**Kuba Jołoszyński**

# Terroryzm niekonwencjonalny - perspektywa zmiany charakteru zagrożenia terrorystycznego we współczesnym świecie

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 15, 92-101

2014

**Kuba Jałoszyński**
Wyższa Szkoła Policji w Szczytnie

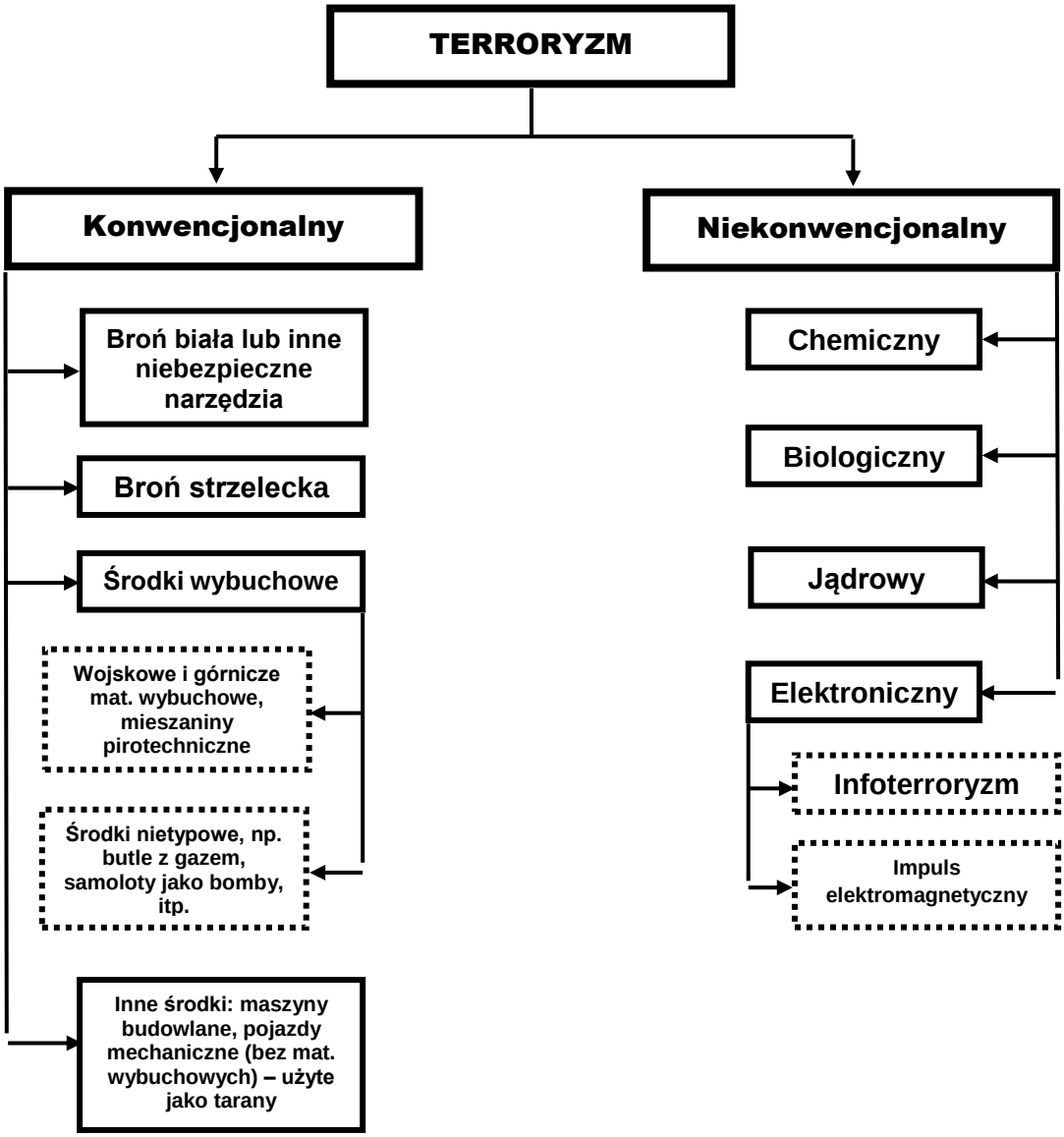
# TERRORYZM NIEKONWENCJONALNY – PERSPEKTYWA ZMIANY CHARAKTERU ZAGROŻENIA TERRORYSTYCZNEGO WE WSPÓLCZESNYM ŚWIECIE

