Założenia teorii CPTED w uodpornieniu infrastruktury krytycznej portu lotniczego

Assumptions of CPTED theory immunization in the critical infrastructure of the airport

Agata Tyburska

Mł. insp. dr hab.

Wyższa Szkoła Policji w Szczytnie,
Wydział Bezpieczeństwa
Wewnętrznego

a.tyburska@wspol.edu.pl

Streszczenie: Akty terrorystyczne są typowymi zagrożeniami, które prowokują sytuacje kryzysowe o znacznych rozmiarach nie tylko w skali kraju, ale również państw czy regionów. Szczególne zainteresowanie terrorystów zawsze wzbudzać będą elementy infrastruktury państwa, które określane są jako kluczowe dla codziennego funkcjonowania ludzi i administracji publicznej. Porty lotnicze obsługujące ludzi oraz zapewniające szybki przewóz towarów są w szczególnym zainteresowaniu współczesnych terrorystów. Ataki terrorystyczne skierowane na elementy infrastruktury portu lotniczego spowodować mogą zarówno ich zniszczenie, uszkodzenia, jak również zainicjować awarie skutkujące nie tylko olbrzymimi stratami materialnymi, ale co istotne, śmiercią oraz uszkodzeniem ciała znacznej liczby osób. W konsekwencji wywołać mogą poczucie braku bezpieczeństwa, panikę oraz rezygnację z korzystania z usług gwarantowanych przez przewoźników i porty lotnicze. Opracowanie realnych, a zarazem skutecznych planów ochrony, opartych na wynikach badań i analiz naukowych oraz dobrych praktykach – pozwala na skuteczną ochronę kluczowego obszaru portu lotniczego, a w sytuacji kryzysowej - na zminimalizowanie kosztów będących następstwem przeprowadzonego ataku. Koncepcja Crime Prevention Trough Environmental Design (CPTED) zapobiegania przestępczości przez kształtowanie przestrzeni koncentruje się na przestrzeni fizycznej jako istotnym czynniku wpływającym na zachowania przestępcze. Przestrzeń ta w różny sposób powiązana jest z aktem przestępczym. Teoria kształtowania bezpiecznych przestrzeni zakłada, że przestępcy w sposób racjonalny dokonują wyboru celu, a ich decyzje poparte są analizą warunków istniejących w danej przestrzeni (szacowanie ryzyka). Ich wybór dotyczy zarówno miejsc, które preferują jako miejsca popełnienia przestępstw, jak również obszarów, których unikają. Celem artykułu jest przedstawienie elementów koncepcji CPTED, które zostały zaadoptowane w ochronie infrastruktury portów lotniczych.

Słowa kluczowe: *Terroryzm; Bezpieczne przestrzenie; Uodpornienie; Infrastruktura krytyczna*

Abstract: Terrorist acts are typical threats that provoke a crisis of considerable size not only in the country but also in the countries or regions. Terrorist interest will always be aroused by elements of state infrastructure, which are defined as essential for the daily functioning of people and public administration. Airports serving people and providing fast transport of goods are of particular interest to modern terrorists. Terrorist attacks targeting the airport infrastructure can cause both their destruction and damage, as well as initiate breakdowns that result in not only huge material losses, but significant deaths and damage to a substantial number of people. As a consequence, they may cause insecurity, panic and abandon the use of services guaranteed by carriers and airports. Developing real and effective protection plans, based on the results of research and analysis and good practice - allows for effective protection of a key airport area and, in a crisis situation, to minimize costs resulting from an attack. The Crime Prevention Trough Environmental Design (CPTED) concept of prevention of crime by shaping space focuses on physical space as an important factor influencing criminal behavior. This space is connected in various ways with the criminal act. The theory of shaping safe spaces assumes that criminals make a rational choice of purpose, and their decisions are supported by an analysis of the conditions existing in a given space (risk analysis). Their choice applies to both the places they prefer as the crime scene and the areas they avoid. The aim of the article is to present elements of the CPTED concept, which may be adopted in the protection of airport infrastructure

Keywords: *Terrorism; Safe areas; Immunization; Critical infrastructure*

Charakter zagrożeń początku XXI wieku uświadomił teoretykom i praktykom z zakresu bezpieczeństwa narodowego (bezpieczeństwa państwa), nie tylko konieczność zweryfikowania wiedzy dotyczącej identyfikacji i oceny zagrożeń, ale również potrzebę zmodyfikowania dotychczasowych koncepcji ochrony infrastruktur kluczowych państwa. Aktywność terrorystów skupiona głównie (obok systemów działających w cyberprzestrzeni), na miejscach gromadzenia się znacznej liczby ludzi oraz obiektach, instalacjach i urządzeniach mających znaczenie dla sprawnego funkcjonowania państwa, a w konsekwencji jego znaczącej pozycji na arenie międzynarodowej - wyznacza coraz to nowe kierunki działań skierowanych na zwiększenie odporności celów potencjalnego ataku. Takim celem coraz częściej padają elementy infrastruktury transportowej państwa, a w konsekwencji osoby korzystające z tej formy podróżowania. Porty lotnicze i morskie, statki powietrzne i morskie, dworce kolejowe, pociągi, stacje metra – to tylko przykłady elementów infrastruktury będącej w zainteresowaniu współczesnych zamachowców. Szczególny charakter zagrożeń dotyczący portów lotniczych wymaga od zarządzających bezpieczeństwem obiektu zintensyfikowania działań ochronnych, a co za tym idzie korzystania z coraz to nowszych technologii oraz zweryfikowania wdrożonych wcześniej rozwiązań.

