Wybrane aspekty zjawiska cyberterroryzmu

Mariusz Czyżak

Artykuł został poświęcony wybranym aspektom zjawiska cyberterroryzmu, które towarzyszy współczesnemu rozwojowi techniki, opartemu w znacznej mierze na teleinformatycznych narzędziach wymiany informacji i towarów. Wyjaśniono pojęcie cyberprzestrzeni oraz omówiono istotę cyberterroryzmu jako formy cyberprzestępczości o charakterze terrorystycznym. Przedstawiono ponadto zidentyfikowane obecnie formy działalności przestępczej i terrorystycznej w cyberprzestrzeni, a także wybrane regulacje polskiego systemu prawnego służące jej zwalczaniu.

cyberterroryzm, cyberprzestępczość, internet, prawo karne

Wprowadzenie

Rozwojowi techniki towarzyszą również próby wykorzystywania go do działalności godzącej w dobra prawem chronione. Niezbędna jest więc reakcja ustawodawcy zmierzająca do przeciwdziałania zjawiskom patologicznym i karania sprawców przestępstw popełnianych z użyciem środków technicznych. Problem ten w pełni znajduje swoje odzwierciedlenie na gruncie teleinformatyki. Bankowości elektronicznej, handlowi elektronicznemu, usługom telekomunikacyjnym, e–learningowi, i innym podobnym aktywnościom współczesnego człowieka, towarzyszą: rozsyłanie reklam i komunikatów (*spamming*), naruszenie tajemnicy telekomunikacyjnej, szeroko rozumiana przestępczość komputerowa, itp. Nie są to zjawiska nowe i nieznane zarówno w aspekcie prawnym, jak i etycznym. Warto w tym miejscu bowiem odnotować, że za pierwsze przestępstwo zbliżone do przestępstwa komputerowego, które można by nazwać „programowym", uznaje się zwykle incydent, który miał miejsce we Francji już w 1820 roku. Joseph Marie Jacquard – tkacz i wynalazca, skonstruował urządzenie przemysłowe do wiązania sieci, wykorzystujące perforowane karty do sterowania podnoszeniem nitek osnowy, jego pracownicy zaś, obawiający się utraty pracy, dopuścili się sabotażu, niszcząc wybudowaną maszynę[①].

Poddając ocenie moralnej problem wykorzystania do działań nieetycznych zdobyczy techniki, w szczególności w dziedzinie informatyki, wypada w tym miejscu przytoczyć pogląd katolickiej nauki społecznej na niczym nieograniczone korzystanie z postępu nauki i techniki. *„Dostęp do wielorakich rzeczywistych dobrodziejstw, jakich w ostatnim czasie dostarczyły wiedza i technika, łącznie z informatyką nie przynosi z sobą wyzwolenia spod wszelkiego rodzaju zniewolenia"*. Co więcej, doświadczenie uczy, *„że jeśli cała wielka masa zasobów i możliwości oddana do dyspozycji człowieka nie jest kierowana zmysłem moralnym i zorientowana na prawdziwe dobro rodzaju ludzkiego, łatwo obraca się przeciwko człowiekowi – jako zniewolenie."* [1]. *„Rozwój technologiczny może zrodzić ideę samowystarczalności techniki […]. Z tego też powodu technika przyjmuje dwuznaczne oblicze. Zrodzona z twórczości ludzkiej jako narzędzie wolności człowieka, może być ona pojmowana jako element wolności absolutnej, tej wolności, która chce abstrahować od ograniczeń, jakie rzeczy zawierają w sobie."* [2].

① *http://www.freelegaladvicehelp.com/.../First-Documented-Cybercrime.html*

Do jednych z najgroźniejszych zjawisk, które stanowią przejaw wykorzystania zdobyczy techniki wbrew ich istocie i przeznaczeniu, należy z pewnością działalność przestępcza i terrorystyczna prowadzona w tzw. cyberprzestrzeni.

Pojęcie cyberprzestrzeni

Cyberprzestrzeń (*cyberspace*) już samą nazwą jest związana z cybernetyką tj. nauką o procesach sterowania oraz przekazywania i przekształcania informacji w systemach (maszynach, organizmach żywych i społeczeństwach) [13]. Za autora tego pojęcia uznaje się Wiliama Gibsona. W swojej powieści zatytułowanej „Neuroromancer" napisał bowiem: *„To jest cyberprzestrzeń, konsensualna, halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność."* [4].

