Piotr Karasek
Katedra Kryminalistyki Uniwersytetu Warszawskiego

OGRANICZANIE MOŻLIWOŚCI ATAKU JAKO STRATEGIA DZIAŁAŃ ANTYTERRORYSTYCZNYCH[1]

Reducing the risk of attack as a strategy for counterterrorism

Wstęp

Zapewnienie społeczeństwu bezpieczeństwa przed atakiem terrorystycznym stanowi ciągłe i bieżące wyzwanie dla krajowych agencji bezpieczeństwa. Problem terroryzmu, choć we współczesnym rozumieniu tego zjawiska istniejący przynajmniej od XIX wieku[2], pozostaje nierozwiązany u swych źródeł, co wymusza opracowywanie i implementowanie szeregu metod i strategii zapobiegania zdarzeniom tego typu. Obejmują one stosowane z mniejszym albo większym powodzeniem działania defensywne – podejmowane przez organy ścigania i agencje bezpieczeństwa, ale też przez inne instytucje państwowe i organizacje pozarządowe. *Aktywne* metody przeciwdziałania zamachom terrorystycznym, zarówno przeprowadzanym przez zorganizowane grupy, jak i pojedyncze osoby, obejmują stosowanie dostępnych technik pracy operacyjnej oraz i prowadzenie działań zapobiegających radykalizacji. W celu obrony przed atakami wypracowano jednak także szereg działań *pasywnych*, zmierzających do uniemożliwienia dokonania ataku lub pozbawienia go skuteczności oczekiwanej przez sprawców. Obejmują one w szczególności ograniczanie dostępu do szeroko rozumianych środków i narzędzi ataku. W niniejszym artykule zawarto opis i wstępną klasyfikację tego rodzaju pasywnych działań obronnych, obejmujących zwłaszcza dążenie do pozbawienia sprawców zamachów

[1] Artykuł został przygotowany w ramach projektu FP7 PRIME realizowanego z funduszy Siódmego Programu Ramowego Unii Europejskiej (umowa grantowa nr 608354).

[2] Należy oczywiście mieć na uwadze, że od początku istnienia zjawiska „terroryzmu" ewolucji ulegały zarówno cele, metody działania, jak i ideologie towarzyszące grupom terrorystycznym i pojedynczym sprawcom zamachów. Na temat początków terroryzmu zob. J. Tomasiewicz, *Terroryzm na tle przemocy politycznej: zarys encyklopedyczny*, Apis, Katowice 2000, s. 11; R. Law, *Terrorism: A History*, Malden, MA, Polity Press 2009, s. 85–86.

dostępu do fizycznych i intelektualnych narzędzi ataku oraz dostępu do potencjalnych celów ataku.

Wspomniane działania pasywne polegające na ograniczaniu dostępności środków przeprowadzania ataków znajdują podstawy w teorii działań terrorystycznych. Zorganizowane ograniczanie dostępu do celów zamachów terrorystycznych stosowane jako metoda zapobiegania atakom zostało już zresztą, chociaż częściowo i wyłącznie w kontekście zabójstw politycznych, omówione przez M. Lipkę, który słusznie przywołując poglądy m.in. R.F White'a, R.L. Oatmana czy S. Stewarta i F. Burtona, podkreślił, że zachowania prowadzące do dokonania ataku terrorystycznego kształtowane są przez dwa podstawowe zbiory złożonych zmiennych[3]. Pierwszym z nich jest odpowiednia motywacja sprawców i ich determinacja w dążeniu do przeprowadzenia ataku. Drugim zaś, nie mniej istotnym, są faktyczne możliwości jego dokonania. Częściowo są one uzależnione od potencjału osobistego odpowiednio zmotywowanego sprawcy, który przy pewnej dozie determinacji może pokonać część trudności w zdobyciu odpowiednich środków ataku. Z założenia jednak, co wydaje się oczywiste, zamachowiec zamierzający dokonać zamachu z użyciem pistoletu musi mieć broń i amunicję oraz odpowiednie umiejętności, a także dostęp do obranego celu. Musi więc zdobyć sprzęt i odpowiednie informacje oraz przetworzyć je dla własnych potrzeb[4]. W praktyce możliwości przeprowadzenia ataku w konkretny sposób determinowane są dostępnością danego rodzaju środków[5].

Biorąc to pod uwagę, należy zauważyć, że pośród „środków" czy też „narzędzi" służących dokonaniu ataku terrorystycznego można wyróżnić ich dwie zasadnicze, wzajemnie się uzupełniające kategorie[6]:

a) fizyczne narzędzia i środki służące przeprowadzeniu ataku – w tym m.in. broń palna i amunicja, materiały pirotechniczne i inne materiały lub narzędzia niebezpieczne mogące posłużyć do tego celu;

---

3 M. Lipka, *Strategia ograniczania dostępności*, w: J. Cymerski, K. Wiciak (red.), *Przeciwdziałanie zagrożeniom powstałym w wyniku bezprawnego i celowego użycia bezzałogowych platform mobilnych*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji, Szczytno 2015, s. 171–194, za: R.F. White, *Asssassination discourse and political power*, „Assassination Research" 2008, t. 5, nr 2; R.L. Oatman, *Executive Protection: Rising to the Challenge*, ASIS International, Alexandria 2009, s. 95–97; Zob. też: S. Stewart, *Demystifying the Criminal Planning Cycle*, online: https://worldview.stratfor.com/article/demystifying-criminal-planning-cycle, dostęp 22 listopada 2017 r.

4 M. Lipka, *Strategia ograniczania…*, *op.cit.*, s. 172.

5 F. Iwaniuk, *Identyfikacja współczesnych zagrożeń bezpieczeństwa osób, obiektów i urządzeń objętych ochroną Biura Ochrony Rządu*, w: J. Cymerski, K. Wiciak (red.), op. cit., s. 64.

6 Zob. B.D. Barnes, *Confronting the one-man wolfpack: adapting law enforcement and prosecution responses to the threat of lone wolf terrorism*, „Boston University Law Review" 2012, t. 92, nr 1613, s. 1639.

b) wiedza, umiejętności i informacje niezbędne do przeprowadzenia skutecznego ataku – w tym m.in. wiedza i umiejętności w zakresie pozyskiwania, konstruowania i obsługi broni i innych niebezpiecznych materiałów, jak również wiedza i informacje quasi-wywiadowcze na temat potencjalnych celów ataku.

Ograniczenia w dostępie do środków należących do obu wymienionych wyżej kategorii są do pewnego stopnia wdrażane w praktyce działań wzmagających bezpieczeństwo. To właśnie one stanowią jedne z wspomnianych wcześniej *pasywnych* działań antyterrorystycznych; całkowite pozbawienie potencjalnych sprawców dostępu do takich narzędzi – w teorii – skutecznie zapobiegłoby występowaniu ataków terrorystycznych z ich wykorzystaniem. Z wielu powodów nie jest to jednak możliwe w praktyce i nie może być racjonalnie oczekiwane[7]. Dlatego też kolejnym kierunkiem rozwiązań w ramach szeroko rozumianego ograniczania możliwości przeprowadzania ataków jest:

c) fizyczna ochrona miejsc lub osób będących potencjalnymi celami ataków terrorystycznych. Fizyczne ograniczenie dostępności celów ataku zmierza do zapobieżenia atakowi, przeszkodzenia mu lub przynajmniej zminimalizowania szkód wyrządzonych ewentualnym atakiem[8].

Biorąc pod uwagę wyjątkowo silną motywację i determinację w działaniu sprawców ataków terrorystycznych, za istotny element systemu bezpieczeństwa trzeba uznać właśnie próby pozbawienia ich faktycznych możliwości działania z zastosowaniem ograniczeń mieszczących się w trzech wyżej określonych kategoriach. Celowe jest więc dokonanie krytycznej oceny ich skuteczności na podstawie informacji zgromadzonych w toku realizacji projektu FP7 PRIME oraz danych ze źródeł otwartych – zwłaszcza na temat przeprowadzonych dotychczas ataków terrorystycznych, w których sprawcy działali skutecznie pomimo istniejących już przecież ograniczeń. Zdarzenia terrorystyczne powtarzające się w państwach Europy w ciągu wielu ostatnich miesięcy nieodwracalnie zmieniają społeczne podejście do problemu bezpieczeństwa i przyzwolenie na ograniczenia praw i swobód z tym związane[9]. Tym bardziej więc należy zwrócić szczególną uwagę na możliwości przeprowadzania ataków przez sprawców działających pojedynczo lub w bardzo niewielkich grupach, jedynie inspirowanych szerszą ideologią ekstremistyczną.

---

7 Ibidem, s. 1640.

8 Centre for the Protection of National Infrastructure, *Protecting against terrorism*, online: http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf?epslanguage=en-gb, dostęp 10.09.2015, s. 15.

9 E. Ganley, G. Katz, *What's safe? European security changes after wave of terror attacks*, Global News, online: http://globalnews.ca/news/2857322/whats-safe-european-security-changes-after-wave-of-terror-attacks/, dostęp 12.05.2017.

