MARCIN SZCZUR

Terroryzm wyzwaniem i zagrożeniem współczesności

1. Podstawowa terminologia zjawiska terroryzmu

Zjawisko terroryzmu pojawiało się w historii już w czasach starożytnych, jednak obecnie, w dobie XXI wieku, przybrało ono wymiar międzynarodowy. Już od zarania dziejów wszelkiego rodzaju hordy bojowników, czy też grupy działaczy politycznychi społecznych stosowały krwawe metody celem realizacji własnych idei oraz przekonań. Dokonując przeglądu akcji terrorystycznych opisanych w literaturze z tegoż zakresu należy stwierdzić, że ich liczba jest wręcz ogromna, dlatego nie sposób przytoczyć tutaj wszystkich. Warto jednak odnotować, że omawiane zjawisko istnieje już od setek tysięcy lat, a zmianie ulega tylko nazewnictwo oraz terminologia bezpośrednio z nim powiązana.

Geneza terroryzmu przedstawia się niezwykle dynamicznie. Na uwagę zasługuje fakt, że w dzisiejszych czasach, aby przetrwać, terroryści ciągle muszą dostosowywać oraz uzupełniać własną działalność. Ewolucja, jakiej zostało poddane owo zjawisko powoduje, że w historii świata istnieją wydarzenia, które w sposób bezpośredni zmieniły obraz omawianego problemu. Mowa tu m.in. o ataku z 11 września 2001 r. Z całą pewnością ww. incydent można uznać za kluczowy właśnie z punktu widzenia przeobrażeń oraz modyfikacji. Odtąd bowiem terroryzm zyskał miano międzynarodowego zagrożenia, a o problemie jego zwalczania mówiono na całym świecie. Kwestie dotyczące bezpieczeństwa są codziennie na ustach całego świata. Jeszcze nie tak dawno temu, bo w XX wieku, głównym zagrożeniem dla ładu oraz spokoju społecznego

były wojny, bitwy oraz wszelkiego rodzaju operacje o charakterze militarnym.

Obecnie jednak najważniejszym zagrożeniem, wpływającym na bezpieczeństwo, jest właśnie terroryzm. To, co niegdyś uważane było za niedorzeczne i nierealne, dzisiaj stanowi światowe wyzwanie. Terroryzm ewoluuje oraz przybiera nowe wymiary i znaczenia. Aktualnie terroryści działają ciągle przy pomocy siły, jednak wraz z postępem mogą oni sięgać po coraz to nowsze rozwiązania z zakresu technologii czy informatyki.

Dokonując przeglądu dostępnej literatury próżno doszukać się jednej legalnej definicji terroryzmu. Na przeszkodzie stoi szereg czynników, zarówno politycznych, ideologicznych, religijnych, kulturowych, wojskowych, jak również indywidualnych. To, co dla jednych jest terroryzmem, inni uznają np. za usprawiedliwioną metodę walki narodowowyzwoleńczej lub obronę tożsamości religijnej[1]. Taka różnorodność jawi się ogromną złożonością pojęcia. Wolumen rodzajów i odłamów terroryzmu jest tak duży, że nie sposób pogodzić wszystkich stanowisk. Liczba dostępnych definicji sprawia też, że ciężko wybrać jedną kompletną, która w pełni odda istotę omawianego problemu. Nauka wielokrotnie podejmowała próby definiowania zjawiska terroryzmu, jednak zawsze były one mało owocne. Obecnie problem ten uległ umiędzynarodowieniu, dlatego też nauka po raz kolejny stanie przed zadaniem pełnego, całkowitego zdefiniowania. Czas pokaże, czy owe próby okażą się skuteczne.

Niepowodzenia w definiowaniu są problemem nie tylko nauki, lecz całej społeczności międzynarodowej. Nie wiedząc czym właściwie jest terroryzm, ciężko zaplanować rozsądne działania, mające na celu walkę z owym zagrożeniem. Przedstawiony „mankament" powoduje, że ciężko czasem odróżnić działania legalne od tych mających charakter zakazany.