Koncepcja zapobiegania przestępczości poprzez projektowanie środowiska (crime prevention through envi-

ronmental design – CPTED) proponuje proste, a zarazem skuteczne rozwiązania zwiększające obronny charakter przestrzeni, co również znajduje swoje odzwierciedlenie w rozwiązaniach służących bezpieczeństwu osób i infrastruktury portu lotniczego.

Zagrożenia terrorystyczne infrastruktury krytycznej

Infrastruktura krytyczna charakteryzuje się niezwykle złożonymi, heterogenicznymi oraz niezależnymi zespołami (kompleksami) obiektów, systemów i funkcji, które są podatne na różnorodne zagrożenia. Sama liczba elementów krytycznych, wszechobecność i wzajemne powiązania skupiają zainteresowania hakerów czy terrorystów jako potencjalnego celu ataku, którego efekty będą na tyle skuteczne, że mogą zmusić administrację rządową do zmiany w prowadzonej polityce wewnętrznej czy zagranicznej.

Skutki zamachów terrorystycznych przeprowadzonych na początku XXI wieku zwróciły uwagę zarówno teoretyków, jak i praktyków związanych z obszarem bezpieczeństwa, na potrzebę zwiększenia odporności infrastruktury, która jest kluczowa dla funkcjonowania państwa i jego obywateli. Badacze problemu zwracają jednocześnie uwagę na trudności związane z prawidłowym wyznaczaniem tego typu infrastruktury oraz niezwykle złożony i dynamiczny charakter współczesnych infrastruktur.

Obecnie większość badaczy problemu postrzega infrastrukturę krytyczną jako majątek, usługi i systemy, które wspierają życie gospodarcze, polityczne i społeczne kraju, a których znaczenie jest na tyle istotne, że ich całkowite lub częściowe zniszczenie lub uszkodzenie mogłoby wywołać masowe przypadki utraty życia; mieć poważny wpływ na gospodarkę kraju; wywoływać inne poważne konsekwencje społeczne dla życia i zdrowia obywateli czy też wywołać poważny problem dla administracji publicznej [1].

W większości państw stosowane jest systemowe podejście do wyodrębnia infrastruktury krytycznej państwa. Pośród systemów określanych jako krytyczne duże znaczenie (z punktu widzenia sprawnego funkcjonowania państwa i bezpieczeństwa ludzi), odgrywa system transportu (powietrzny, wodny, drogowy, kolejowy), który jest bezpośrednio powiązany z takimi systemami krytycznymi, jak zaopatrzenia w energię, surowce energetyczne i paliwa, zaopatrzenia w wodę, z systemem ratowniczym czy teleinformatycznym. Powiązania i zależności istniejące pomiędzy elementami infrastruktury krytycznej oraz elementami innych infrastruktur kluczowych są niekiedy tak złożone i skomplikowane, że częstokroć utrudniają ich właściwe diagnozowanie oraz wyznaczanie poziomu krytyczności powstałych węzłów i punktów kluczowych. Te skomplikowane ścieżki powiązań i zależności niejednokrotnie przenoszą się poza granice kraju, łącząc się z elementami infrastruktury innych państw - obciążając w ten sposób elementy kluczowe dodatkową wrażliwością. Ważnym podkreślenia jest również twierdzenie wyprowadzone przez Alvina i Heidi Toffler, iż *„wszystkie części systemu są (…) w stanie stałej fluktuacji. I są nadzwyczaj podatne na wpływy zewnętrzne (…). Mnożą się pętle dodatniego sprzężenia zwrotnego, co znaczy, że pewne procesy, wprowadzone raz w ruch, zaczynają żyć swoim życiem i, dalekie od stabilizacji, wprowadzają jeszcze większą niestabilność w obrębie systemu (…). Zbieżność fluktuacji wewnętrznej i zewnętrznej może doprowadzić do całkowitego załamania systemu albo do jego reorganizacji na wyższym poziomie"* [13]. Współcześni badacze podkreślają, iż z uwagi na rozmiary i zasięg potencjalnego celu, nie można zakładać możliwości stuprocentowej ochrony wszystkich elementów infrastruktury krytycznej przed możliwymi zagrożeniami [11].

Po zamachu z 11 września 2001 r. administracje rządowe państw wysokorozwiniętych uznały ataki terrorystyczne jako szczególny rodzaj zagrożeń bezpieczeństwa państwa. Obecnie terroryzm niezwykle silnie oddziałuje nie tylko na poczucie i faktyczny stan bezpieczeństwa pojedynczych osób, ale również wpływa na politykę rządów, przedsiębiorców oraz (pośrednio) na przemysł. Ataki terrorystyczne odnotowane na przełomie XX i XXI wieku skutkowały zniszczeniem bądź uszkodzeniem budynków administracji publicznej, obiektów handlowych, infrastruktury metra czy lotniska, zniszczeniem samolotów, a w konsekwencji utratą życia i zdrowia wielu ludzi. Wywołały też poważne zakłócenia w funkcjonowaniu administracji, rurociągów i ropociągów czy portów w lotniczych.