Terroryzm we współczesnym świecie jest zjawiskiem niesłychanie złożonym i dynamicznym. Nie można go ująć w zadane sztywne ramy trendów i tendencji. Nie zastyga w czasie lecz podlega nieustannym, różnorodnym i chaotycznym często transformacjom[1]. Patrząc retrospektywnie w przeszłość minionych 50. lat widać jego przeobrażenia. Od terroryzmu lewackiego, walczącego „ze zgniłym" kapitalizmem, po terroryzm islamskich fanatyków, walczących z „diabłem" spersonifikowanym przez nich w USA i Izraelu oraz wszystkich państwach reprezentujących podobne wartości ekonomiczne i polityczne. Terroryzm nie jest zjawiskiem łatwym do zdefiniowania. Społeczność międzynarodowa ma do dziś problemy z wygenerowaniem wspólnej definicji tego zjawiska, a przyczyny takiego stanu rzeczy leżą miedzy innymi w[2]:

- **Dynamice i złożoności**, głębokim osadzeniu w realiach politycznych, społecznych i ekonomicznych;
- **Postępie technicznym**. Zamiast używać środków walki można wykorzystać np. wirus komputerowy, który to spowoduje nieodwracalne zniszczenia w systemach baz danych;
- **Ocenie danego aktu terroru**. To co dla jednych jest aktem bezdusznego terroryzmu dla innych czynem bohaterskim;
- **Mass mediach** – „darmowe" źródło „reklamy" działalności terrorystycznej.

Wśród wielu istniejących obecnie podziałów współczesnego terroryzmu kolejny z nich wyróżnia jego dwa podstawowe rodzaje: konwencjonalny i niekonwencjonalny (ryc. 1.), w którym to podstawowymi zmiennymi, wyróżniającymi go spośród innych, są środki walki jakimi posługują się terroryści. Środki służące do osiągnięcia celów terroryzmu, do unicestwiania istnień ludzkich, powodowania strat materialnych, wywoływania destrukcji i destabilizacji w państwie.

[1] BOLECHÓW B., *Terroryzm w świecie podwubiegunowym*, Toruń 2003, s. 33.
[2] ALEKSANDROWICZ T., *Terroryzm definicja zjawiska, ABW*, Emów 2003, materiały pokonferencyjne, s. 9 – 10.




Ryc. 1. Podział terroryzmu według kryterium wykorzystywanych do zamachu środków walki (Źródło: opracowanie własne)

Rozpatrując terroryzm niekonwencjonalny, ogromny skok technologiczny ubiegłego i początków obecnego stulecia, należy odnieść się do terroryzmu elektronicznego. Jest to forma terroryzmu związana z ogromną rolą jaką ma aktualnie w naszym świecie informatyka. Polega głównie na włamywaniu się do komputerowych baz danych, wprowadzaniu do programów komputerowych zakłóceń i wirusów w celu wywołania chaosu i dezinformacji. Może to sparaliżować systemy łączności, sieci bankowe, systemy obronne (w tym sterujące bronią masowego rażenia), może stać się przyczyną katastrof lotniczych i kolejowych znacznych rozmiarów. Współczesna historia wskazuje nam na skutki, jakie może wywołać awaria systemu komputerowego

sterującego przesyłem energii elektrycznej. Mogły się o tym przekonać Stany Zjednoczone jak też część państw europejskich.

Naukowcy, prowadząc swoje badania, odkrywają nowe możliwości współczesnych informatycznych „gadżetów". Hugo Teso, niemiecki programista i pilot samolotowy oznajmił, że jego nowa aplikacja *PlaneSploit* na smartfon z systemem Android jest w stanie przejąć kontrolę nad samolotem. Potencjalnie podatna na tego typu atak jest na przykład maszyna Airbus A380. Swój nowy wynalazek Teso zaprezentował na konferencji „Hack in the Box", która odbyła się w dniach 10-11 kwietnia 2013 roku w Amsterdamie. Praca nad programem *PlaneSploit* zajęła mu 3 lata. Smartfon z tą aplikacją ma możliwość łączenia się drogą radiową z systemem elektronicznym samolotu, dzięki czemu jest w stanie przejąć nad nim kontrolę. Skuteczność *PlaneSploit* Teso sprawdził na symulatorze sytemu elektronicznego samolotu pasażerskiego. Szczegółowe dane swojego wynalazku przekazał odpowiednim służbom, które mają zabezpieczyć elektronikę samolotów przed programami tego typu. Wynalazek Teso jest innowacją przydatną nie tylko w sytuacjach służących poprawie bezpieczeństwa. Strach pomyśleć, co by się mogło stać, gdyby *PlaneSploit* wpadł w ręce terrorystów[3].