Brak jednej legalnej definicji w nauce, doktrynach czy też aktach prawnych jest wyrazem tego, że zasadnym wydaje się doko-

[1] Z. Cesarz, E. Stadmuller, *Problemy polityczne współczesnego świata*, Wrocław 2000, s. 351.

nanie analizy wszystkich dostępnych sformułowań. Na podstawie owych wywnioskować możemy, czym właściwie jest terroryzm, jak również znaleźć w nich charakterystyczne określenia, którew większości także odpowiedzą nam na to pytanie. Wśród wyróżniających się elementów wymienić możemy m.in.: ścisły związek z polityką, używanie siły oraz przemocy celem realizacji własnych przekonań, stosowanie groźby i wszelakich środków nacisku, czy przeprowadzanie ataków, których skutki oraz następstwa wykraczać będą poza obrany cel lub określoną ofiarę.

Prób definiowania pojęcia terroryzmu, jak to już wcześniej zostało wspomniane, było bardzo dużo. Brak jednego wzoru jest niewątpliwie wyrazem niepowodzenia. Przyczyn w tym zakresie jest wiele. Mają one wymiar złożony i opierają się na wielu czynnikach. Dynamika oraz złożoność rozwoju działalności terrorystycznej są powodem tego, że próżno doszukać się stabilizacji. Głównymi przyczynami są odmienne stanowiska państw, ochrona własnych interesów, czy obawa o własne bezpieczeństwo. Definiowanie terroryzmu nastręcza wiele pytań oraz zagadek. To, co dla jednych będzie już terroryzmem, dla drugich może być czynem iście bohaterskim. Dokładne określenie tego elementu stosunków międzynarodowych wydaje się być niezwykle trudne. Próżno doszukać się także kompromisu pomiędzy zwolennikami islamu, wzywającymi do walki o własną religię, wynikającej z ich mentalności oraz przekonań, a zwolennikami pokoju, stabilizacji czy równowagi społecznej i kulturowej. Te dwa odmienne stanowiska są wyrazem rozbieżności już przy próbie jakiegokolwiek definiowania.

Podsumowując, na świecie istnieje wiele definicji terroryzmu. Prób ujednolicenia terminu było mnóstwo, jednak każda z nich okazywała się niepowodzeniem. Wpływ na taki stan rzeczy miało wiele czynników, przy czym do głównych zaliczyć można odmienność kulturowo-religijną oraz sprzeczne interesy. Moim zdaniem, pogodzenie tych odmiennych stanowisk oraz wypracowanie jednej, wspólnej, międzynarodowej formuły, byłoby krokiem milowym w zwalczaniu owego zagrożenia. To od współpracy wszyst-

kich zainteresowanych państw zależeć będzie, na jakim etapie będą rozwijać się badania oraz w jakim czasie dojdzie do zgodnego stanowiska w sprawie terroryzmu. Jedno jest pewne: sprawa dookreślenia oraz odpowiedniego nazwania zjawisk terrorystycznych powinna być priorytetem dla wszystkich państw, walczących z tym międzynarodowym niebezpieczeństwem.

2. Istota współczesnego terroryzmu

Terroryzm jako zjawisko poddawany jest nieustannie ewolucji. Obecnie przybrał on miano międzynarodowego zagrożenia XXI wieku. Jego gwałtowny rozwój spowodowany był wieloma czynnikami. Efektem ich wystąpienia było zastąpienie klasycznego terroryzmu, opierającego swe ataki na broni konwencjonalnej, terroryzmem nowym, którego działalność uzupełniana jest nowinkami z zakresu informatyki, techniki, biologii czy chemii. Istota współczesnego terroryzmu tkwi w jego złożoności. Powyższym wnioskom towarzyszy stwierdzenie, iż świat całkowicie wolny od terroryzmu to iluzja. Realne i zasadne jest jednak dogłębne poznanie terrorystycznego zagrożenia[2].

Wiek XXI utożsamia się z przełomem w zakresie walki z terroryzmem. Kluczowym momentem był wówczas zamach z 11 września 2001 r. Od tego momentu problem terroryzmu na stałe zakotwiczył się w postrzeganiu bezpieczeństwa światowego. Dokonując porównania zagrożeń terrorystycznych bezpośrednio przed zamachem z 11.09.2001 r., należy wskazać wiele różnic, których wyliczenie uzasadni nam, iż mamy do czynienia z czymś nowym. Zjawisko nowego terroryzmu jest jakościowo zupełnie inne od swojej klasycznej wersji. Jest ono bardziej niebezpieczne oraz trudniejsze do zwalczania. Postępująca globalizacja i nowości technologiczne stały się przyczyną tego, że stykamy się teraz z czymś zupełnie nieznanym dotychczas w skali świata. Patrząc na cechy, wyróżniające współczesny terroryzm, warto podkreślić ich

[2] S. Wojciechowski, *Terroryzm na początku XXI wieku*, Bydgoszcz–Poznań 2011, s. 230.