Jak wskazują analizy – największe zagrożenia dla bezpieczeństwa narodowego stanowią sytuacje niebezpieczne, wywołane cyberterroryzmem. Wynika to chociażby z powszechnego dostępu do Internetu i możliwości przeprowadzenia ataku bez ponoszenia strat własnych. Jak podkreśla Krzysztof Liedel dokonanie ataku w Sieci nie wymaga od sprawcy specjalnie wyrafinowanych umiejętności przy znacznym procencie zachowania anonimowości [6]. Stwierdzenie to koresponduje z opinią sformułowaną przez Piotra Sienkiewicza, którego zdaniem cyberterroryzm stanie się coraz powszechniejszym zjawiskiem ze względu na niskie koszty ponoszone przez terrorystów na przygotowanie i przeprowadzenie ataku w Sieci, postępujący proces globalizacji, wykorzystywanie efektu zaskoczenia, całkowitą anonimowość związaną z niewielkim ryzykiem wykrycia [10].

Rozwój nowych technologii informacyjnych oraz związane z nim cyberzagrożenia – ze względu na specyfikę i sposób funkcjonowania elementów wrażliwych – szczególnie silnie oddziałują na infrastrukturę krytyczną. Coraz większe prawdopodobieństwo przeprowadzenia ataku w cyberprzestrzeni, rozmiary i skutki tego typu ataków, wynikają z powiązań (sieciowości) pomiędzy elementami kluczowymi oraz wykształcenie się społeczeństwa informacyjnego. Zagrożenia w cyberprzestrzeni najczęściej kojarzone są z wykorzystaniem sieci komputerowych jako narzędzia do sparaliżowania lub istotnego ograniczenia możliwości wykorzystania struktur narodowych (np. transport, energetyka, instytucje rządowe) lub też do zastraszenia lub wymuszenia na rządzie lub społeczeństwie określonych działań (bądź ich zaniechania) [3]. Są częstokroć efektem nieuprawnionego działania w systemach komputerowych i sieciach teleinformatycznych zarówno ze strony osób nieuprawnionych, jak i ich użytkowników. Z sieci informatycznych korzysta obecnie większość podmiotów zaliczanych do infrastruktury krytycznej w tym systemów kontroli ruchu lotniczego, czy obsługi klientów korzystających z tego rodzaju transportu. Zdaniem Haliny Świebody, zagrożenia

cyberatakiem na elementy infrastruktury kluczowej mogą „przyczynić się do wzmocnienia efektu ataku klasycznego przez wywołanie dodatkowego zamieszania i paniki ludności (…), co w wyniku kaskadowego rozprzestrzeniania się uszkodzeń w systemach elektronicznych może stanowić zagrożenie dla gospodarki i bezpieczeństwa publicznego"[12]. Stąd też wśród sytuacji najczęściej wymienianych jako zagrażających bezpieczeństwu systemów działających w cyberprzestrzeni są działania mające charakter sabotażu komputerowego (rozpowszechnianie wirusów i robaków, blokowanie systemów), czy też zamachy na infrastrukturę krytyczną polegające na ingerowanie w jej funkcjonowanie. Stąd też współcześni terroryści coraz częściej korzystają ze środków niemilitarnych (cywilnych), łatwiej dostępnych, a jednocześnie pozwalających na spektakularne osiągnięcie zakładanego celu. Wartym podkreślenia jest bowiem fakt, że terroryści doskonale szacują ryzyko podczas typowania celów potencjalnego ataku. Nie jest trudno przewidzieć, że gromadzą wszelkie informacje na temat odporności elementów infrastruktury krytycznej państw będących w ich zainteresowaniu. Po rozpoznaniu zastosowanych zabezpieczeń (systemu ochrony) obiektu, instalacji czy urządzenia - w przypadku stwierdzenia wysokiego poziomu jego odporności - niewątpliwie zmieniają obiekt zainteresowań, aby skupić niszczycielską siłę na celach, które uważają za słabiej chronione, co sprzyja szybkiemu osiągnięciu przez zamachowców zamierzonego efektu. Dotychczasowe doświadczenia wskazują na zmiany w prowadzonej taktyce: terroryści coraz częściej przeprowadzają ataki na kilka elementów infrastruktury państwa jednocześnie (bądź ataków występujących po sobie w krótkim okresie czasu – tzw. „efekt kuli śnieżnej") tak aby utrudnić prowadzenie akcji ratowniczych, skomplikować prowadzenie pościgów (ustalanie sprawców), a w konsekwencji zwiększyć liczbę ofiar i społeczny oddźwięk zamachów. Liczba, cel oraz zasięg przeprowadzanych współcześnie ataków coraz częściej skłaniają do podjęcia aktywności w celu zwiększenia odporności infrastruktury krytycznej.