Postindustrialne społeczeństwo drugiej połowy XX wieku weszło w nowy etap egzystencji, który można nazwać erą informacji. Każdy składnik narodowej siły staje się coraz bardziej zależny od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Wojsko, gospodarka, energetyka, media, system finansowy i transportowy są szczególnie z tym związane[4]. Naiwnie można byłoby twierdzić, że terroryzm „przejdzie obojętnie" obok możliwości wykorzystania cyberprzestrzeni do swoich celów. W dzisiejszych czasach, kiedy każdy właściwie aspekt naszego życia zależy od sieci informatycznych, terroryści mają ogromne pole do działania. Podczas gdy nowe technologie mające na celu obsługiwanie i ochranianie tych sieci są bardzo kosztowne, środki potrzebne do ich zaatakowania są stosunkowo niedrogie. W najprostszym przypadku potrzebny jest komputer, modem i dobry hacker. Dlatego nawet uboższe kraje mogą sobie pozwolić na atakowanie innych państw od tej newralgicznej strony.

Cały świat zachodni bazuje na rozbudowanej technologii komputerowej i dlatego konieczne jest zabezpieczenie się przed atakami terrorystycznymi w sieci. Informatyczne „środki walki" są bardzo pomysłowe i stanowią spore zagrożenie, szczególnie jeżeli zaatakowane zostaną komputery kontrolujące ważne instytucje strategiczne: system obrony, służbę zdrowia, przemysł itp. Do potencjalnych zagrożeń należą:[5]

- **wirusy komputerowe**, które mogą być wprowadzone do komputera „na odległość", poprzez Internet, a także przez „najemnego" informatyka;
- **bomby logiczne**, będące odmianą wirusa komputerowego, które mogą pozostawać uśpione przez długie lata, dopóki nie otrzymają odpowiedniego sygnału „do ataku";

[3] Na podstawie informacji medialnej przekazanej przez stację CNN w programie informacyjnym w 2013 roku.
[4] CIBOROWSKI L., *Walka informacyjna*, Toruń 1999, s. 7.
[5] BARNAS R.M., *Terroryzm. Od Asasynów do Osamy bin Ladena,* Wrocław 2001, s.16.

- **„podrzucanie”** do komputerów układów scalonych z wmontowaną informatyczną bombą-pułapką;
- **wirusy-robaki**, których zadaniem jest powielanie się bez końca i pożeranie zasobów systemu;
- **„konie trojańskie”**, nieprawidłowe kody wstawiane do legalnego oprogramowania w celu wykonywania niszczycielskich funkcji;
- **„tylne drzwi’ i „zapadnie”**, mechanizmy wbudowane w system przez programistę w celu umożliwienia producentowi „wślizgiwania się” do systemu, kiedy zachodzi potrzeba.

Odpowiednio przygotowany wirus komputerowy może wprowadzić do sieci fałszywe informacje, zmienić istniejący zapis, wziąć udział w działalności szpiegowskiej, wyszukując dane i przekazując je przeciwnikowi. Jeżeli uzyskają dostęp do właściwej sieci, potrafią, przynajmniej w teorii, uzbroić, rozbroić, a także nakierować broń na niezamierzone przez jej dysponenta cele. Najgroźniejszy, ten, którego informatycy i osoby zajmujące się zabezpieczaniem sieci boją się najbardziej, jest tzw. wirus samosterujący – inteligentna broń zorientowana na określony cel. Jej zadaniem nie jest ślepe wyrządzanie szkód. Zmierza on do przechwycenia określonego hasła, wykradzenia określonej informacji, zniszczenia konkretnego twardego dysku. W dziedzinie programowania jest to odpowiednik inteligentnego samosterującego pocisku[6].