Analiza cech tej cybernetycznej przestrzeni prowadzi do wniosku, że jest to swoisty technosystem globalnej komunikacji społecznej, który odznacza się interaktywnością i multimedialnością. Został on ukształtowany w wyniku trzech procesów:

- integracji form przekazu i prezentacji informacji, która przyniosła ucyfrowienie tzw. infosfery,
- konwergencji systemów informatycznych i telekomunikacyjnych oraz mediów elektronicznych,
- integracji tzw. technosfery, która doprowadziła w rezultacie do powstania globalnej zintegrowanej platformy teleinformatycznej [5].

Cyberprzestrzeń stanowi zatem swego rodzaju przestrzeń komunikacyjną tworzoną przez system powiązań internetowych.

Jak już wspomniano, cyberprzestrzeń jest obszarem zarówno kooperacji pozytywnej, prowadzącej do rozwoju w sferze edukacji, komunikacji społecznej, gospodarki narodowej, bezpieczeństwa powszechnego, itp., jak i kooperacji negatywnej. Ta ostatnia aktywność może przybierać czworaką postać:

- cyberinwigilacji (obostrzonej kontroli społeczeństwa za pośrednictwem narzędzi teleinformatycznych w państwach autorytarnych i totalitarnych),
- cyberprzestępczości (wykorzystania cyberprzestrzeni do celów kryminalnych, w szczególności w ramach przestępczości zorganizowanej i przestępczości o charakterze ekonomicznym),
- cyberterroryzmu (wykorzystania cyberprzestrzeni w działaniach terrorystycznych),
- cyberwojny (użycia cyberprzestrzeni jako czwartego, obok ziemi, morza i powietrza, wymiaru prowadzenia działań wojennych) [5].

Istota cyberterroryzmu

Pojęcie cyberprzestępczości, zwanej również „przestępczością internetową" jako określenie zabronionych prawem działań, dokonywanych za pomocą komputera w sieci internetowej lub przy jej wykorzystaniu, godzących m.in. w bezpieczeństwo wykorzystania technologii informatycznych, znalazło już swoje miejsce zarówno w doktrynie nauk prawnych, jak i wśród ekspertów zajmujących się bezpieczeństwem teleinformatycznym [6]. Można przyjąć, że cyberprzestępczość obejmuje trzy kategorie przestępstw:

- tradycyjne przestępstwa popełniane z wykorzystaniem sieci i systemów informatycznych,
- publikację nielegalnych treści w mediach elektronicznych,

– inne przestępstwa typowe dla sieci łączności elektronicznej.

Dotychczas zidentyfikowano wiele ich postaci, a wśród nich [7], [8]:

– usługi finansowe on-line (m.in. propozycje udziału w wirtualnym hazardzie, tzw. oszustwa nigeryjskie,
– *cyberlaundering*, tzn. wykorzystanie bankowości i handlu elektronicznego do tzw. „prania brudnych pieniędzy",
– naruszanie praw autorskich (m.in. plagiaty),
– rozpowszechnianie pornografii i pedofilii,
– praktyki nieuczciwej konkurencji (np. *spamming*),
– nielegalny handel (np. antykami i dziełami sztuki, zagrożonymi gatunkami roślin i zwierząt, medykamentami, bronią, materiałami wybuchowymi, materiałami radioaktywnymi, wraz z instruktażem ich użytkowania); szpiegostwo gospodarcze,
– propagowanie treści nazistowskich, rasistowskich, itp.,
– *hacking* – włamania do komputera,
– nielegalne podsłuchy,
– *cybersquatting*.

Wszystkie przytoczone typy przestępstw mogą być oczywiście powiązane z działalnością terrorystyczną. Mowa tutaj m.in. o nielegalnym internetowym handlu bronią, propagowaniu terroryzmu na stronach internetowych, czy też zmasowanych atakach na krytyczne infrastruktury informatyczne poszczególnych państw [9], których przykłady przedstawione będą w dalszej części niniejszych rozważań.