Ograniczenie dostępu do fizycznych narzędzi i środków

Pozbawienie potencjalnego terrorysty dostępu do zaplecza technicznego jest zadaniem bardzo trudnym chociażby ze względu na szeroki wachlarz narzędzi, jakimi może on chcieć się posłużyć. Wdrożenie ograniczeń tego typu jest możliwe do zrealizowania tylko do pewnego stopnia i głównie w zakresie dostępu tylko do najbardziej niebezpiecznych narzędzi i uzbrojenia „wysokiej technologii". Ograniczenia tego rodzaju mają na ogół odpowiednie podstawy prawne – w zakresie dostępu do broni palnej i amunicji[10] czy nabywania, przechowywania, używania, transportowania, wytwarzania i obrotu materiałami wybuchowymi, bronią i technologiami wojskowymi[11]. Dostęp do niektórych niebezpiecznych materiałów jest też przedmiotem prawa międzynarodowego, m.in. Konwencji o ochronie fizycznej materiałów jądrowych[12] ustalającej międzynarodowe standardy dotyczące ich przechowywania czy Konwencji o znakowaniu elastycznych materiałów wybuchowych w celach detekcji[13], nakazującej ich znakowanie na etapie ich produkcji tak, aby niemożliwe było użycie „anonimowego" ładunku wybuchowego dużej mocy. Celem takich rozwiązań jest utrudnienie i kontrola dostępu do pewnych środków i narzędzi, a niekiedy, jak w przypadku tych najbardziej niebezpiecznych środków (zaawansowanego uzbrojenia, środków masowego rażenia) – wręcz likwidacja ich podaży na rynku prywatnym. W praktyce strategia ta nie jest jednak w pełni skuteczna, nawet w stosunku do najbardziej niebezpiecznych środków.

Przede wszystkim należy pamiętać, że do ataków może dochodzić z wykorzystaniem znacznie prostszych narzędzi, chociaż ich siła rażenia będzie wówczas stosunkowo niewielka. Dobrą ilustrację tego problemu mogą stanowić chociażby wydarzenia z Woolwitch (Wielka Brytania), gdzie w maju 2013 r. dwaj mężczyźni zaangażowani w poparcie islamskich grup terrorystycznych potrącili samochodem, a następnie używając jedynie tasaka i noża, brutalnie zamordowali brytyjskiego żołnierza[14]. Niecałe pół roku później w Kanadzie Martin Couture-Rouleau celowo wjechał samochodem w żołnierzy armii kana-

[10] Ustawa z dnia 21 maja 1999 r. o broni i amunicji (DzU 1999, Nr 53, poz. 549).

[11] Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (DzU 2001, Nr 67, poz. 679), Ustawa o materiałach wybuchowych przeznaczonych do użytku cywilnego z dnia 21 czerwca 2002 r. (DzU 2002, Nr 117, poz. 1007).

[12] Konwencja o ochronie fizycznej materiałów jądrowych wraz z załącznikami I i II, otwarta do podpisu w Wiedniu i Nowym Jorku w dniu 3 marca 1980 r. (DzU 1989, Nr 17, poz. 93).

[13] Konwencja w sprawie znakowania plastycznych materiałów wybuchowych w celu ich wykrywania, podpisana w Montrealu w dniu 1 marca 1991 r. (DzU 2007, Nr 135, poz. 948).

[14] BBC News, *Woolwitch machete attack leaves man dead*, online: http://www.bbc.com/news/uk-22630303, dostęp 7.09.2015.

dyjskiej, zabijając jedną osobę i drugą ciężko raniąc[15]. W 2014 r. w Nowym Jorku Zale H. Thomson siekierą zaatakował grupę policjantów, ciężko raniąc dwóch z nich, a tuż przed atakiem umieścił w Internecie nagranie popierające tzw. Państwo Islamskie[16]. Zamachy tego typu są przeprowadzane na małą skalę, nie wymagają specjalnego przygotowania, a do ich dokonania wystarczają narzędzia, do których dostęp bez ponoszenia dużych kosztów ma w zasadzie każdy. Ataki tego rodzaju (np. z użyciem samochodów, tzw. *run-over-attacks*, czy noży lub podstawowych narzędzi) są stosunkowo często przeprowadzane w ostatnim czasie także w krajach Europy[17], co częściowo wynika właśnie z ograniczeń w dostępie do innych, bardziej śmiercionośnych środków. Paradoksalnie świadczy to zarówno o skuteczności takich ograniczeń, jak i o jej braku. Oczywiście, na tej podstawie w żadnym razie nie jest jednak uprawniona konkluzja, że należałoby zakazać np. posiadania samochodów czy ostrych narzędzi w ogóle. Tym bardziej że dotychczas podejmowanych w niektórych państwach prób ograniczenia obecności noży w przestrzeni publicznej nie można uznać za sukces: polska ustawa o broni i amunicji zakazuje posiadania tzw. broni ukrytej (np. ostrza ukrytego w parasolce) i obrotu nią. Prawo węgierskie zabrania posługiwania się ostrzem o długości ponad 8 cm – z wyjątkiem noży służących do celów sportu, pracy lub domowego użytku[18]. Ustawodawca w Szkocji ustanowił nakaz posiadania licencji na sprzedaż noży i ostrych narzędzi innych niż te przeznaczone do domowego użytku[19]. Przykłady tego rodzaju można mnożyć, jednakże nie da się powiedzieć, że w którymkolwiek z tych krajów problem przestępczego wykorzystania ostrych narzędzi zniknął wraz z wprowadzeniem regulacji.

---

15 Sprawca został zastrzelony przez policję podczas pościgu, lecz jego związki z ideologią dżihadystyczną były znane organom ścigania, zob.: *Martin Couture-Rouleau, hit and run driver arrested by RCMP in July*, CBC News, 21 października 2014 r., online: http://www.cbc.ca/news/canada/montreal/martin-couture-rouleau-hit-and-run-driver-arrested-by-rcmp-in-july-1.2807078, dostęp 10.09.2015.

16 C. Pleasance, *Hatchet-wielding Muslim radical who attacked rookie New York cops spent months visiting jihadist websites and stalked officers for hours*, Daily Mail Online, 4 listopada 2014 r., online: http://www.dailymail.co.uk/news/article-2820584/Hatchet-wielding-Muslim-radical-attacked-rookie-New-York-cops-spent-months-visiting-jihadist-websites-stalked-officers-hours.html, dostęp 10.09.2015.

17 Bardzo dobrym przykładem ataku, podczas którego sprawca połączył obie te metody, może być ten przeprowadzony 22 marca 2017 r. Londynie. Zob.: *London attack: What we know so far*, BBC News z 7 kwietnia 2017 r., online: http://www.bbc.com/news/uk-39355108, dostęp 12.05.2017.

18 175/2003. (X. 28.) Korm. Rendelet, CompLEX 2003, online: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300175.KOR, dostęp 10.09.2015.

19 *Custodial Sentences and Weapons (Scotland) Act*, online: http://www.legislation.gov.uk/asp/2007/17/pdfs/asp_20070017_en.pdf, dostęp 10.09.2015.

Pomimo istniejących ograniczeń na przestrzeni ostatnich lat bardzo wiele ataków terrorystycznych zostało także przeprowadzonych z użyciem broni palnej – czy to w charakterze głównego narzędzia zamachu[20], czy też pomocniczo oprócz innych środków[21]. Istotne ograniczenia w dostępie do niej istnieją praktycznie w każdym państwie europejskim, choć zazwyczaj można je „obejść", np. występując o pozwolenie na broń sportową czy myśliwską. Ograniczenia takie nie odniosą także skutku, jeżeli sprawcą przestępstwa terrorystycznego jest osoba posiadająca broń służbową – np. żołnierz, który uległ radykalizacji. Niemniej jednak zdarzeń kryminalnych (i terrorystycznych) z użyciem broni palnej jest w Europie zdecydowanie mniej niż tam, gdzie dostęp do niej podlega mniejszej reglamentacji (w Stanach Zjednoczonych ofiarami zabójstw z użyciem broni palnej pada 3,5 osoby na 100 tys. mieszkańców[22], podczas gdy średnia europejska wynosi 0,24[23]). Nie należy jednak wyciągać zbyt daleko idących wniosków z tego rodzaju statystyk – broń palna staje się popularnym narzędziem także w rękach europejskich terrorystów (można przykładowo przywołać atak w Kopenhadze na początku 2015 r.[24]). Pod wieloma względami broń ta doskonale nadaje się do przeprowadzania ataków przez pojedynczych, samotnie działających terrorystów: jest względnie śmiercionośna, jej zarówno legalne, jak i nielegalne zdobycie nie jest trudne (nawet w Europie[25]), jest lekka, łatwa do ukrycia i nietrudna w podstawowej obsłudze. Ograniczenia w dostępie do broni palnej wydają się zarazem konieczne pomimo ich niepełnej

[20] Jako przykład można przywołać atak przeprowadzony przez żołnierza w amerykańskiej jednostce wojskowej w Fort Hood w 2009 r. Szczegółowe informacje na temat tego zdarzenia znajdują się w raporcie specjalnym Senatu Stanów Zdjednoczonych, zob.: J.I. Lieberman, S.M. Collins, *A ticking time bomb: counterterrorism lessons from the U.S. Government's failure to prevent the Fort Hood attack*, US Senate Committee on Homeland Security and Governmental Affairs, Washington D.C. 2011, online: http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2, dostęp 10.09.2015.

[21] Tak jak w przypadku ataku przeprowadzonego przez Andersa Breivika, który posłużył się zarówno bronią palną, jak i materiałami wybuchowymi. Zob.: E. Mala, J. Goodman, *At least 80 dead in Norway Shooting*, „New York Times" z 22 lipca 2011 r., online: http://www.nytimes.com/2011/07/23/world/europe/23oslo.html, dostęp 12.05.2017.