Bez względu na to, jaki zastosujemy termin na określenie sprawców włamań do systemów informatycznych z pewnością mogą oni wyrządzić szkody państwom, krajom, a nawet, choć z pewną trudnością, armiom oddalonym o dziesięć tysięcy mil. Sprawozdanie National Research Council[7], zatytułowane „Computer in Crisis”, stwierdza: *Jutro terrorysta może wyrządzić większe szkody posługując się klawiaturą komputera niż bombą*[8].

Współczesny świat nie odczuł jeszcze skutków spektakularnego ataku w ramach infoterroryzmu. W opinii ekspertów, zajmujących się problematyką zagrożeń terrorystycznych, taki stan rzeczy wynika ze sceptycznego podejścia do tego typu środka walki przez liderów organizacji terrorystycznych. Są to ludzie dla których zamach terrorystyczny kojarzy się nierozerwalnie z koniecznością sięgania po środki powodujące namacalne unicestwienie istnień ludzkich i zniszczenia materialne. W sposób mistrzowski natomiast wykorzystują sieci internetowe do działalności propagandowej.

Drugą płaszczyzną internetowej aktywności, doskonale obecnie wykorzystywaną przez terrorystów, jest wykorzystanie sieci do porozumiewania się pomiędzy terrorystami. Działalność ta jest praktycznie nie do wykrycia. Do przesyłania informacji wykorzystywane są „anonimowe” – ze względu na brak tożsamości między ich właścicielem a użytkownikiem, końcówki internetowe. Urządzenia tego typu są powszechnie dostępne w kawiarenkach internetowych, poczekalniach dworów lotniczych, kolejowych, bibliotekach, szkołach i uczelniach wyższych, jak też innych miejscach publicznych[9].

[6] Tamże, s. 220.
[7] National Research Council (ang.) – Narodowe Centrum Badań Naukowych USA.
[8] TOFFLER A. i H., wyd. cyt., s. 220.
[9] Tamże, s. 141.

Problem wykorzystania sieci jako środka wymiany informacji jest na tyle istotny, że służby specjalne na całym świecie powołują specjalne komórki, których zadaniem jest monitorowanie Internetu pod względem wykorzystywania go przez organizacje terrorystyczne. Czas, kiedy zmieni się optyka terrorystycznego postrzegania zamachu, z krwawego spektaklu na spowodowanie destabilizującego ataku za pomocą cyberprzestrzeni (który to również może przynieść liczone w tysiącach ofiary ludzkie), zapewne nie jest tak odległa. Dlatego też ważnym jest wcześniejsze podejmowanie przedsięwzięć mogących, jeżeli nie zapobiec, to ograniczyć skutki takiego zamachu.

Każdy zamach terrorystyczny jest sam w sobie aktem zbrodni, którego efektem są ofiary – zabici i ranni. Terroryści nie ustają w dążeniu do wykorzystywania w swych zamachach środków walki pozwalających na spotęgowania skali jego skutków we wszystkich możliwych wymiarach – materialnym, psychologicznym, ekonomicznym i innym. Ich działania ukierunkowane są na atak z wykorzystaniem środków niekonwencjonalnych (środków zaliczanych do broni masowego rażenia – BMR). Prawdopodobieństwo użycia przez terrorystów BMR rośnie z kilku zasadniczych powodów. Po pierwsze skierowanie się współczesnego terroryzmu w kierunku maksymalizacji zadawanych strat. Powstają nowe coraz bardziej radykalne grupy zakładające właśnie wykorzystanie BMR jako idealnego sposobu nagłośnienia swych poglądów lub żądań lub ukarania potencjalnych przeciwników poprzez doprowadzenie do poziomu zadanych strat do skali masowej (BMR jest idealnym środkiem do tego celu). Po drugie rozpowszechnianie broni i technologii jądrowych, chemicznych lub biologicznych w szeregu krajach wspierających terroryzm umożliwia terrorystom dostęp do tej broni. Wreszcie po trzecie rozwój nauki i techniki, rosnąca dostępność komponentów i technologii niezbędnych do wytworzenia takiej broni powoduje coraz większe prawdopodobieństwo wytworzenia jej „domowym" sposobem. Opracowany w 2001 roku przez Biuro Sekretarza Obrony Stanów Zjednoczonych raport podaje, że siatka organizacja Osamy Bin Ladena od początku lat dziewięćdziesiątych zaczęła interesować się możliwościami pozyskania BJ[10]. Tenże raport podaje przykłady prób zakupienia przez agentów irańskich materiałów jądrowych pochodzących z byłego Związku Radzieckiego. Od 1998 zanotowano na świecie około 8000 ataków terrorystycznych z tej liczby około 60 można zaliczyć do ataków z wykorzystaniem środków zaliczanych do BMR. Środki zaliczane do BMR dzielimy na trzy zasadnicze grupy:

- Broń jądrową (ładunki nuklearne lub środki promieniotwórcze);
- Broń chemiczną (bojowe środki trujące, toksyczne środki przemysłowe, krystaliczne postaci toksyn bakteryjnych lub organicznych);
- Broń biologiczną (bakterie i wirusy wybranych chorób zakaźnych, niektóre rodzaje grzybów, riketsji, toksyny bakteryjne, zwierzęce, roślinne)[11].

Broń biologiczna jest jednym z najgroźniejszych środków masowego rażenia i nazywana jest często bronią masowego rażenia ubogich, ponieważ przy ogromnej skuteczności nakłady na jej pozyskanie są minimalne. Substancje biologiczne używane w BB (bakterie, wirusy, itp.) mogą występować w środowisku naturalnym samoistnie lub

[10] Proliferation: *Threat and Response*, Office of the U.S. Secretary of Defense Raport. Washington, 2001, s. 63.
[11] JAŁOSZYŃSKI K., *Organy administracji…,* s.

mogą być produkowane dla potrzeb służby zdrowia. Sytuacja taka powoduje, że ich pojawienie się w środowisku może nie zostać zauważone dostatecznie szybko. Dodatkową jej zaletą jej zaletą jest to, że charakteryzują ja niewielkie rozmiary i waga, co ułatwia transport, przechowywanie i wreszcie samo wykonanie ataku. Skuteczność tej broni polega między innymi na tym, że atakowany oprócz poniesienia znacznych strat musi ponosić kolosalne koszty związane z likwidacją skażenia oraz leczeniem wszystkich zarażonych szczepionkami itd. W przeprowadzonych w Stanach Zjednoczonych symulacjach ustalono, że koszty związane z zakażeniem 100 000 ludzi laseczkami wąglika (postać płucna) wyniosłyby 26,2 mld. dolarów. W przypadku tularemii koszt wyniósłby 5,5 mld. dolarów a w przypadku brucelozy 579 mln. dolarów[12]. Na szczęście dla cywilizowanego świata użycie broni biologicznej wymaga spełnienia pewnych warunków technicznych, które dotychczas nie zostały przez terrorystów opanowane. Pierwszym problemem jest zdobycie odpowiedniego materiału biologicznego będącego substratem wyjściowym do produkcji BB.

Atak terrorystyczny przy użyciu środków biologicznych przyniesie efekty dopiero po kilkunastu dniach lub kilku tygodniach od momentu wystąpienia. Sam moment wykonania takiego ataku może zostać niezauważony. O tym, że zostaliśmy zaatakowani, dowiemy się w momencie wybuchu epidemii lub, co jeszcze gorsze, pandemii mogącej objąć nawet kilka kontynentów. Praktycznie więc odpowiedź na pytanie, jak zachować się podczas ataku z użyciem środków biologicznych jest taka sama, jak odpowiedzi na pytanie, jak się zachować podczas pandemii? Przy gwałtownym wzroście liczby zachorowań może nastąpić załamanie możliwości służb sanitarnych. Będą problemy z fachową pomocą lekarska, dostępem do szczepionek itp. Dezorganizacja życia społecznego i systemów gospodarczych może doprowadzić do zerwania więzi społecznych, upadku praworządności, wzrostu przestępczości itd. Wszystko to może spowodować, że problem przetrwania okresu zanim wszystko wróci do normy będzie zależny wyłącznie od nas. Okres ten może potrwać nawet kilka miesięcy.

Po wrześniowych atakach w 2001 r., w Stanach Zjednoczonych mieliśmy wiele ataków z wykorzystaniem biologicznego środka walki — wąglika. Był on przesyłany do miejsc będących siedzibami urzędów publicznych w przesyłkach listowych. Stworzono procedury, które mają wspomagać reakcję człowieka, jeżeli podejrzewa, że otrzymany np. list, może zawierać szkodliwą substancje biologiczną.