Port lotniczy z uwagi na swój charakter wynikający z:

a) dostępności zarówno dla użytkowników zewnętrznych, jak również wewnętrznych;
b) złożoność infrastruktur (urządzeń, sieci, instalacji);
c) międzynarodowy charakter;
d) dynamiczną rozbudowę rozmiarów i struktury;
e) konieczność prowadzenia współpracy z wieloma podmiotami obsługującymi port lotniczy;
f) liczne powiazania i zależności z innymi kluczowymi elementami infrastruktury krytycznej (infrastrukturami państwa);
g) rozrastającą się konkurencję;
h) znaczną liczbę osób przebywających (skoncentrowanych) na stosunkowo niewielkiej przestrzeni jest szczególnie podatny na przeprowadzenie aktu sabotażu czy ataku terrorystycznego.

Koncepcja CPTED w uodpornieniu infrastruktury kluczowej portów lotniczych

Współczesny charakter zagrożeń uświadomił teoretykom i praktykom zajmującym się bezpieczeństwem narodowym (bezpieczeństwem państwa) nie tylko konieczność zweryfikowania wiedzy dotyczącej infrastruktury i oceny zagrożeń, ale – co istotne – wymusiło potrzebę zmodyfikowania dotychczasowych koncepcji ochrony infrastruktury kluczowej państwa. Współcześnie ochrona infrastruktury krytycznej jest różnie definiowana i interpretowana. W literaturze przedmiotu termin ten odnosi się najczęściej do działań ukierunkowanych na ochronę „wrażliwych" systemów oraz tworzących je struktur i obejmuje: ludzi, majątek trwały oraz te elementy systemów, które są niezbędne dla bezpieczeństwa państwowego, infrastruktury kluczowej miast, stabilności gospodarczej i bezpieczeństwa publicznego [8]. Niektórzy autorzy ochronę infrastruktury krytycznej postrzegają jako określone strategie, decyzje oraz gotowość potrzebną do ochrony, zapobiegania oraz — w razie potrzeby — reagowania na ataki (w tym również terrorystyczne), skierowane na krytyczne sektory, systemy oraz kluczowe dobra i wartości [5].

Stosowane w ramach ochrony metody, środki i procedury kierowane są na zapobieganie lub (i) złagodzenie skutków ataków na infrastrukturę krytyczną wywołanych przez ludzi (terrorystów, hakerów), katastrofy naturalne czy awarie techniczne. Ochronę infrastruktury krytycznej należy zatem traktować jako część ochrony i obrony narodowej obejmującą wszelkiego rodzaju przedsięwzięcia o charakterze zapobiegania, przygotowania, reagowania - mające na celu podniesienie odporności infrastruktury krytycznej na wszelkiego rodzaju zakłócenia ograniczające jej prawidłowe działanie, jak również skierowane na szybkie przywrócenie realizowanych funkcji w przypadku zniszczenia, uszkodzenia lub awarii. Przedsięwzięcia te obejmują zarówno działania legislacyjne, edukacyjne, fizyczne i techniczne, jak również wszelkie rozwiązania systemowe prowadzone na wszystkich poziomach administracji publicznej, a także realizowane przez sektor prywatny, społeczeństwo oraz inne podmioty działające na rzecz bezpieczeństwa narodowego [14]. Infrastruktura krytyczna osadzona jest w określonej przestrzeni. Przestrzeń ta może mieć charakter fizyczny lub symboliczny. Przestrzeń fizyczna definiowana jest jako *„obszar postrzegany całościowo wraz ze znajdującymi się w nim obiektami"* [15]. W określonej przestrzeni fizycznej zlokalizowane są rzeczywiste obszary, budynki, urządzenia, instalacje czy też sieci tworzące infrastrukturę gminy, miasta, powiatu, województwa, które składają się na infrastrukturę państwa. Z kolei przestrzeń symboliczna określana jest jako *„całość zjawisk określonego rodzaju"* [15]. Stąd też przestrzeń symboliczna może być kojarzona m.in. z cyberprzestrzenią, która w konsekwencji daje szerokie możliwości oddziaływania na elementy zlokalizowane w przestrzeni fizycznej. Oddziaływanie to może spowodować zwiększenie odporności konkretnego elementu infrastruktury, bądź zainicjować sytuacje skutkujące jego zniszczeniem, uszkodzeniem bądź awarią. Szeroki dostęp do cyber świata spowodował, że obszar ten zaczęto określać mianem nowej przestrzeni społecznej" [2].