[22] Centers for Disease Control and Prevention, *Fast Stats – Mortality, firearm homicides*, online: http://www.cdc.gov/nchs/fastats/homicide.htm, dostęp 15.09.2015.

[23] N. Duquet, M. Alstein, *Firearms and Violent Deaths in Europe*, Flemish Peace Institute 2015, online: http://www.vlaamsvredesinstituut.eu/sites/vlaamsvredesinstituut.eu/files/files/reports/firearms_and_violent_deaths_in_europe_web.pdf, dostęp 15.09.2015, s. 1.

[24] L. Smith-Spark, N. Roberts, *Who was Copenhagen Guzman Omar Abdel Hamid El-Hussein?*, CNN, 27 lutego 2015 r., online: http://edition.cnn.com/2015/02/17/europe/denmark-copenhagen-gunman/, dostęp 16.09. 2015.

[25] G. Witte, K. Adam, *Getting a gun legaly in Europe may be hard, but terrorists have little trouble*, „The Washinton Post", 19 lutego 2015 r., online: https://www.washingtonpost.com/world/europe/getting-a-gun-legally-in-europe-may-be-hard-but-terrorists-have-little-trouble/2015/02/19/9eb6bce2-b78b-11e4-bc30-a4e75503948a_story.html, dostęp 16.09. 2015.

skuteczności. Warto także zauważyć, że w praktyce samotnie działający terrorysta rzeczywiście nie ma dostępu do bardziej zaawansowanych jednostek broni, amunicji czy innego sprzętu bojowego.

Poważne zagrożenie stanowi też wykorzystanie przez terrorystów materiałów wybuchowych. Konwencjonalne ładunki znajdują się w zainteresowaniu terrorystów niemalże „tradycyjnie" – ich duża siła rażenia (zarówno fizycznego, jak i psychologicznego) doskonale odpowiada realizacji ich celów. Kwestie związane z obrotem materiałami wybuchowymi do zastosowań cywilnych zostały uregulowane na gruncie prawa europejskiego[26] i krajowego[27], a uzyskanie koncesji na handel nimi uzależnione jest od spełnienia szeregu kryteriów, w tym przejścia badań psychologicznych. Podobne przepisy funkcjonują także w innych krajach Europy[28]. Nie jest to jednak regulacja szczelna – nadzór nad produkcją, sprzedażą, transportem i wykorzystaniem materiałów wybuchowych nie zawsze jest prawidłowo wykonywany, co zostało stwierdzone w wynikach niezależnych kontroli[29]. Materiały wybuchowe znajdujące się w rękach terrorystów mogą więc pochodzić zarówno z kradzieży legalnie wprowadzonych do obrotu materiałów, jak i z powojennych niewybuchów czy z nielegalnej produkcji[30]. Istnieją zresztą kategorie materiałów pirotechnicznych, takich jak te przeznaczone do celów widowiskowych (tzw. fajerwerki), które nie podlegają ścisłemu nadzorowi. Jednocześnie jednak możliwość nielegalnego uzyskania profesjonalnie przygotowanych, zwłaszcza wojskowych materiałów wybuchowych mają raczej zorganizowane grupy terrorystyczne niż samotnie działający radykałowie (warto jednak odnotować, że chociażby w lipcu 2015 r. z bazy wojskowej w południowej Francji skradziono zapas materiałów wybuchowych, detonatorów i granatów bojowych[31] – nie sposób przewidzieć, przez kogo i do jakich celów zostaną one wykorzystane).

---

[26] M.in. zob. Dyrektywa Rady 93/15/EWG z dnia 5 kwietnia 1993 r. w sprawie harmonizacji przepisów dotyczących wprowadzania do obrotu i kontroli materiałów wybuchowych przeznaczonych do użytku cywilnego.

[27] DzU 2001, Nr 67, poz. 679.

[28] Np. w Anglii na podstawie *The Control of Explosives Precursors Regulations* 2014 (2014 No. 1942).

[29] Najwyższa Izba Kontroli – Delegatura w Katowicach, *Zapewnienie bezpieczeństwa obywateli w związku z wytwarzaniem, transportem, przechowywaniem i stosowaniem materiałów wybuchowych do użytku cywilnego*, Informacja o wynikach kontroli LKA-4101-010/2014 nr ewid. 40/2015/P/14/073/LKA.

[30] Najwyższa Izba Kontroli, *NIK o materiałach wybuchowych*, online: https://www.nik.gov.pl/aktualnosci/nik-o-materialach-wybuchowych.html, dostęp 16.09.2015.

[31] France24france, *Explosives stolen from French military base*, online: http://www.france24.com/en/20150707-explosives-stolen-france-military-base-terrorism-miramas, dostęp 20.05.2017.

W praktyce znacznie poważniejszym zagrożeniem są będące w zasięgu samotnych sprawców materiały wybuchowe domowej roboty. Kwestia umiejętności niezbędnych do ich skonstruowania zostanie jeszcze rozwinięta w dalszej części niniejszej publikacji. Już w tym punkcie należy jednak wskazać, że amatorskie ładunki wybuchowe można przygotować z wykorzystaniem materiałów ogólnodostępnych, takich jak nawozy azotowe, które po odpowiednim przetworzeniu doskonale nadają się do tego celu. Właśnie tego typu materiał wykorzystał w swoim zamachu Anders Breivik (który sześć ton nawozu nabył w Polsce)[32], a planował jego wykorzystanie (pod okiem funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego) Brunon Kwiecień[33]. Istotą improwizowanych urządzeń wybuchowych (ang. *Improvised Explosive Devices*, IED) jest ich nieskomplikowana konstrukcja i łatwość, z jaką można pozyskać ich komponenty. Co do zasady urządzenia takie składają się z materiału wybuchowego (profesjonalnego lub „domowej roboty"), obudowy oraz elementów dodatkowych, często mających na celu wzmożenie siły działania (np. benzyna, gwoździe, szkło)[34]. W charakterze obudowy często wykorzystywane są garnki ciśnieniowe[35] – bombami skostruowanymi w ten sposób skutecznie posłużyli się sprawcy ataku przeprowadzonego podczas maratonu bostońskiego w 2013 r.[36] Podobnie jednak jak w przypadku noży i pojazdów – nie jest ani możliwe, ani społecznie pożądane wprowadzenie pełnej reglamentacji przedmiotów codziennego użytku, które niestety mogą posłużyć zbudowaniu IED.

Warto jednak zauważyć, że ładunki budowane z codziennych przedmiotów samodzielnie przez terrorystów są często zawodne – przykładowo w 2010 r. nie powiódł się z tego powodu potencjalnie bardzo groźny zamach przy Times Square w Nowym Jorku (sprawca, Faisal Shamazad, usiłował zdetonować samochód-pułapkę w centrum Manhattanu. Bomby przez niego przygotowane były w zasadzie sprawne, jednak mimo to nie wybuchły)[37] czy w Sztokholmie, także w 2010 r. (sprawca zamachu zginął od wybuchu, jednakże większość ła-

[32] Reuters, *Polish farm sold fertilizer to Norway Bomber*, online: http://uk.reuters.com/article/2011/07/25/us-norway-poland-agency-idUKTRE76O28E20110725, dostęp 20.05.2017.

[33] B. West, *Mimicking Breivik in Poland*, Stratfor Global Intelligence, 29 listopada 2012 r., online: https://www.stratfor.com/weekly/mimicking-breivik-poland, dostęp 20.05.2017.

[34] Department of Homeland Secirity, National Academies, *IED attacks – improvised explosive devices*, News & Terrorism – a fact sheet from the National Academies and the Department of Homeland Security, online: http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, dostęp 20.05.2017.

[35] Zob. US Department of Homeland Security, *Potential terrorist use of pressure cookers*, online: http://www.5nr.org/downloads/notice/PotentialTerrorist.pdf, dostęp 20.05.2017.

[36] CNN, *What we know about the Boston bombing and its aftermath*, online: http://edition.cnn.com/2013/04/18/us/boston-marathon-things-we-know/, dostęp 20.05.2017.

[37] BBC News, *Car bomb found in New York's Times Square*, online: http://news.bbc.co.uk/2/hi/americas/8656651.stm, dostęp 20.05.2017.

dunków przygotowanych przez niego nie zadziałała, co uczyniło go jedyną ofiarą całego zdarzenia)[38].

Istnieją jeszcze jednak bardziej niebezpieczne narzędzia i materiały, które należy zabezpieczyć przed dostępem niepowołanych do tego osób. Choć może wydawać się to problemem mało realnym, zdecydowanie warto rozważyć także możliwości dostępu terrorystów do broni masowego rażenia – zarówno biologicznej, chemicznej, jak i nuklearnej lub radiologicznej. Wbrew pozorom, pomimo teoretycznie ścisłej kontroli państw nad środkami tego rodzaju, nie można wykluczyć ich zastosowania przez terrorystów w niedalekiej przyszłości.