Podkładanie ładunków wybuchowych, które z założenia mają eksplodować w celu spowodowania strat w ludziach i mieniu, należy rozpatrywać w kategoriach określanych w sztuce wojennej mianem rażenia *(destrukcyjne oddziaływanie na siły i środki przeciwnika*[13]*).* Jest to element we współczesnym świecie, z którym stykają się siły zbrojne i policyjne w państwie[14] – w tym z różną formą sposobu detonacji oraz miejsca podłożenia ładunku. Podkładanie bomb, jak zwykło się mawiać potocznie o tego rodzaju działalności przestępczej, stanowi dla wielu synonim terroryzmu[15].

[12] KAUFMANN A.F., MELTZER M.I., SCHMIDT G.P., *The Economic Impact of a bioterroristic Attack: Are Prevention and Postattack Intervention Programs Justfable?*, Emerging Infectious Diseases 1997, s. 74 oraz 46.

[13] *Regulamin działań taktycznych Wojsk Lądowych*, cz. II (pododdziały), Sztab Generalny WP, Warszawa 1994, s. 7.

[14] HUZARSKI M., *Zagadnienia taktyki wojsk lądowych*, Toruń 1999, s. 46.

[15] JAŁOSZYŃSKI K., *Współczesny wymiar antyterroryzmu*, Warszawa 2008, s. 195.

Zasadniczym elementem bomb, którymi posługują się terroryści i przestępcy, jest **ładunek wybuchowy**, przez który należy rozumieć: *kruszący materiał wybuchowy, znajdujący się w granatach, minach itp. lub w postaci np. kostek, przeznaczony do niszczenia obiektów i wojsk nieprzyjaciela (...)*[16].W wypadku działań terrorystycznych, wyżej wymienioną definicję można wykorzystać jako płaszczyznę do określenia tzw. **domowego urządzenia wybuchowego**.

Największy strach, poruszający wyobraźnię współczesnego świata, jest potencjalna możliwość wykorzystania przez terrorystów broni jądrowej. Powszechnie wiadomo, że organizacje terrorystyczne starają się zdobyć tego rodzaju broń. Niewątpliwie znaczącą aktywność w tym względzie wykazuje Al-Kaida, której lider Osama Bin Laden, już w latach 90. nie ukrywał dążeń do pozyskania tego typu broni niekonwencjonalnej: *Zdobywanie broni dla obrony muzułmanów jest religijną powinnością. Jeżeli uzyskamy taką broń, podziękuje za to Bogu. I jeśli usiłuję zdobyć taką broń, to tylko spełniam swój obowiązek. Dla muzułmanów najcięższym grzechem byłoby zaniechanie starań o taką broń, która może zapobiec zadawaniu zła muzułmanom przez niewiernych*[17].

Eksperci od zagrożeń terrorystycznych uspokajają, informując, że możliwość pozyskania klasycznej broni jądrowej przez organizacje terrorystyczne jest obecnie praktycznie żadna. Wskazują przy tym inny wariant dokonania zamachu, przy wykorzystaniu materiałów promieniotwórczych, po przez wyprodukowanie tzw. brudnej bomby. Obecny terroryzm jądrowy to przede wszystkim próby zdobycia materiałów promieniotwórczych[18]. Wiele faktów świadczy o dużym zainteresowaniu terrorystów czeczeńskich wykorzystaniu do zamachów materiałów promieniotwórczych[19]:

- Na początku 1995 roku czeczeńscy terroryści ukradli materiały radioaktywne z zakładu spalania odpadów Radon pod Groznym;
- W grudniu 1999 roku wojska rosyjskie odkryły pod Gudermesem dwie 200. litrowe beczki z odpadami radioaktywnymi, które zgodnie z dokumentacją miały być zniszczone w 1983 roku;
- W kwietni 2001 roku dwa kontenery z odpadami radioaktywnymi odkryto w Groznym – stwierdzono próby wyprodukowania z ich wykorzystaniem granatów i pocisków do granatników.