Koncepcja Crime Prevention Trough Environmental Design (CPTED) zapobiegania przestępczości przez kształtowanie przestrzeni koncentruje się na przestrzeni fizycznej jako istotnym czynniku wpływającym na zachowania potencjalnych sprawców przestępstw. Przestrzeń

ta w różny sposób może być powiązana z aktem łamania prawa. Teoria kształtowania bezpiecznych przestrzeni zakłada, że przestępcy w sposób racjonalny dokonują wyboru celu i miejsca ataku, a ich decyzje poparte są analizą warunków istniejących w danej przestrzeni, które sprzyjają (bądź nie) podjęciu decyzji o złamaniu normy prawnej. Wyniki prowadzonych badań wskazują, że zachowania antyspołeczne koncentrują się w określonych miejscach, punktach czy obszarach, które to z kolei – z uwagi na różnego rodzaju czynniki – mogą utrudniać bądź ułatwiać sprawcy dokonanie przestępstwa. Miejsca te generować mogą u potencjalnych sprawców/społeczności subiektywny, a zarazem tak różny poziom poczucia bezpieczeństwa jako satysfakcjonujący bądź znikomy. Stąd też wybory jakich dokonują sprawcy przestępstw dotyczą zarówno obszarów, obiektów, urządzeń, czy instalacji, które preferują jako miejsca dla nich „bezpieczne" do popełnienia przestępstw, jak również miejsc, których z uwagi na duży poziom ryzyka, z reguły unikają traktując je jako miejsca „zagrożone".

Dlatego też filozofia Crime Prevention Trough Environmental Design (CPTED) opiera się na założeniu, co do logicznego i przemyślanego doboru celów przez sprawców przestępstw (zamachów), popartego drobiazgową analizą ryzyka (szacowania zysków i start). Jedno z podstawowych założeń filozofii CPTED odzwierciedla stwierdzenie: „im większe ryzyko bycia zauważonym, wykrytym lub złapanym tym mniejsze prawdopodobieństwo popełnienia przestępstwa; im większy jest wysiłek, który trzeba włożyć w popełnienie przestępstwa, tym mniejsze prawdopodobieństwo jego popełnienia; im mniejszy rzeczywisty lub prawdopodobny zysk z przestępstwa, tym mniejsze prawdopodobieństwo jego popełnienia" [4].

Prowadzone badania pozwoliły na wyodrębnienie obszarów, a w nich konkretnych miejsc określanych jako kryminogenne. Badacze problemu, posługując się określoną metodologią, potrafią z dużą precyzją określić te elementy przestrzeni, które ułatwiają potencjalnemu sprawcy popełnienie czynu zabronionego. Wśród elementów kryminogennych, odnoszących się do konkretnej przestrzeni, najczęściej wymienianie są: duża liczba osób równocześnie korzystających z przestrzeni; wysoki stopień anonimowości; brak dostatecznego nadzoru, utrudniony zakres obserwacji, wiele możliwości (dróg, wyjść, przejść itp.) ucieczki sprawców. Dodatkowo wymieniane są takie czynniki, jak:

a) przejścia, tunele, ścieżki, wyznaczone trasy - łączące dwa lub większą liczbę miejsc, umożliwiające anonimowe przemieszczanie się osób (tzw. generatory ruchu);
b) znaczne rozmiary, gabaryty obiektów charakterystyczne dla miejsc przebywania znacznej liczby osób (porty lotnicze, obiekty handlowe, stadiony, miejsca manifestacji i festynów) (tzw. honey pots);
c) obszary chętnie wybierane przez sprawców na miejsca zamachów (tzw. punkty zapalne);
d) miejsca „zapomniane" o czym świadczy ich zaniedbanie oraz brak podejmowania jakiejkolwiek aktywności (tzw. generatory strachu) [4].

Filozofia działań określanych jako Crime Prevention Trough Environmental Design (CPTED) sięga początku lat 60 ubiegłego wieku. Protoplastami koncepcji byli E. Wood, J Jacobs. Duży wkład w jej rozwój wnieśli również tacy badacze, jak: C. Jeffery; Oscar Newman, czy Timothy D. Crowe. Wskazani badacze przyjęli założenie, że istnieją możliwości (narzędzia) przekształcania środowiska (przestrzeni) w taki sposób aby odstraszała potencjalnych sprawców, a przez to ograniczyć liczbę zdarzeń niezgodnych z prawem. W literaturze przedmiotu CPTED określana jest również jako proces składający się z kilku etapów: projektowania; tworzenia; użytkowania i utrzymania (zarzadzania) przestrzenią. Stąd też obejmuje „strategie, metody, techniki i narzędzia kształtowania przestrzeni fizycznej oraz jej efektywne użytkowanie i zarządzanie zorientowane na zapobieganie i eliminację przestępczości, zachowań antyspołecznych, jak również redukcję poczucia zagrożenia" [7].

Wśród cech konstytutywnych CPTED wskazane są następujące obszary:

1. Kontrola dostępu;
2. Nadzór;
3. Zabezpieczenie techniczne;
4. Stan utrzymania;
5. Wsparcie użytkownika.

W literaturze przedmiotu odnaleźć można również podejście tzw. 3D w kształtowaniu bezpiecznych przestrzeni, które polega głównie na „kształtowaniu przestrzeni fizycznej w kontekście normalnego i oczekiwanego sposobu jej wykorzystywania przez użytkowników. Uwzględnia więź pomiędzy funkcjonalnością, użytkowaniem i zarządzaniem, a zachowaniami ludzkimi (…)., jest prostym sposobem oceny przestrzeni przydatnym użytkownikom w zorientowaniu się, czy przestrzeń jest odpowiednio zaprojektowana i użytkowana" [4].