Wykorzystanie czynników biologicznych w atakach terrorystycznych było dotychczas rzadkością, choć zdarzyły się takie przypadki. Dwa ataki odnotowano w Stanach Zjednoczonych – do pierwszego z nich doszło w 1984 r. w stanie Oregon, gdzie zorganizowana grupa fanatyków religijnych doprowadziła przypadkową grupę osób do zakażenia salmonellą w celu zmniejszenia frekwencji w lokalnych wyborach (i w konsekwencji wpłynięcia na ich wynik). Drugi zdarzył się wkrótce po zamachach z 11 września 2001 r., kiedy w wyniku zakażenia rozsyłanymi pocztą bakteriami wąglika zmarło 5 osób[39]. Warto zdać sobie sprawę, że samo pozyskanie biologicznego czynnika chorobotwórczego nie jest szczególnie skomplikowane. Większość czynników chorobotwórczych (z wyjątkiem wirusa czarnej ospy, przechowywanego obecnie jedynie w dwóch laboratoriach na świecie) występuje bowiem w naturze: u zainfekowanych zwierząt, ludzi czy nawet w glebie. W żaden sposób nie da się więc ograniczyć dostępu do nich. Zdobyte w ten sposób czynniki biologiczne będą charakteryzowały się jednak niewielką przydatnością bojową – wyhodowanie wysoce agresywnego szczepu bakterii czy wirusa chorobotwórczego nadającego się do zastosowania w broni masowego rażenia jest już znacznie trudniejsze[40]. Wobec tego większość terrorystów będzie raczej poszukiwać gotowych czynników – mogą starać się wykraść je z magazynów laboratoriów biologicznych lub zamówić, wykorzystując legalne sposoby[41]. Wydawałoby się więc, że przeprowadzenie ataku bioterrorystycznego jest poza zasięgiem sa-

[38] M.E. Hanson, C. Håkansson, *Man sprängde sig själv i Stockholm*, „Svenska Dagbladet", 11 grudnia 2010 r., http://www.svd.se/man-sprangde-sig-sjalv-i-stockholm_5802915, dostęp 20.05.2017.

[39] J.B. Tuckes, *Biosecurity: limiting terrorist access to deadly pathogenes*, US Institute of Peace 2003, s. 11.

[40] Należy jednak zauważyć, że raz zdobyte nawet w małej ilości czynniki chorobotwórcze można swobodnie namnażać, chociaż wymaga to dodatkowego zaplecza technicznego i przeszkolenia. Zob. US General Accounting Office, *Combating terrorism – need for comprehensive threat and risk assessments of chemical and biological attacks*, GAO Report to Congressional Requests 1999, s. 14.

[41] J.B. Tuckes, op. cit., s. 15.

motnie działającego sprawcy. Próba zarażenia wielu osób którąś z najgroźniejszych chorób (takich jak czarna ospa) wymagałaby bowiem przygotowań i organizacji „bardziej przypominających działania wojenne niż terrorystyczne”[42].

Nie oznacza to jednak, że nie jest to możliwe na mniejszą skalę, zwłaszcza gdy potencjalny terrorysta posiada odpowiednią wiedzę. Dobrym przykładem takiego sprawcy może być sympatyzujący z ruchami neonazistowskimi Larry W. Harris, który w 1995 r., podając się za kierownika laboratorium mikrobiologicznego (w rzeczywistości pracował przy uzdatnianiu wody pitnej na terenie stanu Ohio), zamówił „do badań” bakterie dżumy, którymi najprawdopodobniej planował zakazić wodę[43]. Jego zamówienie zostało skutecznie złożone i zapewne zostałoby zrealizowane. Harris wzbudził jednak podejrzenia, gdy wielokrotnie telefonował do siedziby dostawcy, aby dopytywać o czas i przebieg realizacji[44].

Atrakcyjna dla terrorystów może być także broń chemiczna, która w porównaniu z bronią biologiczną jest znacznie prostsza w obsłudze. Jej elementy są łatwiejsze w przenoszeniu i transporcie niż w przypadku broni biologicznej, a ich działanie – znacznie szybsze[45]. Aby wywołać duże szkody, konieczna jest jednak duża ilość szkodliwej substancji, a jej skutki mogą zostać zniwelowane chociażby przez nieodpowiednie warunki atmosferyczne. Mimo to wykorzystanie środków chemicznych może być atrakcyjnym dla terrorystów sposobem przeprowadzenia ataku – czego przykładem są wydarzenia z Tokio z 1995 r.[46] Oczywiście, broń chemiczna nie jest obecnie wytwarzana, przechowywana ani wykorzystywana w państwach demokratycznych. Środki takie w dużej ilości mogą jednak pochodzić z arsenałów upadłych państw północnej Afryki[47] czy

[42] B. Kellman, *Biological terrorism: legal measures for preventing catastrophe*, „Harvard Journal of Law and Public Policy” 2001–2001, nr 24/417, s. 438.

[43] *Police arrests white supremacist who ordered plague bacteria*, „Daily News” z 17 maja 1995 r., s. A10.

[44] J.E. Stern, *Larry Wayne Harris*, w: J.B. Tucker, *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, MIT Press 2000, s. 227–46.

[45] Zob. D.A. Shea, *Chemical weapons: a summary report of characteristics and effects*, Congressional Research Service 2013.

[46] Zob.: K. Kay, *Nerve gas attack shocks Tokyo*, BBC News Archive, online: http://www.bbc.com/news/av/world-asia-18455007/archive-gas-attack-shocks-tokyo, dostęp: 12.05.2017.

[47] Wiadomo na przykład, że bronią chemiczną dysponował Mu’ammar Al-Kaddafi, który użył jej m.in. w wojnie przeciw Czadowi w 1987 roku. Po układach rozbrojeniowych Trypolis zamknął badania nad bronią chemiczną i rozpoczęto proces jej neutralizacji, przerwany jednak w związku ze zbrojnym powstaniem przeciwko rządom Kaddafiego (do tego momentu zniszczono ok. 55% gazu musztardowego i 40% prekursorów broni chemicznej). Obecnie, ze względu na sytuację w regionie, należy poważnie brać pod uwagę zagrożenia związane z utratą kontroli nad tymi materiałami. Zob. M.R. Gordon, *U.S. thinks Libya may plan to make chemical weapons*, „New York Times”, 24 grudnia 1987 r., online: http://www.nytimes.

z terenów Syrii i północnego Iraku[48]. Wykorzystanie tego akurat arsenału przez pojedynczych sprawców lub niewielkie ich grupy na terenie Europy wydaje się jednak mało prawdopodobne. Zarazem mogą mieć oni łatwy dostęp do bardzo wielu innych szkodliwych substancji chemicznych, które, tak jak np. chlor, są na masową skalę wykorzystywane przemysłowo, a mogą zostać użyte do ataku. Problem ten jest zresztą stopniowo dostrzegany zarówno w Europie[49], jak i w Stanach Zjednoczonych[50].

Skutki ewentualnego terrorystycznego wykorzystania broni nuklearnej czy chociażby groźnych środków radioaktywnych są trudne do wyobrażenia. Szkody wyrządzone w ten sposób byłyby równie duże co psychologiczny efekt takiego typu ataku. Chociaż wykluczony jest dostęp terrorysty do gotowych, wojskowych głowic nuklearnych, to możliwa jest samodzielna budowa pełnosprawnego ładunku jądrowego. Sama konstrukcja tego rodzaju urządzenia wybuchowego nie jest wbrew pozorom trudna, jednak wymaga dostępu do wysoko wzbogaconego uranu (*highly enriched uranium*, HEU) lub do plutonu. Są to oczywiście materiały pilnie strzeżone. Należy jednak podkreślić, że do skonstruowania groźnego ładunku nuklearnego wystarczy już jedynie około 50 kg HEU, które ze względu na gęstość tego pierwiastka zajęłyby objętość zaledwie około 2 litrów[51]. Jeżeli materiał jest naprawdę wysoko wzbogacony (90%), to do osiągnięcia masy krytycznej wystarczy ok. 18 kg, a nawet jeszcze mniej – choć wówczas bomba staje się jednak coraz bardziej skomplikowana w budowie[52]. Groźny w rękach terrorystów może być także pluton o cywilnym zastosowaniu (niezużyte paliwo jądrowe)[53], aczkolwiek jego wykorzystanie w budowie bomby jest już znacznie trudniejsze. Wszelkie materiały radioaktywne nadają się jednak doskonale do konstrukcji tzw. brudnej bomby radiologicznej – w której materiał radioaktywny jest jedynie rozrzucany siłą eksplozji konwencjonalnego ładunku wybuchowego. Z drugiej strony należy zauważyć, że

com/1987/12/24/world/us-thinks-libya-may-plan-to-make-chemical-weapons.html, dostęp 20.05. 2017.

48 A. Tilghman, *US confirms Islamic State use of chemical weapons*, „Military Times", online: http://www.militarytimes.com/story/military/2015/08/21/isis-used-mustard-gas-makhmour-against--kurds/32116637/, dostęp 16.09.2015.

49 C. Turner, *Fears over jihadi chemical attack on British soil*, „The Telegraph", online: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11627958/Fears-over-jihadi-chemical-attack-on-British-soil.html, dostęp 20.05.2017.

50 B. Brodsky, *Industrial chemicals as weapons: chlorine*, The Nuclear Threat Initiative, online: http://www.nti.org/analysis/articles/industrial-chemicals-weapons-chlorine/ dostęp 17.09. 2015.

51 A. Newman, M. Bunn, *Securing global nuclear stockpiles: the first line of defense in preventing nuclear terrorism*, „Fletcher Forum of World Affairs" 2009, t. 33/109, s. 109.