Powyższe próby pozyskania materiałów radioaktywnych przez terrorystów świadczą o ich aktywności w tym zakresie i dążeniu do stworzenia tzw. brudnej bomby. Jej konstrukcja oparta jest na połączeniu konwencjonalnego materiału wybuchowego oraz substancji promieniotwórczych. Materiał wybuchowy ma za zadanie rozprzestrzenienie – rażenie, środkiem radioaktywnym – skażenie terenu, a poprzez to ludzi znajdujących się w pobliżu eksplozji, jak też tych będących w dalszej odległości. Wiatr, w takiej sytuacji, rozprzestrzenia „niewidzialną śmierć" na znacznym obszarze, co w przypadku typowej bomby ograniczone jest praktycznie do zasięgu oddziaływania odłamków oraz fali uderzeniowej. Do głównych czynników, wpływających na siłę

[16] KORZUN M., *1000 słów o materiałach wybuchowych i wybuchu*, Warszawa 1986, s. 93.
[17] JAŁOSZYŃSKI K., *Terroryzm fundamentalistów islamskich*, Warszawa 2001, s. 65.
[18] ADAMSKI J., *Nowe technologie w służbie terrorystów*, Warszawa 2007, s. 85.
[19] Tamże, s. 86.

rażenia „brudnej bomby" należą[20]:

- Ilość rozprzestrzenionego materiału radioaktywnego;
- Właściwości promieniotwórcze użytego materiału radioaktywnego;
- Czynniki pogodowe;
- Teren na którym nastąpiła detonacja – budynek (jego wielkość) lub otwarta przestrzeń.

Skutki wykorzystania do zamachu terrorystycznego „brudnej bomby" związane byłyby z[21]:

- Rannymi oraz ofiarami śmiertelnymi ataku;
- Skażeniem środowiska naturalnego;
- Paniką oraz skutkami psychicznymi;
- Wysokimi kosztami działań ratowniczych – długofalowość takich działań;
- Skutkami politycznymi.

Przebywanie ludzi w rejonie skażonym materiałem radioaktywnym (oddziaływanie promieniowania jonizującego), w wyniku eksplozji „brudnej bomby", miałoby wpływ na prawidłowe funkcjonowanie ich organizmów.

Świadomość realnego bądź potencjalnego wystąpienia zagrożenia bezpieczeństwa budzi potrzebę przedsięwzięcia odpowiednich środków zaradczych, które to mogłoby ograniczyć lub też zapobiec ich powstaniu. Dotyczy to także zagrożeń o charakterze terrorystycznym, w tym związanych z możliwością stworzenia i użycia przez terrorystów „brudnej bomby".

Uznając atak terrorystyczny z wykorzystaniem materiałów promieniotwórczych za zagrożenie o najwyższym stopniu niebezpieczeństwa 15 lipca 2006 roku prezydenci Stanów Zjednoczonych – George W. Busch, oraz Rosji – Władimir Putin, wystąpili z inicjatywą międzynarodowej współpracy państw w obszarze zapobiegania i zwalczania terroryzmu jądrowego – nazwaną: *Globalną Inicjatywą Walki z Terroryzmem Nuklearnym*[22]. W ramach tego przedsięwzięcia organizowane są ćwiczenia, na które zapraszani są obserwatorzy z państw zaangażowanych w przedmiotową współpracę.

Walka i przeciwdziałanie wszelkim zagrożeniom terrorystycznym wymaga zaangażowania znacznego spektrum podmiotów administracji państwowej. Wymaga to podejmowania przez państwo przedsięwzięć o charakterze koordynacyjnym. Pozyskiwane informacje powinny podlegać weryfikacji, a także trafiać do odpowiednich służb w celu ich właściwego wykorzystania. Stąd też pierwszorzędne znaczenie ma właściwe zorganizowanie ośrodka koordynacji podmiotów państwa (służb specjalnych, resortów, agend rządowych, itp.) odpowiedzialnych za bezpieczeństwo w odniesieniu do zagrożeń terrorystycznych. Ośrodek kierowania (dowodzenia) systemem bezpieczeństwa antyterrorystycznego powinien być umiejscowiony w ośrodku najwyższych szczebli władzy wykonawczej w państwie, tak aby jego działanie nie było ograniczane przez szczeble pośrednie.