W powszechnie przyjętym znaczeniu zjawisko terroryzmu rozumiane jest jako *„planowana, zorganizowana i zazwyczaj uzasadniana ideologicznie, a w każdym bądź razie posiadająca polityczne podłoże motywacyjne, działalność osób lub grup mająca na celu wymuszenie od władz państwowych, społeczeństwa lub poszczególnych osób określonych świadczeń, zachowań, czy postaw, a realizowana w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszającego rozgłosu w opinii publicznej oraz z reguły polegające na zastosowaniu środków fizycznych, które naruszają dobra osób postronnych, tj. takich, które nie dały wyrazu swemu negatywnemu nastawieniu do aktu terrorystycznego, jego celu lub uzasadnienia, ani nawet do określonej ideologii czy zapatrywań"* [10].

Do klasycznych form terroryzmu – na podstawie przedstawionego postrzegania tego zjawiska – zalicza się w szczególności: piractwo morskie i powietrzne, uprowadzanie osób w celu wymuszenia okupu lub podjęcia przez władze państwowe żądanej przez terrorystów decyzji politycznej, zamachy bombowe na infrastrukturę publiczną zmierzające do destabilizacji politycznej, akty terroru wymierzone przeciwko określonym grupom etnicznym, religijnym, itp. [11]. Jeszcze do niedawna katalog przestępstw popełnianych przez grupy terrorystyczne obejmował przede wszystkim przestępstwa skierowane przeciwko bezpieczeństwu lotnictwa cywilnego oraz przestępstwa przeciwko życiu, zdrowiu i wolności osób. Mimo, że w ostatnich latach nadal znacząca część ataków terrorystycznych jest kierowana przeciwko ludności cywilnej, to jednak działania terrorystyczne nabrały wymiaru globalnego (z dotychczasowego regionalnego) i są coraz częściej wymierzone przeciwko członkom sił zbrojnych państw uznanych przez organizacje terrorystyczne za wrogie. Mowa tutaj w szczególności o sytuacji w Iraku i Afganistanie, gdzie zwalczanie działalności terrorystycznej przybrało postać walki zbrojnej, działalność terrorystyczna zaś, w tym z wykorzystaniem różnorodnych narzędzi technicznych, prowadzona jest przez członków Al-Kaidy na całym świecie.

Zatem można uznać, że współczesny terroryzm odznacza się trzema charakterystycznymi cechami [12]. Po pierwsze, akty terrorystyczne są przeprowadzane w sposób umożliwiający uzyskanie przez nie międzynarodowego rozgłosu. Po drugie, cechuje je wysoki stopień zorganizowania grup terrorystycznych. Po trzecie wreszcie, organizacje terrorystyczne dysponują obecnie pokaźnym zasobem środków ekonomicznych i technicznych, wykorzystując na masową skalę narzędzia teleinformatyczne, w tym internet, do działań skierowanych przeciwko społeczeństwu oraz aparatowi państwowemu wrogich krajów.

Czym jest więc cyberterroryzm? Zdaniem amerykańskiego eksperta do spraw cyberbezpieczeństwa D. E. Denninga, *„Cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien on skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczające szkody by stwarzać strach."* [13]. Jest przy tym obecnie najmniej przewidywalnym, m.in. z uwagi na powszechne korzystanie z sieci internetowej, instrumentem oddziaływania zorganizowanych grup terrorystycznych na funkcjonowanie infrastruktury krytycznej państwa, a więc krajowych systemów: łączności, energetyki, transportu, zaopatrzenia w wodę, finansowych, itd. [14].

Zgodnie z opiniami osób zajmujących się bezpieczeństwem teleinformatycznym, jeszcze do niedawna internet był wykorzystywany przez terrorystów zazwyczaj w niemal tym samym zakresie, co przez zorganizowane grupy przestępcze i indywidualnych przestępców, a więc w takich obszarach zachowań kryminalnych jak:

- włamania do komputerów (*hacking*),
- włamania do systemów informatycznych dla osiągnięcia korzyści (*cracking*),
- wykorzystanie programu umożliwiającego wejście do serwera z pominięciem zabezpieczeń (*back door*),
- podsłuchiwanie pakietów między komputerami i przechwytywanie haseł i loginów (*sniffing*),
- podszycie się pod inny komputer (*IP spoofing*),
- wirusy i robaki komputerowe,
- bomby logiczne,
- wyłudzanie poufnych informacji (*phishing*).

Nie doceniono jednakże, między innymi, propagandowych możliwości internetu. Tymczasem, od kwietnia 2004 roku, kiedy to Al-Kaida opublikowała w sieci odezwę wzywającą naród iracki do walki z okupantem, internet stał się narzędziem wojny propagandowej terrorystów islamskich, nie tylko dostarczając informacji o przebiegu wojny i przeprowadzanych atakach terrorystycznych, ale krzewiąc również ideę „świętej wojny", służąc rekrutacji członków grup terrorystycznych, czy też dostarczając instruktażu konstruowania bomb i dokonywania zamachów z ich użyciem, itp. [3].