52 B. Kellman, D.S. Gualtieri, *Barricading the nuclear window – a legal regime to curtail nuclear smuggling*, „University of Illinois Law Review" 1996, nr 3, s. 684.

53 D. Hughes, *When terrorists go nuclear*, „Popular Mechanics", styczeń 1996, s. 56.

już zużyte paliwo jądrowe, wbrew powszechnej opinii, nie stanowi dużego zagrożenia, a środki bezpieczeństwa stosowane w elektrowniach atomowych, jak również przy jego transporcie i przechowywaniu, są w praktyce wystarczające do zagwarantowania ochrony (w ramach przeprowadzonego w 1988 r. eksperymentu z testową betonową ścianą imitującą otoczenie reaktora nuklearnego zderzono niewielki samolot, uzyskując jedynie kilkucentymetrową penetrację)[54].

Dotychczas nie zdarzyło się, aby środki tego typu zostały wykorzystane przez samotnego terrorystę (nie użyły ich także grupy terrorystyczne, chociaż to zagrożenie jest poważnie brane pod uwagę[55]). Dostęp do materiałów radioaktywnych jest silnie ograniczony, a kwestia ich faktycznego bezpieczeństwa pozostaje do rozważenia na gruncie ochrony informacji niejawnych (np. o tym, gdzie są przechowywane i w jaki sposób są chronione) oraz faktycznej ochrony fizycznej w miejscach ich przechowywania. Jednostka odpowiednio zdeterminowana, posiadająca odpowiednią wiedzę i kontakty, byłaby prawdopodobnie w stanie uzyskać pewną ilość substancji radioaktywnych na czarnym rynku. W Polsce w 2010 r. zostało zresztą zatrzymanych kilka osób oferujących zakup antymonianu rtęci (substancji samej w sobie silnie trującej, która po napromieniowaniu może służyć do wytworzenia tzw. czerwonej rtęci – potencjalnego składnika brudnej bomby atomowej)[56]. Nie wiadomo, jak wiele materiałów tego typu rzeczywiście jest obecnie dostępnych w nielegalnym obrocie. Zwłaszcza po upadku Związku Radzieckiego, w latach 90., materiały rozszczepialne nadające się do konstrukcji broni atomowej znajdowano regularnie w posiadaniu przemytników i handlarzy bronią. Przykładowo czeska policja skonfiskowała w tym czasie 3 kg HEU, ukraińska – 6 kg, a władze litewskie – ponad 99 kg[57].

Nie ulega wątpliwości, że nieskrępowany i nieewidencjonowany obrót materiałami umożliwiającymi skonstruowanie groźnej broni masowego rażenia w zasadzie nie jest możliwy. Jednakże w pewnych okolicznościach nawet samotnie działający terrorysta może starać się zdobyć takie substancje z legalne-

[54] D.M. Chapin, K.P. Cohen, W.K. Davis, E.E. Kintner, L.J. Koch, J.W. Landis, M. Levinson, I.H. Mandil, Z.T. Pete, T. Rockwell, A. Schriesheim, J.W. Simpson, A. Squire, C. Starr, H.E. Stone, J.J. Taylor, N.E. Todreas, B. Wolfe, E.L. Zebroski, *Nuclear power plants and their fuel as terrorist target*, „Science" 2002, t. 297, nr 5589, s. 1997–1999.

[55] D. Watson, *Preventing nuclear terrorism*, „Notre Dame Journal of Legal Ethics and Public Policy" 2005, t. 19/333, s. 333–337.

[56] A. Jasińska, *Łódź: sąd za handel materiałem do wyrobu bomby atomowej*, „Dziennik Łódzki" z 7 kwietnia 2010 r., online: http://www.dzienniklodzki.pl/artykul/241455,lodz-sad-za-handel-materialem-do-wyrobu-bomby-atomowej,id,t.html?cookie=1, dostęp 20.05.2017.

[57] B.L. Rothberg, *Averting armegeddon: preventing nuclear terrorism in the United States*, „Duke Journal of Comparative and International Law" 1997–1998, t. 8/79, s. 105.

go źródła lub na czarnym rynku, i może mu się to udać. Ochrona przed uzyskaniem takich materiałów przez osoby nieuprawnione realizowana jest przede wszystkim w drodze ścisłego ewidencjonowania zasobów, ochrony informacji o nich, a także przez fizyczną ochronę miejsc ich przechowywania i transportu – a więc przez stosowanie dodatkowych ograniczeń wymienionych jako kategorie (b) oraz (c) według zaproponowanej we wstępie klasyfikacji.

Ograniczenie dostępu terrorystów do środków i narzędzi służących do przeprowadzania ataku jest zadaniem niezwykle trudnym, niemożliwym do zrealizowania w pełni. Stosowane ograniczenia w pewnym stopniu zabezpieczają społeczeństwo przed najgroźniejszymi z ataków lub przynajmniej odwlekają je w czasie (koniecznym do ich przygotowania), dzięki czemu planujące je osoby mogą zostać wykryte z wykorzystaniem innych metod. Samo ograniczenie dostępności fizycznych narzędzi ataku wywołuje też dodatkowe utrudnienie w postaci konieczności uzyskania przez potencjalnego sprawcę informacji o tym, w jaki sposób może on dane środki zdobyć z pominięciem tych przeszkód – a więc przesuwa problem do wyróżnionej wcześniej kategorii (b) ograniczeń. Zarazem materiały, do których dostęp jest zastrzeżony, są przechowywane w określony sposób, co powoduje konieczność przełamania lub ominięcia istniejących zabezpieczeń fizycznych – przenosząc problem do wyróżnionej wcześniej kategorii (c). W wielu przypadkach kategorie te przenikają się wzajemnie.

Ograniczenie dostępu do wiedzy, umiejętności i informacji

Wiedzę i umiejętności pozwalające na zdobycie odpowiednich do przeprowadzenia ataku środków także należy potraktować jako swoiste „narzędzia" intelektualne mogące służyć dokonaniu ataku terrorystycznego. Dotyczy to zarówno umiejętności w zakresie konstruowania ładunków wybuchowych i obsługi broni oraz informacji o możliwych źródłach ich pozyskania, jak i informacji na temat potencjalnych celów ataków terrorystycznych[58]. Próby ograniczenia dostępu do wiedzy tego typu stanowią kolejny poziom omawianej pasywnej strategii ograniczania możliwości działań terrorystycznych.

Już na wstępie warto dostrzec poważny problem, jaki mogą stanowić specjaliści różnych dziedzin, którzy z rozmaitych powodów zwracają się niekiedy ku aktywności terrorystycznej i stanowią zawsze cenny nabytek dla organizacji terrorystycznej. Udział takich osób w planowaniu i przeprowadzaniu zamachu zwiększa szanse jego skuteczności, minimalizując równocześnie ryzyko poniesienia kosztów ewentualnej porażki (także kosztów ekonomicznych, co

[58] B.D. Barnes, op. cit., s. 1639.

w przypadku organizacji terrorystycznych ma niebagatelne znaczenie)[59]. Problem dotyczy w równym stopniu samotnie działających terrorystów będących specjalistami w swoich dziedzinach[60]. Osoby takie często zdobywają odpowiednie wykształcenie na długo przed rozpoczęciem choćby wstępnego planowania ataku, trudno więc temu zapobiec. Znane są jednak przypadki, gdy terroryści zdobywali odpowiednie umiejętności wyłącznie w celu przeprowadzenia ataku, tak jak np. sprawcy zamachów z 11 września 2001 r., którzy wcześniej przechodzili szkolenia w zakresie pilotażu samolotów pasażerskich. Niestety, nie istnieje w pełni skuteczna metoda uniemożliwienia potencjalnym terrorystom przejścia specjalistycznych szkoleń. Przeprowadzane w ramach dostępu do niektórych zawodów testy psychologiczne czy wywiady środowiskowe mogą pozwolić na wykluczenie części osób potencjalnie niebezpiecznych, jednakże nie wszystkich – Malik Hasan, będący przecież wojskowym psychiatrą, przechodził wiele tego rodzaju testów, zanim dopuścił się ataku w Fort Hood[61].

Aby zdobyć wiedzę na temat potencjalnych sposobów przeprowadzenia ataku, nie trzeba jednak przechodzić specjalistycznych szkoleń. Wskazanie w tym zakresie na Internet jako „wirtualny obóz treningowy"[62] dla terrorystów staje się stopniowo truizmem. Informacje „niebezpieczne" nie są wcale szczególnie ukryte w sieci, zwłaszcza że duże organizacje terrorystyczne dążą do upowszechnienia takiej wiedzy i przeprowadzania dzięki temu ataków rękami niepowiązanych z nimi ochotników. Publikowane są więc materiały propagandowe zachęcające do radykalnych działań, a także pisane prostym językiem broszury zawierające szczegółowe scenariusze przeprowadzenia ataku. Znanym przykładem jest wydawany przez Al-Kaidę magazyn internetowy *Inspire*, przekazujący wiedzę na temat np. budowy bomby „w kuchni swojej mamy" czy przerobienia samochodu tak, aby lepiej nadawał się do wykorzystania jako narzędzie ataku[63]. Informacje są przekazywane przez „doświadczonych" terrorystów niczym nieograniczonej rzeszy chcących się z nimi zapoznać odbiorców. Istnieje zarazem wiele podstawowych narzędzi ułatwiających poszukiwa-

[59] A.B. Krueger, *What Makes a Terrorist – Economics and the Roots of Terrorism*, Princeton University Press, Princeton, NJ 2007, s. 46.