ścisłe powiązanie oraz wzajemną zależność. Zsumowanie tychże elementów daje zupełnie inny obraz omawianego zagrożenia, aniżeli jego wcześniejszy odpowiednik. Dokonując więc analizy, warto podkreślić następujące elementy charakteryzujące ten rodzaj terroryzmu. Zaliczyć do nich możemy m.in. silną motywację działania opartą na brutalnych metodach oraz dalekosiężnych skutkach, specyficzne środowisko nakierowane religią oraz ideologią, jak i dynamiczną strukturę współczesnych organizacji terrorystycznych. Powiązanie ze sobą tych wszystkich cech było źródłem wyodrębnienia nowego międzynarodowego zagrożenia. Omawiając istotę współczesnego terroryzmu, nie sposób przejść obojętnie obok źródeł jego finansowania. Ich pochodzenie przedstawia się różnorodnie. Zdobyte środki ugrupowania terrorystyczne przekazują na działania ogólne (rekrutacja, utrzymanie infrastruktury, szkolenia) oraz tzw. działalność specjalną, mającą ścisły związek z przygotowywaniem zamachów terrorystycznych.

Dokonując przeglądu literatury, wyróżnić możemy trzy główne kanały działalności finansującej terroryzm. Wśród nich wymienia się: wsparcie ze strony państw, środki mające korzenie w procederze kryminalnym, a także fundusze pochodzące od legalnych organizacji oraz z własnej działalności. Warto podkreślić tutaj ścisły związek finansowania z rodzajem prowadzonej aktywności terrorystycznej. Organizacje, prowadzące przedsięwzięcia na szeroko zakrojonym terenie potrzebują większych środków, natomiast ugrupowania lokalne – znacznie mniejszych. Jedne ograniczają się do legalnych zbiórek, datków czy darowizn, inne natomiast swe przychody opierają na procederze nielegalnym (narkotyki, prostytucja, porwania czy przemyty). Finansowanie terroryzmu jest problemem niezwykle trudnym do wykrycia. Od zawsze pozyskiwanie środków przez terrorystów owiane było tajemnicą. Na uwagę zasługuje ta ogromna różnorodność sposobów pozyskiwania środków. Należy tutaj podkreślić, że dzięki tej różnorodności, źródła finansowania „nie wysychają". Według mnie, terroryści, nawet przy pomocy stosunkowo niewielkich pieniędzy, są

w stanie dokonać ogromnych zniszczeń na skalę międzynarodową.

Ciekawym elementem charakteryzującym istotę współczesnego terroryzmu są także narzędzia, dzięki którym terroryści realizują własne cele oraz zamierzenia. Szeroki zakres prowadzonych przedsięwzięć powoduje, że prócz składników materialno-technicznych, ogromną rolę przypisuje się również czynnikowi ludzkiemu. Szczególne znaczenie mają tutaj zamachowcy-samobójcy oraz dzieci. Liczba zamachów samobójczych jest tak ogromna, że nie sposób nie pokłonić się nad fenomenem owego zjawiska. Popularność przedstawionej metody związana jest w sposób bezpośredni z religią. Jak wynika z doktryn islamu, męczennik ma uprzywilejowaną pozycję po śmierci, dlatego oddanie swojego życia w imię własnej wiary jest sprawą honoru.