Gromadzenie informacji o terrorystach, ich zamiarach, organizacjach, w których

[20] Tamże, s. 3.
[21] Tamże, s. 5.
[22] Tamże, s. 15.

działają, leży w gestii służb specjalnych. Mają one pierwszorzędne znaczenie dla analizy zagrożenia terroryzmem państwa. Pozwalają skutecznie przeciwdziałać atakom terrorystycznym. Skuteczne prowadzenie działań antyterrorystycznych w obszarze przeciwdziałania zamachom na osoby podlegające ochronie wymaga wspólnych przedsięwzięć podmiotów odpowiedzialnych za bezpieczeństwo antyterrorystyczne w państwie – układu i militarnego pozamilitarnego.

Koordynacja i kierowanie działaniami antyterrorystycznymi musi odbywać się w oparciu o precyzyjne akty normatywne, zawierające hierarchiczną podległość oraz kompetencje poszczególnych podmiotów odpowiedzialnych za nie w sytuacjach prowadzenia działań o charakterze prewencyjnym (rozpoznawczych, wyprzedających), jak również podczas operacji związanej z zaistniałym aktem terroryzmu. Ważne jest określenie możliwości użycia w tego typu działaniach sił zbrojnych, w tym jednostek specjalnych mogących realizować zadania w ramach opcji siłowej rozwiązania powstałej sytuacji kryzysowej w wyniku zamachu terrorystycznego. Równie istotne jest formalne przypisanie konkretnych zadań, w odniesieniu do różnych metod działalności terrorystycznej, pomiędzy funkcjonujące w państwie podmioty przeznaczone do fizycznej walki z terroryzmem. Jest to rozwiązanie niezwykle pragmatyczne. Pozwala to na oszczędności finansowe, tak w sferze wyposażenia jak też szkolenia.

Bezpieczeństwo kosztuje. Jest to powszechnie znana prawda. Stąd też oszczędzanie na bezpieczeństwie może przynieść fatalne skutki w niedalekiej przyszłości. Nawet najlepiej wyszkolony człowiek nie będzie miał szans w walce z zagrożeniem, jeżeli nie będzie dysponował właściwymi, najnowszymi, zdobyczami techniki, stanowiącymi narzędzie w walce i przeciwdziałaniu terrorystycznemu zagrożeniu.

Nowa sytuacja wymaga innych niż dotychczas obowiązujące rozwiązań legislacyjnych. W ślad za deklaracjami poparcia dla amerykańskiej koalicji antyterrorystycznej muszą iść konkretne rozwiązania formalnoprawne umożliwiające przełożenie ich na praktyczny grunt, zwłaszcza zaś wykorzystanie wszystkich odpowiednich sił i środków, będących w dyspozycji państwa, do zabezpieczenia go przed potencjalnym atakiem terrorystycznym.

Świadomość społeczeństwa w zakresie współczesnych zagrożeń terrorystycznych, sposobów zachowania wobec zaistniałego ataku terrorystycznego, umiejętna współpraca z mediami w tym obszarze, stanowi pierwszorzędną rolę dla skuteczności działania systemu bezpieczeństwa antyterrorystycznego.

## Bibliografia

1. ADAMSKI J., *Nowe technologie w służbie terrorystów*, Warszawa 2007.
2. ALEKSANDROWICZ T., Terroryzm definicja zjawiska, ABW, Emów 2003.
3. BARNAS R. M., *Terroryzm. Od Asasynów do Osamy bin Ladena,* Wrocław 2001.
4. BOLECHÓW B., *Terroryzm w świecie podwubiegunowym*, Toruń 2003.
5. CIBOROWSKI L., *Walka informacyjna*, Toruń 1999.
6. HUZARSKI M., *Zagadnienia taktyki wojsk lądowych*, Toruń 1999.
7. JAŁOSZYŃSKI K., *Terroryzm fundamentalistów islamskich*, Warszawa 2001.
8. JAŁOSZYŃSKI K., *Współczesny wymiar antyterroryzmu*, Warszawa 2008.

9. KAUFMANN A. F., MELTZER M.I., SCHMIDT G.P., *The Economic Impact of a bioterrristic Attack: Are Prevention and Postattack Intervention Programs Justfable?*, Emerging Infectious Diseases 1997.
10. KORZUN M., *1000 słów o materiałach wybuchowych i wybuchu*, Warszawa 1986.
11. *Regulamin działań taktycznych Wojsk Lądowych*, cz. II (pododdziały), Sztab Generalny WP, Warszawa 1994.