[60] W ramach przypadków wspomnianych we wcześniejszej części niniejszego rozdziału warto wspomnieć chociażby o Larrym W. Harrisie (mikrobiologu usiłującym przeprowadzić atak bioterrorystyczny), Brunonie Kwietniu (ekspercie akademickim w zakresie materiałów wybuchowych, konstruującym ładunki pod okiem służb specjalnych) czy o sprawcy zamachu w Fort Hood (będącym przeszkolonym żołnierzem).

[61] J.W. Jones, J.R. Haygood, *The Terrorist Effect: Weapons of Mass Disruption, the Danger of Nuclear Terrorism*, iUniverse Publishing, Bloomington, IN 2011, s. 124.

[62] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, online: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, dostęp 20.05.2017.

[63] Ibidem.

nie i gromadzenie informacji: wyszukiwarki, czaty, fora[64]. Nawet zaś gdyby zdobycie i przeanalizowanie koniecznych informacji okazało się dla konkretnej osoby zbyt trudne, może ona z łatwością skorzystać z pomocy kogoś takiego jak Younis Tsouli – aresztowany w 2005 r. mężczyzna prowadzący liczne dżihadystyczne strony internetowe i zdalnie wspierający potencjalnych zamachowców informacjami i wskazówkami[65].

Zamieszczone umyślnie w Internecie informacje, porady oraz instrukcje pozyskiwania i wykorzystywania niebezpiecznych środków są tylko częścią problemu upowszechnienia wiedzy specjalnej. Wiele informacji tzw. podwójnego zastosowania jest zamieszczanych w domenie publicznej w zupełnie otwarty sposób, choć ich autorzy nie mają zamiaru udzielenia wsparcia terrorystom. Umożliwia to świadome lub intuicyjne wykorzystanie przez terrorystę technik OSINT (*Open Source Intelligence*[66]) do ich gromadzenia. Oczywiście, także i w tym kontekście podstawowym źródłem wiedzy jest Internet. Przykładem może być „popularnonaukowy" wpis na stronie internetowej producenta chemikaliów, dotyczący prostych i skutecznych domowych sposobów produkcji chloru, wręcz zachęcający do samodzielnych eksperymentów z jego produkcją[67].

Samotni terroryści wykorzystują Internet także do zbierania danych na temat potencjalnych celów ataków. Zgromadzenie informacji o celu jest bardzo istotnym elementem planowania zamachu: istotne mogą być dane o układzie pomieszczeń, budynków, rozkładach jazdy komunikacji zbiorowej, godzinach otwarcia różnych instytucji i organizacji i tak dalej. Wszystko to może być przydatne terroryście planującemu zamach i można to odnaleźć w Internecie. W niezwykle czytelny sposób ukazuje to „ekoterrorystyczna" akcja okupowania komina elektrowni gazowej w Wielkiej Brytanii – na opublikowanym przez grupę nagraniu widać dokładnie, w jaki sposób jej członkowie planowali swoją akcję i się do niej przygotowywali i w jaki sposób pomogły im w tym materiały udostępnione w formie filmu wyprodukowanego bezpośrednio przez dział marketingu właściciela elektrowni[68].

---

64 G. Weimann, *Terror on the Internet – the New Arena, the New Challenges*, United States Institute of Peace Press, Washington DC 2006, s. 111–112.

65 G. Corera, *The world's most wanted cyber-jihadist*, BBC News, 16 stycznia 2008 r., online: http://news.bbc.co.uk/2/hi/7191248.stm, dostęp 20.05.2017.

66 Czyli pozyskiwania wiedzy, która jest „dostępna dla każdego, na podstawie obserwacji własnych lub próśb o udzielenie informacji", NATO Open Source Intelligence Reader, luty 2002 r., s. 9.

67 Zob.: EuroChlor, *How is chlorine produced*, online: http://www.eurochlor.org/the-chlorine-universe/how-is-chlorine-produced.aspx, dostęp 20.05.2017.

68 Zob.: *Reclaim Power: The Story of the No Dash for Gas 21*, online: https://www.youtube.com/watch?v=HovQqw9jEJY, dostęp 20.05.2017.

Nie istnieje skuteczny sposób wyeliminowania dostępu osób poszukujących takiej wiedzy do tego rodzaju materiałów znajdujących się już w otwartych źródłach. Warto też pamiętać, że wiele informacji przydatnych terrorystom jest niezbędnych społeczeństwu w codziennym funkcjonowaniu (np. rozkład jazdy metra), co czyni ich ukrywanie absurdalnym. Konsekwentnie usuwając zaś z różnych miejsc w sieci np. wydania *Inspire*, można ewentualnie ograniczyć prawdopodobieństwo natknięcia się na taki materiał przez przypadkowe osoby, jednak usunięcie jakiejkolwiek „niebezpiecznej" informacji z Internetu powoduje zazwyczaj jej pojawienie się w innym miejscu, ewentualnie pod inną nazwą – utrudniając co prawda dostęp do niej ekstremistom, ale i obserwującym takie materiały funkcjonariuszom właściwych służb. Warto też podkreślić, że poszukiwanie i zbieranie informacji najczęściej nie jest *per se* nielegalne, aczkolwiek w niektórych krajach podejmuje się próby ścigania osób posiadających materiały pochodzące z *Inspire*[69]. Takie działanie może jednak wzbudzać kontrowersje związane z tworzeniem przestępstwa „bycia zradykalizowanym", w którym zacierają się granice między przygotowaniem, usiłowaniem i dokonaniem czynu zabronionego. Dalece słuszne wydaje się jednak stosowanie metod pracy operacyjnej wobec osób poszukujących takiego rodzaju informacji w Internecie – o ile uda się to wykryć w odpowiednim czasie.

Choć usunięcie informacji znajdujących się już w obiegu otwartym skazane jest na porażkę, to wciąż istnieją takie, nad którymi kontrolę sprawuje ograniczony krąg podmiotów, a więc skuteczne ograniczenie dostępu do nich jest możliwe. Dotyczy to zarówno informacji objętych ochroną na zasadzie tajemnicy państwowej różnych poziomów, jak i informacji pochodzących od podmiotów prywatnych (np. o organizacji i procedurach bezpieczeństwa w dużym centrum handlowym). W związku z obowiązywaniem w tym zakresie określonych przepisów[70] informacje krytyczne dla bezpieczeństwa państwa nie mają prawa znaleźć się w rękach terrorystów – co do zasady jest to skuteczny sposób ich ochrony przed większością zamachowców, zwłaszcza samotnie działających. Zapewnieniu bezpieczeństwa informacji w tym zakresie służą konkretne narzędzia techniczne i procedury, obejmujące także kwestie zapisywania i ka-

[69] Jest to możliwe m.in. na podstawie przepisów obowiązujących w Wielkiej Brytanii (Section 58 of the Terrorism Act 2000), gdzie pod takimi zarzutami skazano już co najmniej kilka osób. Zob.: *Woman jailed after al-Quaida terrorist material found on her phone*, „The Guardian", 6 grudnia 2012 r., online: http://www.theguardian.com/world/2012/dec/06/woman-jailed-al-qaida-material-on-phone, dostęp 20.05.2017.

[70] W Polsce zwłaszcza na podstawie Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (DzU Nr 182, poz. 1228) oraz prawa międzynarodowego i ustaleń pomiędzy sojusznikami w ramach różnych organizacji (m.in. NATO – zob. m.in. umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji sporządzona w Brukseli dnia 6 marca 1997 r.).

sowania tajnych danych z nośników elektronicznych i magnetycznych czy wykorzystania kryptografii w zagwarantowaniu bezpieczeństwa państwa[71]. Można więc powiedzieć, że ścisła kontrola tajemnic i informacji o krytycznym znaczeniu wytycza granicę skuteczności ograniczeń należących do określonej we wstępie kategorii (b) – inne przydatne w przeprowadzeniu ataku informacje można z łatwością uzyskać ze źródeł otwartych.

Fizyczna ochrona potencjalnych celów ataku

Gdy sprawca posiądzie niezbędną wiedzę oraz fizyczne narzędzia umożliwiające mu przeprowadzenie ataku terrorystycznego, ostatnią linię obrony przed nim stanowią zwykle sama atakowana infrastruktura i zastosowane w niej środki ochrony. Nawet gdy celem ataku są konkretni ludzie (np. głowa państwa), ewentualny zamach zostanie dokonany w określonym otoczeniu, zorganizowanym i zabezpieczonym (lub nie) w określony sposób. Fizyczna ochrona celów ataku także zmierza więc do ograniczenia możliwości przeprowadzenia ataku terrorystycznego.

Ochronie przed skutkami ataku mogą w szczególności służyć konkretne rozwiązania konstrukcyjne w budynkach i urządzeniach użyteczności publicznej, mające minimalizować ewentualnie wyrządzone szkody. Dobrym przykładem tego rodzaju działań mogą być metalowe słupki ochronne wbudowywane w ziemię wokół przystanków autobusowych w Jerozolimie. Ich montaż był bezpośrednią odpowiedzią na częste ataki z wykorzystaniem pojazdów po prostu wjeżdżających w zgromadzonych na przystanku pasażerów[72].