Podstawowe założenia koncepcji 3D kształtowania bezpiecznych przestrzeni zasadzają się na trzech kluczowych przesłankach:

1) wcześniejszego określenia przeznaczenia konkretnej przestrzeni (już na etapie projektu architektonicznego budynku, placu, instalacji itp.);
2) zdiagnozowania tzw. społecznych, formalnych, kulturowych i fizycznych cech przestrzeni warunkujących występowanie akceptowanych zachowań;
3) projekt konkretnej przestrzeni oraz usytuowanych tam elementów (obiektów, obszarów, urządzeń, instalacji) daje możliwość kontrolowania zachowań osób funkcjonujących (pojawiających się) w danej przestrzeni.

Przygotowując plany ochrony infrastruktury kluczowej należy zdiagnozować następujące elementy: początkowe przeznaczenie przestrzeni (obiektu, obszaru, urządzenia); obecne jej wykorzystywanie i sposoby użytkowania; formy aktywności ludzkiej występujące na danym obszarze (obiekcie, urządzeniu) oraz prognozowane konflikty wynikające z prowadzenia różnych form aktywności na danej przestrzeni. Niezbędnym jest również zbadanie w jakim zakresie aktywność ludzka (wymagająca zwiększonego zakresu ochrony) dociera czy też ogniskuje się w miejscach kluczowych przestrzeni (obiektu, urządzenia, instalacji). Innymi interesującymi elementami warunkującymi bezpieczeństwo obiektów, urządzeń kluczowych jest zbadanie sposobów rozgraniczenia obszarów o różnym poziomie dostępu, zakresu widoczności oraz czytelności stosowanych

znaków i symboli; konfliktów zarysowujących się pomiędzy przeznaczeniem obiektów (obszarów i urządzeń), a sposobem ich użytkowania.

Z punktu widzenia założeń projektowych sporządzonych dla konkretnej przestrzeni (obiektu, urządzenia, sieci), niezbędne jest ustalenie w jakim zakresie opracowany projekt umożliwia zachowanie pierwotnie zaplanowanych funkcji, czy też umożliwia bądź utrudnia aktywność użytkowników wynikającą z przypisanych im uprawnień i – co istotne – w jakim zakresie umożliwia kontrolę zachowań ludzi przebywających w danej przestrzeni.

Porty lotniczego stanowią dobry przykład zastosowania elementów koncepcji Crime Prevention Trough Environmental Design (CPTED) w podniesieniu odporności elementu kluczowego państwa. Współczesne lotniska stanowią złożone i skomplikowane infrastruktury z bogatą siecią powiązań i zależności z innymi elementami infrastruktury państwa. Sprawną obsługę lotniska zapewnia wiele podmiotów (instytucji), co z jednej strony zapewnia wysoki poziom świadczonych usług, z drugiej zaś stawia dodatkowe wyzwania osobom odpowiedzialnym za bezpieczeństwo portu lotniczego.

Zdaniem Adriana K. Siadkowskiego, zapewnienie bezpieczeństwa portu lotniczego dotyczyć będzie głównie *„infrastruktury obsługi pasażerów oraz operacji lotniczych, czyli obiekty, obszary i urządzenia istotne z punktu widzenia bezpieczeństwa lotu oraz ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji"* [9].

W celu zapewnienia bezpieczeństwa pasażerom, obsłudze oraz przeciwdziałania zniszczeniu bądź uszkodzeniu infrastruktury portów lotniczych stosowane różnorodne rozwiązania, w których odnaleźć można główne pryncypia charakteryzujące koncepcję CPTED, są to propozycje rozwiązań w zakresie:

a) ustalania, kontrolowania dostępu do określonych miejsc (stref) portu lotniczego;
b) prowadzenie nadzoru infrastruktury lotniska (obiektów, urządzeń, instalacji);
c) stosowanie rozwiązań określanych jako zabezpieczenie techniczne;
d) troska o odpowiednio wysoki standard stan utrzymania infrastruktury;
e) stosowanie przemyślanych rozwiązań wspierających użytkowników różnych elementów infrastruktury lotniska (pasażerów, obsługę, techników itd.).

Jak łatwo zauważyć dostęp do różnych (wyznaczonych) stref portu lotniczego jest limitowany według przydzielonych upoważnień i podlega drobiazgowej kontroli. Kontrola dostępu do określonych miejsc (stref) portu lotniczego ma na celu uniemożliwienie wejścia na konkretny teren (obiekt) osobom niepowołanym.

W teorii CPTED kontrola dostępu służyć ma *„kanalizowaniu ruchu pieszego i kołowego w celu ograniczenia dostępu do poszczególnych fragmentów terenu osobom, których obecność w tych miejscach jest niepożądania i nieuzasadniona okolicznościami"* [4]. Kontrolowanie dostępu w takim znaczeniu polega na wydzieleniu określonych stref oraz przypisaniu uprawnień poszczególnym ludziom do przebywania w określonych miejscach (obszarach, obiektach itp.). Przyjęte w tym zakresie rozwiązania pozwalają na ograniczenie swobodnego przemieszczania się ludzi po całym obiekcie (obszarze), ograniczają liczbę osób mających dostęp do elementów krytycznych obiektu, umożliwiają identyfikację osób, a w konsekwencji ograniczają możliwość popełnienia przestępstwa. W tym celu stosowane są różnorodne rozwiązania, w tym bariery fizyczne i symboliczne, a także urządzenia techniczne.