Nie sposób nie wspomnieć również o powiązaniach istniejących między zjawiskami cyberterroryzmu i cyberwojny oraz cyberterroryzmu i cyberinwigilacji.

Jaskrawym przykładem pierwszego z nich stała się tzw. estońska cyberwojna z 2007 roku, kiedy to w następstwie likwidacji pomnika żołnierzy radzieckich w Tallinie, w ciągu kilku dni zaatakowano estońskie witryny rządowe, uniwersyteckie, bankowe i prasowe, doprowadzając do zaprzestania świadczenia usług bankowości elektronicznej on-line, zablokowania stron internetowych partii poli-

tycznych, itp. Kulminacja ataku nastąpiła 9 maja, w rocznicę zakończenia II Wojny Światowej. Ataków dokonywano z komputerów zlokalizowanych w ponad pięćdziesięciu krajach świata, a ustały one po około trzech tygodniach. Cyberwojna cechowała się, analogicznie jak cyberterroryzm: niskimi kosztami działalności, zaniknięciem granic państwowych, możliwością dokonywania nagłych i nieprzewidzianych ataków, anonimowością atakujących, minimalnym ryzykiem wykrycia ataku oraz możliwością sparaliżowania systemu wrogiego kraju [15].

Cyberinwigilacja jest również zjawiskiem pokrewnym cyberterroryzmowi. Za jedną z postaci terroryzmu uznawany jest bowiem terroryzm państwowy, którego istotą, a zarazem celem działań terrorystycznych, jest wymuszenie posłuszeństwa wobec aparatu władzy [12]. Jest oczywiste, że proceder taki nie jest możliwy bez inwigilacji społeczeństwa, w szczególności członków opozycji niedemokratycznego reżimu. Obecnie, cyberprzestrzeń i elektroniczne środki komunikacji jawią się jako wprost idealny instrument działań aparatu bezpieczeństwa w krajach niedemokratycznych. Może on przyjąć zarówno formę ograniczenia obywatelom dostępu do internetu (np. cenzura stron internetowych), jak i postać inwigilujących środków teleinformatycznych (np. podsłuchy, inwigilacja sieci telekomunikacyjnych), stanowiąc niemal doskonałe narzędzie kontroli społeczeństwa.

Rekapitulując, w znaczeniu ścisłym mianem cyberterroryzmu należy określić działalność terrorystyczną prowadzoną wobec systemów teleinformatycznych, w celu zniszczenia lub modyfikacji zasobów informacyjnych znajdujących się w tych systemach, a w konsekwencji utraty życia, zdrowia lub mienia przez ofiary ataku terrorystycznego. W znaczeniu szerokim natomiast, trzeba go utożsamiać z wszelkimi działaniami względem cyberprzestrzeni, w tym również fizycznymi zamachami na infrastrukturę teleinformatyczną oraz aktywnością ideologiczną w internecie [5].

Prawne aspekty zwalczania cyberterroryzmu

Jest oczywiste, że ze względu na szczególną szkodliwość społeczną cyberterroryzmu i zagrożenie jakie stwarza dla współczesnego świata, spotyka się on z wyraźną reakcją prawnokarną zarówno na gruncie prawa międzynarodowego – w imię zasady ścigania przestępstw, tzw. represji wszechświatowej [9, 16], jak i ustawodawstwa krajowego, gdzie zachowania uznane za przejawy cyberterroryzmu podlegają odpowiedzialności karnej bądź to jako czyny noszące znamiona klasycznych przestępstw terrorystycznych – określone na gruncie ustaw karnych szczególnych, bądź to jako tzw. „przestępstwa komputerowe" [17].

Polski ustawodawca pokusił się o zdefiniowanie przestępstwa o charakterze terrorystycznym w ustawie z 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu terroryzmowi [18], za które uznał:

- *„przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne, przestępstwa przeciwko bezpieczeństwu powszechnemu"* [18; art. 2, pkt 7],
- napaść na Prezydenta Rzeczpospolitej Polskiej [17; art. 134],
- napaść i znieważenie przedstawicieli państw obcych na terytorium Rzeczpospolitej Polskiej [17; art. 136].

