedestale problemów współczesnego świata. Analizowane zjawisko jest zresztą tak duże, że wystarczy spojrzeć na nagłówki książek, czasopism, wiadomości, czy internetowych publikacji „Cyberterroryzm jako nowe wyzwanie społeczeństwa”, „Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa”, „Cyberterroryzm znakiem naszych czasów”, „Cyberterroryzm jako nowa forma zagrożenia terrorystycznego”, „Cyberterroryzm zagrożeniem XXI wieku” to tylko kropla w morzu nagłówków mrozących krew w żyłach i spędzających sen z powiek każdego organu odpowiedzialne-

⁴⁷ Konkluzja Rady z dnia 27 listopada 2008 r. w sprawie uzgodnionej strategii pracy i konkretnych środków służących zwalczaniu cyberprzestępczości, Dz. Urz. UE C 062 z 17.03.2009 r., s. 16-18.

go za bezpieczeństwo państwa lub organizacji. Zwracając na to uwagę, na pocieszenie warto podkreślić, że w zakresie zwalczania zarówno zjawiska terroryzmu jak i cyberprzestępczości, prawo zostało na przestrzeni kilku ostatnich lat poważnie zmienione i uzupełnione, co dotyczy także i naszego kraju. W zakresie zwalczania cyberterroryzmu jesteśmy zasadniczo zgodni ze standardami międzynarodowymi, chociaż czytając nagłówki gazet o kolejnym ataku hackerskim i wyczyszczeniu kont bankowych, trzeba by się nad tym dobrze zastanowić. Jedno jest pewne: wraz ze wzrostem znaczenia Internetu w dzisiejszym świecie, ryzyko i znaczenie cyberterroryzmu będzie wzrastać. Będzie zatem wzrastać również zapotrzebowanie na instytucje zajmujące się stricte problematyką cyberterroryzmu, jak to ma się w przypadku choćby CERT Polska. Skutecznym sposobem walki jest również odpowiednia edukacja użytkowników. Niestety, w Polsce niewiele osób ma świadomość z powagi zagrożenia i wielu indywidualnych użytkowników nie wie, w jaki sposób zgłaszać zaobserwowane incydenty. Zagrożenie cyberterroryzmem, wraz z jakościowym i ilościowym rozwojem systemów komputerowych, będzie zatem proporcjonalnie rosło. Szczególnie zagrożone tym rodzajem terroryzmu wydają się państwa o wysokim stopniu uzależnienia infrastruktury od systemów informatycznych, co idzie w parze z powszechnym dostępem do sprzętu komputerowego.

Bibliografia

Pozycje zwarte

1. Adamski A., *Cyberterroryzm*, [w:] *Materiały z konferencji nt. Terroryzmu*, Wyd. Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2002.
2. Adamski D., *Europejskie prawo łączności elektronicznej – telefonia, telewizja, Internet*, wyd. Prawo i Praktyka Gospodarcza Sp. z o.o. Warszawa 2005.
3. Bógdał-Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Wyd. Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.
4. Ciekanowski Z., *Zwalczanie terroryzmu w Polsce*, wyd. PWST-E, Jarosław 2015.
5. Gołaczyński J. (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, wyd. LexisNexis, Warszawa 2003.
6. Kuźniar R., *Europejska Strategia Bezpieczeństwa*, „Polska w Europie” 2004, nr 2.
7. Liderman K., *Bezpieczeństwo teleinformatyczne*, Wyd. Naukowe PWN, Warszawa 2013.

8. Loska K., *Encyklopedia filmu science fiction*, wyd. Rabid, Kraków 2004.
9. Podolski A., *Program Haski (Bezpieczeństwo wewnętrzne i sprawiedliwość w latach 2005 – 2006) – Polska perspektywa*, Centrum Stosunków Międzynarodowych, „Raporty i Analizy” 2004, nr 14.

Akty prawne

10. Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne.
11. Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. dotycząca przetwarzania danych osobowych oraz ochrony prywatności w sektorze telekomunikacyjnym, Dz. Urz. UE L24 z 30.01.1998.
12. Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).
13. Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.
14. Dyrektywa Parlamentu Europejskiego i Rady 2004/38/WE z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium państw członkowskich.
15. Komunikat Komisji dla Rady i Parlamentu Europejskiego, *Obszar Wolności, Bezpieczeństwa i Sprawiedliwości: bilans programu Tampere i przyszłe kierunki działania z dnia 2 czerwca 2004 r.*, COM (2004) 401.
16. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, *W kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r.*, COM (2007) 267.
17. Konkluzja Rady z dnia 27 listopada 2008 r. w sprawie uzgodnionej strategii pracy i konkretnych środków służących zwalczaniu cyberprzestępczości, Dz. Urz. UE C 062 z 17.03.2009 r.
18. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz. Urz. UE L 77 z 13.03.2004.
19. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz.U. z 2011 r. Nr 222, poz. 1323.

Strony internetowe

20. www.tecfa.unige.ch (dostęp: 11.07.2016).
21. www.sjp.pwn.pl (dostęp: 11.07.2016 r.).
22. www.idg.pl (dostęp: 11.07.2016 r.).
23. www.abw.gov.pl. (dostęp: 11.07.2016)
24. www.ec.europa.eu. (dostęp: 11.07.2016)
25. www.internetworldstats.com (dostęp: 11.07.2016).
26. www.conventions.coe.int (dostęp: 11.07.2016).
27. bip.ms.gov.pl (dostęp: 11.07.2016).

Liczba znaków ze spacjami: 71 875