W przypadku portów lotniczych stosowany jest podział na strefy ogólnodostępne, strefy operacyjne, strefy zastrzeżone, a w nich na określone części (podstrefy) krytyczne. Adrian K. Siadkowski analizując plany ochrony lotniska wskazuje również na wyodrębniane w niektórych portach lotniczych tzw. strefy wydzielone oraz granice pomiędzy tymi strefami [9]. Strefy ogólnodostępne są w różny sposób oddzielane od stref operacyjnych. Do tego celu wykorzystywane są zarówno siły osobowe (ochrona fizyczna), jak również środki techniczne (w postaci barier, ogrodzeń) i elektroniczne (system monitoringu wizyjnego).

Część krytyczna to zdaniem autora - część strefy zastrzeżonej portu lotniczego, do której zalicza: miejsca dostępne dla odlatujących pasażerów, a także miejsca przewozu, przenoszenia, przechowywania bagażu. Dla zachowania bezpieczeństwa tej części portu lotniczego i przebywających tam osób przeprowadza się szczegółowe kontrole pasażerów oraz rejestrację i kontrolę bagażu.

Z kolei część portu lotniczego wyznaczona na miejsce postoju statków powietrznych przy wprowadzaniu na pokład pasażerów lub umieszczania w nim ładunków i bagaży oznaczona jest jako strefa zastrzeżona. Obowiązujący w portach lotniczych, limitowany system przydzielania dostępu pracownikom do poszczególnych stref wynikający z zakresu obowiązków uniemożliwia swobodne przemieszczanie się po całej infrastrukturze zarówno pasażerom, jak i obsłudze lotniska.

Prowadzenie nadzoru nad infrastrukturą lotniska to element kompleksowego systemu ochrony portu lotniczego. Samo pojęcie nadzór kojarzone jest z uważną obserwacją i kontrolą. W portach lotniczych obowiązuje reguła wyznaczania określonych stref ochrony, określanych mianem: ochrony wewnętrznej, ochrony zewnętrznej oraz ochrony peryferyjnej. W celu zapewnienia bezpieczeństwa chronionej infrastruktury stosuje się różnego rodzaju metody, techniki i narzędzia, a także procedury wypełniane przez pracowników ochrony (wykonywanie patroli, przeprowadzanie kontroli fizycznych itp.), jak również wykorzystujące nowe technologie.

Dla zapewnienia bezpieczeństwa pasażerom oraz infrastrukturze portu lotniczego stosowane są różnego rodzaju rozwiązania określane jako zabezpieczenie techniczne. W teorii CPTED zabezpieczenie techniczne określanie jest jako „zabezpieczenie miejsca lub obiektu, które uniemożliwi lub utrudni popełnienie przestępstwa" [4]. W ramach tego typu środków wymieniane są wszelkiego rodzaju zabezpieczenia fizyczne (ogrodzenia, drzwi, zamki), jak również elektroniczne (alarmy, czujki itp). W przypadku infrastruktury portu lotniczego do zabezpieczeń technicznych zaliczyć można nie tylko różnego rodzaju bariery i przeszkody fizyczne uniemożliwiające swobodne, niekontrolowane przejścia do poszczególnych stref, ale również urządzenia rentgenowskie służące do prześwietlania bagażu i wykrywania przedmiotów niebezpiecznych (zabronionych), urządzenia rentgenowskie i skanery wykorzystywane do

prześwietlania płynów, urządzenia do wykrywania materiałów wybuchowych, bramki magnetyczne lub ręczne detektory do wykrywania metali.

Utrzymanie odpowiednio wysokiego standardu dotyczącego wyglądu (stanu utrzymania) obszaru stanowi kolejne z pryncypiów koncepcji CPTED, które również warunkuje bezpieczeństwo pasażerów i infrastruktury portu lotniczego. Dbałość o odpowiedni wygląd, konserwacja urządzeń i instalacji (przeciwpożarowych, wodno – kanalizacyjnych, wentylacyjnych itp.), szybkie a zarazem sprawne dokonywanie napraw uszkodzonych (niesprawnych) elementów infrastruktury portu, to nie tylko dbałość o komfort pasażerów ale również istotny element prowadzonej polityki bezpieczeństwa.