Należy podkreślić, że w polskim prawie karnym poddano penalizacji przede wszystkim samo branie udziału w zorganizowanej grupie albo związku mającym na celu popełnienie przestępstwa o charakterze terrorystycznym, w szczególności cyberterrorystycznym (kara pozbawienia wolności od 6 mie-

sięcy do lat 8) [17; art. 258 § 2]. Zakładanie lub kierowanie grupą lub związkiem mającym na celu popełnienie takiego przestępstwa, podlega karze pozbawienia wolności na czas nie krótszy niż 3 lata [17; art. 258 § 4].

Przykładem aktu terrorystycznego, który może być popełniony z wykorzystaniem sieci i systemów informatycznych jest spowodowanie katastrofy komunikacyjnej [17; art. 173]. Współczesny ruch lądowy, wodny i powietrzny charakteryzuje się wysokim stopniem nasycenia środków transportu i infrastruktury transportowej rozwiązaniami teleinformatycznymi. Dotyczy to w szczególności komunikacji lotniczej, zwłaszcza systemu kontroli lotów i oprzyrządowania pokładowego samolotów. Dotychczas, w odniesieniu do zagrożenia atakami terrorystycznymi, transport lotniczy był kojarzony z braniem zakładników, towarzyszącym porwaniom samolotów [17; art. 166]. Obecnie, zarówno naziemne, jak i pokładowe systemy informatyczne stanowić mogą potencjalny przedmiot cyberataku terrorystycznego.

Warto zwrócić uwagę, że ustawodawca uznał stopień szkodliwości społecznej wspomnianego powyżej rodzaju aktu terrorystycznego za tak wysoki, że chroni życie i zdrowie ludzkie, a także mienie, wieloaspektowo. Poddał bowiem penalizacji również czynności przygotowawcze do umyślnego spowodowania katastrofy komunikacyjnej [17; art. 175] zarówno w formie rzeczowej np. podjęcia czynności polegających na ingerencji w system informatyczny lotniska, czy też pojedynczego statku powietrznego, zmierzających do spowodowania katastrofy, jak i osobowej w postaci porozumienia osób, których celem jest np. wspólny cyberatak na informatyczny system komunikacji w ruchu lotniczym. Analogicznie, przy wykorzystaniu narzędzi informatycznych może zostać popełnione przestępstwo sprowadzenia bezpośredniego niebezpieczeństwa wspomnianej powyżej katastrofy [17; art. 174]. Penalizacji podlega także spowodowanie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach, w sytuacji, gdy sprawca zakłóca, uniemożliwia lub wpływa w inny sposób na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji np. dotyczących tras przelotowych statków powietrznych [17; art. 165 § 1 pkt 4], a także niszczenie i uszkadzanie lub czynienie niezdatnym do użytku urządzenia nawigacyjnego albo uniemożliwienie jego obsługi np. drogą elektroniczną [17; art. 167 § 2].

Wspomnieć wypada również o kodeksowych tzw. „przestępstwach komputerowych", których konstrukcja prawna może stanowić podstawę odpowiedzialności za działania cyberterrorystyczne. Mowa tutaj w szczególności o przestępstwie udaremniania lub znacznego utrudniania dostępu do informacji zapisanej na komputerowym nośniku informacji osobie do tego uprawnionej [17; art. 268 § 2] oraz przestępstwie sabotażu komputerowego [17; art. 269].

W Kodeksie karnym [17; art. 268 § 2] określono również typ przestępstwa polegającego na niszczeniu, uszkodzeniu, usunięciu lub bezprawnej zmianie zapisu istotnej informacji na komputerowym nośniku informacji, którym jest materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej [19].

Przedmiotem ochrony prawnokarnej w przypadku sabotażu komputerowego jest informacja, która jest dobrem szczególnie ważnym w dobie społeczeństwa informacyjnego. Stanowi on typ kwalifikowany względem czynu zabronionego, o którym mowa powyżej [17; art. 268 § 2]. Za znamię kwalifikujące należy w tym przypadku uznać znaczenie przechowywanej informacji dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, samorządowej lub innego organu państwowego, która musi mieć wymiar szczególny, a dotyczyć może: rozmieszczenia elementów infrastruktury obronnej państwa; systemu kierowania komunikacją kolejową, lotniczą, drogową i wodną; danych szczególnie istotnych dla funkcjonowania danego organu administracji publicznej, itp. [11, 19]. Czyn ten polega na niszczeniu, uszkadzaniu, usuwaniu lub zmianach zapisu informacji. Analogicznie, karalności podlega ponadto niszczenie albo dokonanie wymiany nośnika informacji oraz

niszczenie lub uszkadzanie urządzenia służącego automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji [17; art. 269 § 2]. Przedmiotem czynu zabronionego nie jest tutaj już jednakże sam zapis informacji, ale jej nośnik lub urządzenie, o którym mowa powyżej, przy czym skutek przestępczego działania sprawcy sprowadzać może się również do utraty informacji.