Walka w obronie tożsamości religijnej przyczynia się do tego, iż motywacja zamachowców ulega zwielokrotnieniu, a śmierć niewinnych osób jest usprawiedliwiana i uzasadniania obroną własnych idei oraz przekonań. Istota zamachów terrorystycznych polega na odpowiednim przygotowaniu. Precyzja, anonimowość, odpowiednie szkolenie, zarówno teoretyczne, jak i praktyczne, stają się wyrazem odpowiedniego przygotowania do wykonywanego zadania. Spoglądając z perspektywy organizacji, zamachy samobójcze przynoszą wiele korzyści. Precyzja oraz siła rażenia jest ogromna, dlatego takie ataki powodują bardzo duże straty – zarówno w sferze technicznej (np. eksplozja budynku), jak i ludzkiej (np. śmierć cywilów). Istotną rolę w organizacjach terrorystycznych odgrywają także dzieci. Wykorzystywanie nieletnich jawi się ogromną brutalnością, brakiem skrupułów oraz niezwykłą determinacją. Globalny terroryzm rozprzestrzeniony w XXI wieku związany jest właśnie z wykorzystywaniem dzieci do wszelakich operacji. Szkolenie już od najmłodszych lat daje rękojmię doskonałego przygotowania. Ugrupowania celowo wykorzystują naiwność oraz łatwowierność dzieci. Są one nie tylko celem ataków, ale także częstokroć ich wykonawcami. Kariera zamachowca-samobójcy rozpoczyna się często już w dzieciństwie.

Hamas, na przykład, finansuje placówki edukacyjne od przedszkola do uniwersytetu. Potencjalni zamachowcy są bardzo szybko dostrzegani, wybierani i celowo stymulowani w kierunku fanatyzmu[3].

Reasumując, istotą współczesnego terroryzmu jest jego międzynarodowy charakter. Jak pokazuje historia, swoje apogeum zagrożenie osiągnęło w XXI wieku. Obecnie to nie państwa są dla siebie zagrożeniem. To właśnie terroryzm jest największym niebezpieczeństwem dla świata. Wielu naukowców, badaczy zastanawia się, jak skutecznie z nim walczyć. Moim zdaniem, skutecznej metody nie ma i nie będzie. Państwa powinny konsolidować własne siły tak, aby przeciwstawić się rozwojowi tego zagrożenia. Jego siła jest bowiem tak duża, że całkowite jego wyeliminowanie to rzecz utopijna oraz mało realna. Twierdzę, iż głównym wyzwaniem przyszłości będzie odparcie niebezpieczeństwa pojawiającego się od niedawna tzw. cyberterroryzmu. Jego gwałtowny rozwój dopiero następuje, jednak w następnych latach może w znacznie rozleglejszy sposób oddziaływać na bezpieczeństwo świata, aniżeli jego wcześniejsza, klasyczna, militarno-bojowa odmiana.

3. Cyberterroryzm nowym zagrożeniem współczesności

Wiek XXI przez wielu naukowców, dziennikarzy, badaczy nazywany jest wiekiem technologii oraz informatyki. Oczywiście nie sposób nie zgodzić się w owym twierdzeniem. Liczba nowych rozwiązań z zakresu informatyki jest tak duża, że wymienienie wszystkich mogłoby stać się tematem osobnego artykułu. Warto jednak podkreślić w tym miejscu ścisły związek nowych rozwiązań technologicznych ze współczesnym terroryzmem. Omawiane zjawisko uważane jest za niezwykle dynamiczne oraz nieustannie rozwijające się. Aby przetrwać, terroryści muszą ciągle dostosowywać oraz uzupełniać swoją działalność. Ich odpowiedzią na tak nagły rozwój technologiczno-informatyczny było więc pojawienie

[3] W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm*, Warszawa 2009, s. 224.

się nowego odłamu terroryzmu, mianowicie tzw. cyberterroryzmu.

Jeszcze niedawno temu, bo w XX wieku, nikt z ówcześnie żyjących nie zdawał sobie sprawy z tego, że komputer może być urządzeniem zarówno pomocnym, jak i niezwykle niebezpiecznym. Przełom wieku XX i XXI był momentem skomputeryzowania oraz połączenia wszelakich sfer ludzkiej egzystencji. Tak nagły rozwój był niewątpliwie swego rodzaju rewolucją oraz w sposób bezpośredni przyczynił się do poprawy jakości życia, jednak stał się także przyczyną i przełomem w rozwoju nowych zagrożeń. Niespodziewany atak na jeden ze składników całości może bowiem prowadzić do zakłócenia funkcjonowania pozostałych. Ten efekt domina jest podstawą opinii, że największym zagrożeniem XXI wieku mogą być właśnie ataki informatyczne. Warto odnotować, że zawsze wraz z pojawieniem się czegoś nowego, często pożytecznego dla społeczeństwa, powstaje zagrożenie bezpośrednio z tym związane. Zagrożeniem wynikającym z postępu technologiczno-informatycznego było właśnie wyodrębnienie się zjawiska cyberterroryzmu.