Bezpośredni związek z utrzymaniem odpowiedniego standardu (wyglądu) portu lotniczego i jego otoczenia zauważalny jest z kolejnym elementem koncepcji CPTED jakim jest stosowanie przemyślanych rozwiązań wspierających użytkowników elementów infrastruktury lotniska. Użytkownikami portu lotniczego są zarówno pasażerowie, jak również obsługa techniczna, pracownicy i funkcjonariusze realizujący zadania na rzecz ochrony, pracownicy administracyjni oraz przedstawiciele podmiotów zewnętrznych). W teorii kształtowania bezpiecznych przestrzeni wsparcie użytkownika *„polega na takim zaprojektowaniu przestrzeni, które uniemożliwia lub utrudnia wykorzystanie tej przestrzeni w sposób niezgodny z przeznaczeniem i wskazuje jednoznacznie, które zachowania są nieprawidłowe. Chodzi o jasne i jednoznaczne wskazanie, w jaki sposób przestrzeń powinna być wykorzystana"* [4]. Specyficzny charakter portów lotniczych wymaga między innymi dokładnego poinstruowania pasażerów jakie zachowania są niedopuszczalne, jakiego rodzaju przedmioty objęte są ścisłym zakazem przewozu, jak zachować się w przypadku pożaru czy innego niebezpiecznego incydentu (np. atak terrorystyczny). Wiele informacji przekazywanych jest pasażerom w formie plakatów, tablic informacyjnych albo po prostu schematów, rysunków i symboli z uwagi na międzynarodowy charakter portów lotniczych i wynikającej z tego faktu bariery językowej.

Wnioski

Akty terrorystyczne są typowymi zagrożeniami, które prowokują sytuacje kryzysowe o znacznych rozmiarach nie tylko w skali kraju, ale również państw czy regionów. Szczególne zainteresowanie terrorystów zawsze wzbudzać będą elementy infrastruktury państwa, które określane są jako kluczowe dla codziennego funkcjonowania ludzi i administracji publicznej. Ataki terrorystyczne skierowane na elementy infrastruktury krytycznej spowodować mogą zarówno ich zniszczenie, uszkodzenia, jak również wywołać awarie skutkujące nie tylko olbrzymimi stratami materialnymi, ale również śmiercią, uszkodzeniem ciała znacznej liczby ludzi lub dewastacją środowiska naturalnego.

Akty terrorystyczne zdeterminowały podejście do bezpieczeństwa w komunikacji lotniczej i przyczyniły się do ulepszania rozwiązań ochronnych, co z pewnością wpływa na odporność infrastruktury portu lotniczego i bezpieczeństwo pasażerów. Pomimo upływu lat koncepcja zapobiegania przestępczości poprzez projektowanie środowiska (crime prevention through environmental design – CPTED), nadal odgrywa kluczową rolę w planowaniu ochrony elementów infrastruktury państwa. Z powodzeniem jest stosowana również w przypadku elementów infrastruktury krytycznej państwa. Zwolennicy teorii kształtowania bezpiecznych przestrzeni wskazują na olbrzymi potencjał oraz nieodkryte dotychczas możliwości zastosowania koncepcji CPTED, o czym świadczą innowacyjne rozwiązania stosowane w uodparnianiu portów lotniczych. ◄

Materiały źródłowe

[1] Atlas I .R, 21st Century Security and CPTED. Designing for Critical Infrastructure Protection and Crime Prevention, CRC Press, London-New York 2008, s. 11.

[2] Bendyk E., Melomolekuły" „Polityka" 2006, nr 2574, s. 78-79.

[3] Gizicki W., Państwo wobec cyberterroryzmu (w:) Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, red. A. Podraza, P. Potakowski, K. Wiak, Wyd. Difin, Warszawa 2013, s.46-47.

[4] Głowacki R., Łojek K., Ostrowska E., Tyburska A., Urban A., CPTED jako strategia zapewnienia bezpieczeństwa społeczności lokalnej, Wyd. WSPol., Szczytno 2010, s. 17; 25;33;35;36.

[5] Lewis T.G., Critical Infrastructure Protection in Homeland Security. Defending a networked nation, Wyd. Wiley-Interscience, New Jersey 2006, s. 4.

[6] Lidel K., Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej (w:) Bezpieczeństwo w XXI wieku. Asymetryczny świat, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Wyd. Difin, Warszawa 2011, s. 446-447.

[7] Łojek K., Metodyka rozwiazywania problemów kryminalnych, WSPol., Szczytno 2008.

[8] Radvanowsky R.,. McDougall A, Critical Infrastructutre. Homelad Security and Emergerncy Preparedness, Wyd. CRC Press, London-New York 2010, s. 4).

[9] Siadkowski A. K., Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela, Wyd. WSPol., Szczytno 2013, s. 201.

[10] Sienkiewicz P., Bezpieczeństwo w globalnym społeczeństwie informacyjnym (w:) Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku, red. J. Gryz, R. Kwećka, Wyd. AON, Warszawa 2007, s. 93-96.

[11] Sullivant J., Strategies for Protecting National Critical Infrastructure Assets. A Focus on problem-Solving, New Jersey 2007, s. 111.

[12] Świeboda H., Prognozowanie zagrożeń dla bezpieczeństwa informacyjnego (w:) Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku, red. J. Gryz, R. Kwećka, Wyd. AON, Warszawa 2007, s. 127.

[13] Toffler A., Toffler H., Wojna i antywojna. Jak przetrwać na progu XXI wieku?,Wyd. Kurpisz, Poznań 2006, s. 239.

[14] Tyburska A., Ochrona infrastruktury krytycznej w Polsce – wyzwania w tworzeniu bezpieczeństwa narodowego, „Zeszyty Naukowe AON". Dodatek, Warszawa 2013, 98-99.

[15] Wielki Słownik Języka Polskiego, www.wsjp.pl, 10.10.2017r.