Jak już wspomniano, jednym z najniebezpieczniejszych i szkodliwych, z uwagi na skutki, przejawów współczesnego cyberterroryzmu jest prowadzenie działalności propagującej terroryzm za pośrednictwem internetu. Mowa tutaj w szczególności o swego rodzaju *spammingu*, który podlega na gruncie przepisów powszechnie obowiązującego prawa odpowiedzialności karnoadministracyjnej i karany jest jako wykroczenie, jeżeli ma charakter handlowy [6], jakkolwiek niektóre projekty zmian legislacyjnych zakładają wprowadzenie karalności *spammingu* ideologicznego [6], [21]. Niemniej jednak, jako niezamówiona informacja elektroniczna o charakterze ideologicznym, propagującym terroryzm jako metodę prowadzenia walki, nie stanowi on przestępstwa, wykroczenia, ani nawet deliktu administracyjnego. Rozpowszechnianie tego typu informacji może jednak podlegać na gruncie obowiązującego porządku prawnego odpowiedzialności karnej w pewnych okolicznościach. Należy w tym miejscu bowiem dodać, że na gruncie kodeksu karnego [17; art. 255], penalizacji podlega m.in. publiczne nawoływanie do popełnienia przestępstwa, a także publiczne jego pochwalanie. W konsekwencji działanie polegające na propagowaniu działalności terrorystycznej lub przestępstw o takim charakterze podlega także odpowiedzialności karnej. Nawoływanie do popełnienia przestępstwa, tj. wzywanie do naruszenia ustawy karnej w celu terrorystycznym, może przybierać publiczny charakter, jeżeli – w postaci komunikatów przekazywanych za pośrednictwem sieci internetowej, chociażby w postaci *spamu* – dociera do znacznej i nieokreślonej liczby odbiorców internetu.

Podsumowanie

Cyberterroryzm jest zjawiskiem niezwykle szkodliwym zarówno dla społeczeństwa i prawidłowego rozwoju działalności gospodarczej, jak również dla infrastruktury krytycznej państwa. Różnorodność jego form sprawia, że stanowi pojęcie dość trudne do zdefiniowania, a zatem i zwalczania. O jego istocie świadczą bowiem zarówno wykorzystywane przez grupy i organizacje terrorystyczne rozmaite teleinformatyczne środki techniczne oraz charakter przestrzeni, w której są one wykorzystywane, jak również przyświecający im zawsze cel ideologiczno-polityczny. Z uwagi na zagrożenia towarzyszące funkcjonowaniu współczesnych struktur państwowych, w strategii bezpieczeństwa narodowego Rzeczpospolitej Polskiej z 2007 r. za nadrzędny cel sektorowy w dziedzinie bezpieczeństwa informacyjnego i telekomunikacyjnego uznano zapobieganie próbom destrukcyjnego oddziaływania na infrastrukturę telekomunikacyjną państwa przez obniżenie poziomu jej podatności na ataki, minimalizację skutków ewentualnych ataków na tę infrastrukturę, a także sprawne przywrócenie jej pełnej funkcjonalności [11]. Kluczowego znaczenia dla budowy systemu przeciwdziałania zjawisku cyberterroryzmu nabiera jego zdefiniowanie, umozliwiające identyfikację jego przejawów, oraz określenie zakresów odpowiedzialności i współdziałania podmiotów (publicznych i prywatnych) uczestniczących w systemie zwalczania tego procederu [3], [21], [22]. Niemniej jednak nie można nie doceniać przy tym prawnokarnych instrumentów zwalczania przestępczości, bez których niemożliwe byłoby skuteczne przeciwdziałanie takiemu szczególnie szkodliwemu społecznie zjawisku, jakim jest cyberterroryzm i zjawiska mu pokrewne.