Aby dobrze zrozumieć istotę omawianego problemu, warto pochylić się nad jego terminologią oraz znaczeniem. Zainteresowanie nauki tematyką cyberterroryzmu pojawiło się już w latach 80. XX wieku. Dokonując analizy znanych definicji, zjawisko to zakwalifikować możemy w szeregi działalności szkodliwej oraz niebezpiecznej, realizowanej przy pomocy zdobyczy z zakresu informatyki czy technologii. Ciekawą definicję omawianego zjawiska przytacza Mark M. Pollitt, który twierdzi, że „cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany przeciw informacjom, systemom komputerowym, programom i danym, który prowadzi do oddziaływania na niemilitarne cele, przeprowadzony przez grupy narodowościowe lub tajnych agentów”[4]. Obecnie rozwój cyberterroryzmu przybiera na sile. Ilość pojawiających się jego definicji jest ogromna, dlatego też wybranie

[4] Http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (22.04.2014).

jednej, kompletnej oraz w pełni oddającej istotę omawianego problemu, jest rzeczą kłopotliwą i ciężką do zrealizowania. Powodem wielu sporów czy niedomówień są trudności w klasyfikowaniu zagrożeń. Ze względu na niesłychanie dużą ilość niebezpieczeństw czyhających w sieci, rzeczą podstawową oraz niezmiernie ważną wydaje się być odpowiednie usystematyzowanie. Spory dostrzegalne są na pierwszy rzut oka i to one stają się przyczyną niedomówień. Dla jednych bowiem pewien informatyczny atak jest już cyberterroryzmem, dla innych natomiast zalicza się do cyberprzestępstwa. Rozróżnienie tych dwóch pojęć to rzecz niezwykle trudna, ale jakże pożądana w zakresie samego zwalczania.

W dzisiejszych czasach posiadanie wiedzy jest największą wartością. Ten, kto ją zdobywa, może czuć się zwycięzcą. Przeniesienie wszelkich wojen do sfery teleinformatycznej wydaje się być więc kwestią czasu. Obecnie zjawisko terroryzmu ulega przeobrażeniom. Już dzisiaj trudno oczekiwać od terrorystów, aby ich ataki były prowadzone tylko w sposób konwencjonalny (przy użyciu broni, przemocy, siły). Wraz z postępem technologicznym rozwojowi ulegają ugrupowania terrorystyczne. Według mnie, w niedługim czasie całkowicie realne będzie postrzeganie terrorysty nie tylko jako zamachowca z bronią w ręku, lecz także jako człowieka z laptopem, którego wiedza będzie wyprzedzała rozwój technologiczno-informatyczny. Wiele osób zadaje sobie pytanie, dlaczego Internet stał się narzędziem tak chętnie wykorzystywanym przez terrorystów? Moim zdaniem, powodów jest kilka: po pierwsze, siła ataku jest znacznie bardziej rozległa, aniżeli podczas ataku konwencjonalnego, a zamach może być wykonany niemalże z każdego miejsca. Co więcej, chroni życie terrorystów, a jego przeprowadzenie jest znacznie tańsze. Posiada też dobry kamuflaż, połączony z trudnościami w wykryciu.

Cyberterroryzmjest zjawiskiem, w obliczu którego liczba ataków, w porównaniu z liczbą ataków konwencjonalnych, jest jeszcze stosunkowo niewielka. Wpływ na taki stan rzeczy ma wiele czynników. Po pierwsze, nie wszyscy terroryści przekonali się do siły, jaką posiada wiedza z zakresu technologii czy informatyki.