Pozbawieniu możliwości przeprowadzenia zamierzonego ataku służyć mają też stałe lub doraźne kontrole bezpieczeństwa, np. osób wchodzących na teren danego obiektu. Najbardziej oczywistym przykładem stosunkowo ścisłej kontroli tego typu może być ta prowadzona na lotniskach. Odbywa się ona zresztą w sposób ustalony międzynarodowymi standardami[73]. Oprócz lotnisk

---

[71] Niektóre tego rodzaju instrukcje bezpieczeństwa są po kilku latach ujawniane. Zob. m.in.: U.S. Department of Defence, *Unclassified computer hard drive disposition*, 2001, online: http://iase.disa.mil/policy-guidance/asd_hd_disposition_memo060401.pdf, dostęp 26.09.2015; Government of Canada, Communications Security Establishment, *Clearing and declassifying electronic data storage devices (ITSG-06)*, 2006, online: http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-eng.html, dostęp 26.09.2015; National Security Agency/Central Security Service, *NSA/CSS Storage device declassification manual*, 2007, online: http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf, dostęp: 20.05.2017.

[72] Zob.: *PM orders barriers at bus stops cross Jerusalem after attack*, „Times of Israel" z 14 grudnia 2015 r., online: http://www.timesofisrael.com/pm-orders-barriers-at-bus-stops-across-jerusalem-after-car-ramming/, dostęp 12.05.2017.

[73] Zob. m.in.: Airports Council International Europe, *Security at airports*, w: ACI, *Policy and Recommended Practices Handbook*, 7th ed., 2009.

kontrole bezpieczeństwa stosowane są domyślnie także w innych miejscach narażonych na atak, takich jak budynki sądów czy urzędów publicznych. Oprócz tego kontrole prowadzone są niekiedy w środkach komunikacji zbiorowej (np. w metrze w Delhi w Indiach)[74], w niektórych muzeach[75], w centrach handlowych, na parkingach, uczelniach wyższych i w wielu innych miejscach publicznie dostępnych (zwłaszcza w rejonach bardziej narażonych na ataki – np. w Izraelu)[76]. Niemożliwe jest sporządzenie kompletnej listy miejsc, w których przeprowadzane są kontrole bezpieczeństwa tego rodzaju.

Pomimo powszechności stosowania i stosunkowo dużego stopnia uciążliwości skuteczność kontroli bezpieczeństwa jest dyskusyjna. Po pierwsze, problemem może być rutynowość procedur i efektywność stosowanych w trakcie kontroli urządzeń. Stosunkowo niedawno wyszło na jaw, że tzw. nagie skanery wykorzystywane na niektórych lotniskach (głównie w Stanach Zjednoczonych) praktycznie wcale nie spełniają swojej funkcji[77]. Jednocześnie wiele substancji niebezpiecznych nie jest wychwytywanych przez osoby prowadzące kontrolę, gdy te nie były wcześniej przeszkolone do ich poszukiwania – przykładowo w toku działań śledczych po ataku na samolot pasażerski Pan Am (lot nr 103) w grudniu 1988 r. okazało się m.in., że wykorzystany w zamachu plastyczny materiał wybuchowy był substancją nieznaną funkcjonariuszom prowadzącym wówczas kontrolę i że nie byli oni szkoleni w zakresie jego wykrywania[78]. Po drugie, kontrole bezpieczeństwa można niekiedy ominąć administracyjnie – dysponując odpowiednimi uprawnieniami. Przykładowo w celu ominięcia kontroli bezpieczeństwa prowadzonych w polskich sądach (z zasady dotyczy to wszystkich sądów w Polsce) wystarczy zgłosić się na bezpłatne i zasadniczo łatwo dostępne praktyki sądowe[79]. Po trzecie, wszelka kontrola bezpieczeństwa

---

74 M.S. Singh, *Moscow blasts put Metro security in alert mode*, „The Times of India", 30 marca 2010 r., online: http://timesofindia.indiatimes.com/city/delhi/Moscow-blasts-put-Metro-security-in-alert-mode/articleshow/5740559.cms?referral=PM, dostęp 20.05.2017.

75 Smithsonian Institution, *Security and Policies*, online: http://www.si.edu/Visit/Security, dostęp 20.05.2017.

76 K.M. Bondevik, J. Gahr Støre, E. Solheim, *Voices of Tomorrow. Reflections of Students and Professionals on Peacebuilding*, Tapir Academic Press, Trondheim 2009, s. 105.

77 J. Scholtes, *Price for TSA's failed body scanners: $160 million*, Politico, 17 sierpnia 2015 r., online: http://www.politico.com/story/2015/08/airport-security-price-for-tsa-failed-body-scanners-160-million-121385 dostęp 20.05.2017.

78 Ten i szereg innych problemów w zakresie bezpieczeństwa organizacji lotów w owym czasie ujawniono m.in. w materiałach telewizyjnych w 1990 r., zob.: *Lockerbie bombing*, ABC Prime Time Live z 20 grudnia 1990 r., online: https://www.youtube.com/watch?v=h3NoNH-DPBM, dostęp 12.05.2017.

79 Na podstawie obowiązujących regulaminów pracownicy sądów, a także np. adwokaci, mogą wchodzić do budynku bez kontroli bezpieczeństwa za okazaniem legitymacji, zob. m.in. Zarządzenie Prezesa Sądu Apelacyjnego w Szczecinie z dnia 21 grudnia 2012 r. (nr A.021-

będzie w oczywisty sposób nieskuteczna, gdy środki konieczne do przeprowadzenia zamachu można zdobyć już na terenie danego obiektu – naturalnie, zdobycie ładunku wybuchowego na lotnisku czy w budynku sądu nie będzie możliwe bez wcześniejszych przygotowań, jednakże pozyskanie ostrego noża nie stanowi już problemu (przykładowo na lotnisku w Zurychu w strefie bezcłowej sprzedawane są scyzoryki[80]). Poleganie na tego rodzaju kontroli w zapobieganiu atakom terrorystycznym daje więc jedynie iluzję bezpieczeństwa. Często nowe procedury wdrażane są reaktywnie, dopiero po zdarzeniu, w związku z odkrytą w ten sposób luką bezpieczeństwa (np. zakazy dotyczące przewożenia w kabinie samolotu płynów w określonej objętości wprowadzone w reakcji na wykryte przez Brytyjczyków plany wykorzystania w zamachu płynnych środków wybuchowych[81] czy kontrole obuwia na lotniskach związane z nieudaną próbą zamachu dokonaną przez Richarda Reida w 2001 r.[82]).

Podsumowanie

Wszystkie trzy omówione kategorie działań antyterrorystycznych o charakterze pasywnym mają za zadanie zapobiegać zdarzeniom tego rodzaju lub minimalizować ich skutki przez wykluczenie możliwości przeprowadzenia ataku – pozbawiając sprawcę dostępu do narzędzi, wiedzy oraz celów. Ograniczenia te w żadnej mierze nie stanowią jednak barier nie do pokonania dla odpowiednio zmotywowanego sprawcy, nawet działającego w pojedynkę.

Opisywane strategie szerokiego ograniczania dostępu są jednak stopniowalne – zarówno pod względem zakresu samych ograniczeń, jak i ich skuteczności. W przypadku prób uniemożliwienia terrorystom wejścia w posiadanie niebezpiecznych narzędzi stosunkowo skuteczne ograniczenia wprowadzono w odniesieniu do najbardziej niebezpiecznych i zaawansowanych rodzajów broni „wysokiej technologii". Zarazem jednak już choćby ograniczenie dostępu potencjalnych sprawców do broni palnej, pomimo licznych obowiązujących w tym zakresie regulacji, jest jedynie częściowo skuteczne. Prawdopodobnie nigdy zaś nie będzie możliwe pozbawienie terrorystów szans skorzystania z najbardziej podstawowych narzędzi ataku, w tym w szczególności ostrych

266/12) w sprawie wprowadzenia regulaminu bezpieczeństwa i porządku w Sądzie Apelacyjnym w Szczecinie.

80 S. Murphy, *Airport security farce: deadlier knives than used on 9/11 sold in duty free – and taken on London flight*, DailyMail Online, 17 sierpnia 2013 r., online: http://www.dailymail.co.uk/news/article-2396327/Airport-security-farce-Deadlier-knives-used-9-11-sold-duty-free-taken-London-flight.html, dostęp 20.05.2017.

81 D. Sasciani, *Liquid bomb plot: what happened*, BBC News, 7 września 2009 r., online: http://news.bbc.co.uk/2/hi/uk_news/8242479.stm, dostęp 20.05.2017.

82 Zob.: *Shoe bomb suspect to remain in custody*, CNN News z 25 grudnia 2001 r., online: http://edition.cnn.com/2001/US/12/24/investigation.plane/, dostęp 12.05.2017.

przedmiotów i pojazdów, a także komponentów służących do budowy domowych ładunków wybuchowych. Ograniczenia w dużej mierze mają charakter prawno-administracyjny (np. w zakresie dostępu do broni palnej czy w obrocie materiałami wybuchowymi), a więc zazwyczaj są możliwe do ominięcia legalnymi metodami. Istnieje także wiele kategorii niebezpiecznych materiałów praktycznie w ogóle wyłączonych spod ograniczeń administracyjnych – np. użytkowanie wspomnianych wcześniej „widowiskowych" środków pirotechnicznych, noży „do użytku domowego" czy pojazdów. Wreszcie samotny terrorysta pracujący w odpowiednim zawodzie (np. jako żołnierz czy laborant) będzie miał dostęp do narzędzi i materiałów niebezpiecznych niedostępnych dla osób cywilnych. Podobnie należy ocenić możliwość zablokowania dostępu do wiedzy umożliwiającej przeprowadzenie ataku. Odpowiednie instrukcje i porady są już dostępne w źródłach otwartych i nie jest możliwe ich skuteczne „wycofanie" z obiegu w państwie demokratycznym. Możliwa i celowa jest natomiast ochrona informacji o krytycznym znaczeniu dla bezpieczeństwa. Fizyczna ochrona potencjalnych celów ataków również nie jest pozbawiona wad ze względu m.in. na wysokie koszty oraz iluzoryczną skuteczność niektórych rozwiązań przyjmowanych obecnie jako standard postępowania. Podobnie jednak jak w przypadku ograniczeń kategorii (a) oraz (b), także i fizyczna ochrona celów ataku powinna być utrzymywana tam, gdzie to racjonalnie możliwe.