Bibliografia

[1] Jan Paweł II: *Encyklika Sollicitudo rei socialis*. Kraków, KAI Sp. z o.o., 2007

[2] Benedykt XVI: *Encyklika Caritas in veritate.* Kraków, Wydawnictwo AA, 2009

[3] Szafrański J.: *Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?,* W: *Cyberterroryzm – nowe wyzwania XXI wieku.* Red. T. Jemioła, J. Kisielnicki, K. Rajchel. Warszawa, Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009

[4] Gibson W.: *Neuromancer*. Warszawa, Wydawnictwo Książnica, 2009

[5] Sienkiewicz P.: *Terroryzm w cybernetycznej przestrzeni.* W: *Cyberterroryzm – nowe wyzwania XXI wieku.* Red. T. Jemioła, J. Kisielnicki, K. Rajchel. Warszawa, Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009

[6] Czyżak M.: *Spamming i jego karalność w polskim systemie prawnym*, Pomiary Automatyka Kontrola, 2009, nr 7

[7] Filipkowski W.: *Internet – przestępcza gałąź gospodarki.* Prokurator, 2007, nr 1

[8] Wójcik J.W.: *Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne.* W: *Cyberterroryzm – nowe wyzwania XXI wieku.*, Red. T. Jemioła, J. Kisielnicki, K. Rajchel. Warszawa, Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009

[9] Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości, Bruksela, 22 maja 2007 r., KOM(2007)267

[10] Hanausek T.: *W sprawie pojęcia współczesnego terroryzmu.* Problemy Kryminalistyki, 1980, nr 143

[11] Marek A.: *Prawo karne.* Warszawa, Wydawnictwo C. H. Beck, 2001

[12] Sławik K.: *Terroryzm. Aspekty prawno-międzynarodowe, kryminalistyczne i policyjne,* Materiały sympozjum Wydziału Prawa Uniwersytetu Szczecińskiego. Poznań, Wydawnictwo PDW Ławica, 1993, s. 114-130

[13] Kisielnicki J.: *MIS. Systemy informatyczne zarządzania.* Warszawa, Wydawnictwo Placet, 2008

[14] Bógdoł-Brzezińska A., Gawrycki M. F.: *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa, Oficyna Wydawnicza ASPRA-JR, 2003

[15] Czepielewski M.: *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii).* W: *Cyberterroryzm – nowe wyzwania XXI wieku.* Red. T. Jemioła, J. Kisielnicki, K. Rajchel. Warszawa, Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009

[16] Europejska Konwencja o zwalczaniu terroryzmu, sporządzona w Strasburgu w dniu 27 stycznia 1977 r. (Dz. 1996 r. nr 117, poz. 557)

[17] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997, Nr 88, poz. 553, ze zm.)

[18] Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (Tekst jednolity Dz.U. 2003, Nr 153, poz. 1505, ze zm.)

[19] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, Nr 64, poz. 565, ze zm.)

[20] Górniok O., Hoc S., Przyjemski S. M.: *Kodeks karny. Komentarz.* Tom III. Gdańsk, Wydawnictwo Arche, 2001

[21] Nowakowski Z., Szafran H., Szafran R.: *Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw.* Rzeszów, RS Druk Drukarnia Wydawnictwo, 2009

[22] Rządowy program ochrony cyberprzestrzeni RP na lata 2009-1011, http://www.cert.gov.pl

Mariusz Czyżak

Absolwent Katolickiego Uniwersytetu Lubelskiego Jana Pawła II (1997 r.). Doktor nauk prawnych (2003 r.). Autor ponad trzydziestu publikacji, w szczególności z zakresu prawa karnego i prawa administracyjnego, poświęconych m.in. karnoadministracyjnym i prawnokarnym aspektom wykonywania działalności telekomunikacyjnej i pocztowej. W latach 1998–2001 zatrudniony w Centralnym Zarządzie Poczty Polskiej. Od 2001 r. zatrudniony kolejno w Urzędzie Regulacji Telekomunikacji, Urzędzie Regulacji Telekomunikacji i Poczty oraz Urzędzie Komunikacji Elektronicznej. W latach 2004–2008 adiunkt na Wydziale Administracyjno-Prawnym Akademii Polonijnej w Częstochowie. Od listopada 2006 r. Dyrektor Generalny Urzędu Komunikacji Elektronicznej.

e-mail: m.czyzak@uke.gov.pl