Starsze pokolenia terrorystów skupiają się na metodach konwencjonalnych, które ich zdaniem mają najlepszą moc propagandową. Po drugie, aby móc skutecznie organizować ataki w cyberprzestrzeni, potrzebna jest odpowiednia wiedza. Brak owej wiedzy oraz wyobraźni powoduje, że członkowie wielu ugrupowań nie zdają sobie sprawy z siły, jaką może przynieść atak na sieci komputerowe, bazy danych czy systemy informatyczne. Warto jednak dodać, iż wojna cybernetyczna wymaga nie tylko wiedzy samej w sobie. Jej efektywność uzależniona jest od posiadania ludzi odpowiednio do tego wyszkolonych. Specjaliści, o których mowa, nie weszli jeszcze na stałe w struktury ugrupowań terrorystycznych. Niemniej jednak, łatwo zauważyć rosnące zainteresowanie terrorystów nowymi technologiami. Organizacje takie, jak Hamas czy Hezbollah znane są ze szkolenia specjalistów w zakresie telekomunikacji i informatyki (a inne organizacje są o to podejrzewane), co świadczy o przygotowaniach do rozszerzenia działalności w tych dziedzinach[5].

Przestępczość internetowa stała się tematem niezwykle ciekawym. Istnieje bowiem szereg możliwości, jakimi dysponują terroryści w zakresie ataków w cyberprzestrzeni. Dotychczas zlokalizowano wiele różnorodnych postaci owego zagrożenia. Wśród nich wymienić możemy m.in.: podsłuchy mające charakter nielegalny, wszelkiego rodzaju włamania do komputerów, nielegalny handel różnymi rzeczami, przestępstwa bankowe czy praktyki nieuczciwej konkurencji. Przedstawione rodzaje przestępstw są jedynie przykładami, przytoczonymi w celu uświadomienia ogromnej złożoności oraz dynamiczności omawianego zjawiska. Każdy proceder może być bezpośrednio powiązany z działalnością terrorystyczną. Od czasu, kiedy Internet stał się tak popularny oraz powszechny, grupy terrorystyczne zaczęły dostrzegać jego wielki potencjał. Oczywiście niejako były do tego zmuszone, gdyż aby przetrwać, musiały otworzyć się na nowe technologie z zakresu informatyki. Moim zdaniem, w niedługim czasie możemy do-

[5] J. Adamski, *Nowe technologie w służbie terrorystów*, Warszawa 2007, s. 102.

świadczyć zastosowania aktów cyberterrorystycznych na szeroką skalę. Dlatego już teraz państwa powinny konsolidować siły oraz przeciwdziałać takowym zamiarom. Im później terroryści przekonają się do potęgi informatyki, tym korzystniej dla świata, gdyż państwa będą mogły lepiej przygotować się na odparcie ataków lub też ich udaremnienie.

Cyberterroryzm jako zjawisko ciągle ewoluuje. Już teraz dominuje pogląd, że aby przeprowadzić atak na ogromną skalę, nie potrzeba wcale wyszkolonych terrorystów-zamachowców, a raczej świetnych informatyków czy hakerów. Moim zdaniem twierdzenie, iż w dzisiejszych czasach nic ani nikt nie może czuć się bezpiecznie, jest niezwykle trafne. Zarówno cywilne, jak i wojskowe bazy danych i informacji zagrożone są atakami. Obecnie dostęp do informacji jest czymś mającym cenę większą niż śmierć niewinnych osób. Ten, kto posiada informacje, może czuć się wygranym. Ilość szpiegów, hakerów, złodziei komputerowych jest tak duża, że ich wykrycie staje się wręcz niemożliwe. Również ugrupowania terrorystyczne walczą o informacje. Ich działaniom towarzyszy ogromna determinacja oraz zaangażowanie.

Przykładów wykorzystania technologii oraz informatyki przez ugrupowania terrorystyczne jest mnóstwo. Warto podkreślić, że prócz ataków, terroryści wykorzystują nowe technologie do rozszerzania działalności reklamowo-propagandowej. Obecnie, w dobie rozwoju technologicznego, organizacje posiadają swoje strony internetowe, tworzą własne filmiki czy dodają zdjęcia w Internecie. Ta otwartość na zmiany, w opinii przeciętnego człowieka, może doprowadzać do sytuacji, w której ludzie będą mogli być bliżej danej organizacji oraz, z perspektywy codzienności, śledzić jej działalność.