Wspomniana stopniowalność rozwiązań działa jednak dwukierunkowo: terroryści pozbawieni możliwości działania w preferowany przez siebie sposób będą działać inaczej, z wykorzystaniem metod mniej zaawansowanych, lecz bardziej dostępnych. Jednym z podstawowych czynników wpływających negatywnie na skuteczność omawianych ograniczeń jest problem substytucji środków i celów ataku. Jeżeli dostęp do środka „pierwszego wyboru" (np. powodującej więcej szkód broni) jest zbyt trudny, istnieje bardzo duże prawdopodobieństwo, że zdeterminowany sprawca sięgnie po inny, mniej śmiercionośny, lecz łatwiej dla niego dostępny[83]. Parafrazując wypowiedź Osamy Bin Ladena z 1996 r.[84], można więc powiedzieć, że obowiązująca obecnie wśród terrorystów zasada to: skoro nie możesz użyć buldożera, użyj topora (albo: skoro nie masz bomby, użyj pistoletu, a w jego braku – noża lub samochodu).

[83] Por. W. Enders, *What do we know about the substitution effect in transnational terrorism?*, University of Alabama 2002, online: http://www.utdallas.edu/~tsandler/website/substitution 2ms.pdf, dostęp 20.05.2017.

[84] Cyt. oryg.: „Czemu używać topora, gdy można użyć buldożera?" – ta krytyczna wypowiedź Osamy Bin Ladena stanowić miała jego komentarz do przedstawionych mu planów wyczarterowania małej awionetki, wypełnienia jej materiałami wybuchowymi i dokonania w ten sposób zamachu na siedzibę CIA. Zob. G. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Times Books/Henry Holt, New York 2004, s. 19.

Jeszcze większą rolę problem substytucji odgrywa przy doborze celu ataku. Cele terrorysty nie są bowiem (zwykle) dobierane losowo. Chcąc wyznaczyć odpowiedni obiekt ataku mającego wywołać oczekiwaną przez terrorystę reakcję, sprawca przy założeniu, że podejmuje jakikolwiek wysiłek intelektualny, aby dokonać racjonalnego wyboru w tym zakresie, zawsze weźmie pod uwagę to, jakie środki ochrony są w nim utrzymywane. Odpowiednio do tego wybierze zarówno cel, jak i środki dające mu największą szansę powodzenia[85]. Dodatkowa ochrona nie spowoduje więc, że ataki ustaną, lecz sprawi, że będą przeprowadzone w innym miejscu; nie powstrzyma wszystkich ataków, ale jedynie niektóre ich formy[86]. Tragicznym tego przykładem mogą być wydarzenia z marca 2016 r., kiedy do zamachu bombowego na lotnisku w Brukseli doszło *przed* bramkami kontroli bezpieczeństwa, na hali odlotów[87]. Aby zagwarantować pełne bezpieczeństwo przed atakami terrorystycznymi dzięki fizycznej ochronie potencjalnych celów, należałoby więc zabezpieczyć przed nimi całą przestrzeń publiczną. Z praktycznego punktu widzenia nie jest jednak możliwe zagwarantowanie fizycznej ochrony każdego sklepu, przystanku autobusowego czy publicznie dostępnego budynku – kluczowy zatem staje się wybór, w ramach strategii antyterrorystycznej, które obiekty uznaje się za na tyle zagrożone i istotne, że celowa jest ich szczególna ochrona. Warto w tym kontekście przywołać jedną z fundamentalnych zasad taktyki obronnej: chcąc bronić wszystkiego, nie broni się niczego. Fizyczna ochrona celów ataku, choć może być skuteczna, musi być więc realizowana z uwzględnieniem racjonalnie dostępnych na ten cel zasobów. Można także rozważyć zasadność spostrzeżenia, że wydając coraz więcej środków i poświęcając coraz więcej uwagi publicznej walce z terroryzmem, w pewien sposób pozwalamy mu zatriumfować.

Na koniec warto zwrócić uwagę, że praktycznie wszystkie omawiane ograniczenia mają szansę realnie podnieść ogólny poziom bezpieczeństwa jedynie wtedy, gdy towarzyszy im poczucie społecznej odpowiedzialności ze strony osób sprawujących kontrolę: czy to pracujących przy legalnej produkcji i dystrybucji niebezpiecznych materiałów i narzędzi, obsłudze wrażliwych informacji, czy fizycznej ochronie obiektów. To właśnie wyczulenie na nietypowe sytuacje i czujność pracowników American Type Culture Collection pozwoliły na zatrzymanie wspomnianego wcześniej Larry'ego W. Harrisa i unik-

[85] T. Sandler, H.E. Lapan, *The calculus of dissent: an analysis of terrorists' choice of target*, „Synthese" 1988, t. 76 (2), s. 245–261.

[86] B.D. Barnes, op. cit., s. 1641.

[87] Zob.: *Brussels explosions: what we know about airport and metro attacks*, BBC News z 9 kwietnia 2016 r., http://www.bbc.com/news/world-europe-35869985, dostęp 12.05.2017 r.

nięcie groźnego w skutkach ataku bioterrorystycznego. Inny samotny terrorysta, Naser Abdo, przygotowywał w 2011 r. atak na Fort Hood (ten sam, na który zamachu dokonał w 2009 r. Nidal Malik Hasan). Został on zatrzymany po tym, jak sprzedawca w lokalnym sklepie z bronią poinformował policję o jego zakupach, które w odczuciu sprzedawcy były „dziwne" (zatrzymany w pobliskim motelu Abdo posiadał przy sobie pistolet, dużą ilość czarnego prochu, metalowych odłamków, garnki ciśnieniowe i wydrukowany z Internetu artykuł na temat domowego przygotowywania bomb)[88]. Kontrola społeczna zawsze jest istotnym elementem prewencji zdarzeń kryminalnych, a w kontekście zagrożeń terrorystycznych wydaje się szczególnie ważna. Tymczasem jeden z funkcjonariuszy organów ścigania[89] wskazał na następującą sytuację, której był bezpośrednim świadkiem: ekspedientka w sklepie z artykułami militarnymi powiedziała mu, że „poprzedniego dnia przyszło dwóch chłopaków i kupili kilkanaście maczet", lecz nikomu tego nie zgłosiła. Chociaż przytoczona sytuacja ma głównie wartość anegdotyczną, wyraźnie ilustruje, jak wiele należy poprawić w zakresie społecznej kontroli zagrożeń bezpieczeństwa w Polsce.

Wszystko to nie oznacza, że trzeba rezygnować ze stosowania pasywnych środków ograniczających możliwości sprawców – musimy jednak traktować je wyłącznie jako element wieloskładnikowej strategii bezpieczeństwa, uzupełniając ich niedostatki innymi metodami neutralizowania zagrożeń.

Streszczenie

Skuteczne zwalczanie zagrożeń terrorystycznych wymaga spójnego, wielopoziomowego podejścia zarówno ze strony podmiotów państwowych, jak i prywatnych. Szereg metod stosowanych w walce z atakami terrorystycznymi to aktywne metody pracy operacyjnej i procesowej mające na celu wczesne wykrycie i pociągnięcie do odpowiedzialności sprawcy, zanim nastąpi atak. Równie istotne są pasywne metody pozwalające uniemożliwić przeprowadzenie zamachu dzięki ograniczeniom w dostępie do szeroko rozumianych środków ataku, które zmierzają do zminimalizowania ryzyka i skutków ataków terrorystycznych. Ich rzeczywista skuteczność powinna jednak być oceniana w świetle możliwości przeprowadzenia ataku pomimo tworzonej dzięki ograniczeniom dostępu do środków niebezpiecznych swoistej iluzji bezpieczeństwa.

Słowa kluczowe: terroryzm, ograniczenia dostępu, dostęp do środków ataku, dostęp do celów ataku

[88] K. Coffey, *The lone wolf – solo terrorism and the challenge of preventive prosecution*, „FIU Law Review" 2011, t. 7 (1), s. 12.

[89] Informacja przekazana w toku wywiadu badawczego w ramach projektu FP7 PRIME.

Summary

Effective counterterrorism requires a coherent and multi-level approach from both private and public entities. There is a number of active procedural and operational methods in force, timing to early detect and neutralize terrorist threats. Simultaneously passive methods of attack prevention are also used, aiming to deny future perpetrators the means of attack. Their actual effectiveness should, however, be assessed taking into account the possibility of carrying out an attack despite the illusion of safety created by the restrictions in force.

Keywords: terrorism, access restrictions, means of attack, attack objectives