Aby dobrze zrozumieć związek terrorystów z Internetem, warto wymienić kilka przykładów aktywności terrorystycznej w tym zakresie. Zaliczyć do nich możemy m.in. *flooding* – wysyłanie ogromnej ilości danych na określony adres sieciowy celem zaśmiecenia lub spowolnienia działania serwera, okupowanie sieci, polegające na korzystaniu z danego serwera przez bardzo dużą

ilość użytkowników na raz, przez co jego funkcjonowanie jest mocno ograniczone lub nawet niemożliwe, wysyłanie *koni trojańskich*, które wykonują określone zadania bez zgody użytkownika, *social engineering* – wykorzystywanie braku umiejętności osób, które posiadają dostęp do danej sieci. Ponadto terroryści wykorzystują takie metody, jak m.in. *sniffing* – działalność polegająca na śledzeniu kroków danej osoby po całej sieci, *stealingpasswords* – działalność polegająca na uzyskiwaniu zgody na dostęp do określonej sieci czy *Denial of Service* – blokowanie za pomocą wszelkich możliwych sposobów danej usługi bądź częstokroć całego serwera. Moim zdaniem, ciekawą metodą działalności terrorystycznej, połączoną w sposób bezpośredni z najnowszą technologią, jest tzw. *skimming*. Owa metoda polega na kopiowaniu zawartości karty płatniczej bez zezwolenia posiadacza, celem przechwycenia jej zawartości. Obecnie jest ona rzadko stosowana przez ugrupowania terrorystyczne, jednak z biegiem czasu może być użyta na szeroką skalę. Powodzenie owego przedsięwzięcia byłoby bowiem ogromnei z pewnością przyniosłoby ze sobą znaczne korzyści finansowe. Jak wiadomo, każda działalność, również ta terrorystyczna, nie może odbywać się bez finansów. Dlatego twierdzę, że skimming będzie doskonałą metodą na wzbogacenie się ugrupowań terrorystycznych. Bezpośrednio z ową techniką powiązany jest także tzw. *phishing*. Polega on na wyłudzaniu prywatnych danych, takich jak hasła do witryn internetowych czy numery kart kredytowych. Cyberwłamywacz prezentuje swojej ofierze formularz na witrynie internetowej lub też email do złudzenia przypominający oryginał[6]. Wszystkie przedstawione wyżej metody są dopiero na etapie „prenatalnym" w odniesieniu do funkcjonowania wśród terrorystów.

Jednak z biegiem czasu ugrupowania mogą posiąść odpowiednią wiedzę oraz umiejętności i zastosować owe rozwiązania na masową skalę. Korzyści mogłyby okazać się znaczne. Prócz finansów, na własną działalność terroryści pozyskiwaliby także wiele

[6] Http://www.chip.pl/artykuly/trendy/2009/11/phishing-lowienie-naiwnych (22.04.2014).

informacji, niezwykle cennych i ważnych z punktu widzenia bezpieczeństwa światowego.

Podsumowując, cyberterroryzm zalicza się do nowej generacji działalności terrorystycznej. Jest to odpowiedź terrorystów na rozwój technologiczny XXI wieku. Obecnie jego siła rażenia nie jest duża, jednak z biegiem czasu może on ulec znacznemu rozwojowi. Według mnie, cyberterroryzm jest wyzwaniem oraz zagrożeniem przyszłości. Szybkość i czas jego rozprzestrzeniania się zależy od wielu czynników. Wysoki poziom zabezpieczeń i utrudnianie dostępu do informacji dzięki różnym technikom informatycznym, powodują jego spowolnienie. Jednakże pewne jest, że można się spodziewać zastosowania przez terrorystów nowych form działania, właśnie w postaci cyberterroryzmu na światową skalę. Wywoła to wielkie straty, z uwagi na widoczne już dziś uzależnienie państw rozwiniętych od infrastruktury technologicznej (może nastąpić np. paraliż systemu zasilania energią elektryczną)[7]. Twierdzę, że w przypadku rozwoju cyberterroryzmu siła rażenia może być znacznie bardziej rozległa, aniżeli w przypadku działalności terrorystycznej prowadzonej przy pomocy konwencjonalnych środków. Dlatego tylko przemyślana strategia walki może uchronić świat przed paraliżem systemów informatycznych.

[7] K. Jałoszyński, B. Wiśniewski (red.), *Terroryzm. Diagnoza, zadania administracji publicznej w przeciwdziałaniu zjawisku*, Bielsko-Biała 2007, s. 193.