dr inż. Marian Żuber
Wyższa Szkoła Oficerska Wojsk Lądowych im. generała T. Kościuszki
we Wrocławiu
Wydział Nauk o Bezpieczeństwie
marian.zuber@poczta.fm

INFRASTRUKTURA KRYTYCZNA PAŃSTWA JAKO OBSZAR POTENCJALNEGO ODDZIAŁYWANIA TERRORYSTYCZNEGO

Streszczenie: Pojęcie „infrastruktura krytyczna" opisuje obiekty fizyczne, systemy zaopatrzenia, technologie informacyjne i sieci informatyczne, które w wyniku zniszczenia, zakłócenia, uszkodzenia stają się niedostępne przez dłuższy okres, przez co mogą znacząco uderzać w społeczne lub ekonomiczne warunki społeczeństwa, lub wpływać na możliwości zapewnienia obrony i bezpieczeństwa narodowego. W publikacji autor przedstawia zagrożenia obiektów infrastruktury krytycznej przez terrorystów, które obejmują zabójstwa, porwania osób i samolotów, zagrożenia detonacją ładunków bombowych, cyberatakami (wykorzystującymi systemy komputerowe) i użycie broni chemicznej, biologicznej, nuklearnej i radiologicznej. Cele najbardziej narażone na przeprowadzenie ataku terrorystycznego obejmują obiekty wojskowe i cywilne obiekty rządowe, międzynarodowe porty lotnicze, duże miasta i obiekty o dużym znaczeniu. Terroryści mogą również przeprowadzić ataki na miejsca zgromadzenia dużej liczby osób, systemy zaopatrzenia w wodę i żywność, centra użytkowe oraz centra zarządzania przedsiębiorstwami. Ponadto, terroryści są zdolni do wywoływania strachu poprzez przesyłanie ładunków wybuchowych lub środków chemicznych i biologicznych za pomocą poczty. Opracowanie opisuje przykłady ataków terrorystycznych, elementy infrastruktury krytycznej w historii współczesnego terroryzmu międzynarodowego. Na zakończenie, autor przedstawia metody ochrony infrastruktury krytycznej wobec zagrożeń, w tym także atakami terrorystycznymi.

Słowa kluczowe: bezpieczeństwo państwa, infrastruktura krytyczna, terroryzm międzynarodowy, ataki terrorystyczne.

Dla sprawnego funkcjonowania gospodarki nowoczesnych społeczeństw, opartej na wysoko rozwiniętej technice, niezbędne jest niezakłócone działanie różnorodnych jej elementów (zaopatrzenie w energię, wodę, rozwinięte i szeroko dostępne sieci telekomunikacyjne i komputerowe, sprawnie działający transport). Zabezpieczenie obiektów, instalacji i usług zapewniających zaspokojenie tych podstawowych potrzeb społeczeństwa, w oparciu o systemy określane mianem infrastruktury krytycznej, ma zasadnicze znaczenie w kształtowaniu należnego poziomu bezpieczeństwa obywateli. Te obszary działalności narażone są na nieustanne zakłócenia i awarie, w tym także ataki terrorystyczne (np. atak w 1995r. japońskiej sekty Aum Shinrikyo na tokijskie metro przy użyciu sarinu, atak Al-Kaidy w 2004r. na kolej podmiejską w Madrycie, czy w 2005r. na metro w Londynie).

Rosnące znaczenie obiektów i systemów infrastruktury krytycznej dla bezpieczeństwa państwa wynika z ich strategicznego znaczenia dla podtrzymania niezakłóconego funkcjonowania państwa w warunkach współczesnych zagrożeń. Dlatego niezmiernie ważne jest przedsięwzięcie odpowiednich kroków, mających na celu zabezpieczenie tych elementów poprzez odpowiednią ich ochronę. Pozwoli to na zapewnienie ciągłości działania i integralności infrastruktury krytycznej oraz szybkiego odtwarzania na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Ogólna charakterystyka infrastruktury krytycznej

Pojęcie „infrastruktura krytyczna" (IK) jest stosunkowo nowe. Zaczęto się nim posługiwać w Stanach Zjednoczonych i Kanadzie w latach 90. ubiegłego wieku. Mianem tym określano „systemy i instalacje niezbędne do funkcjonowania nowoczesnego społeczeństwa i administracji" (Cichoń, 2007, s. 28).

Nieco inna definicja infrastruktury krytycznej została zawarta w Dyrektywie Rady UE 2008/114/WE z 8 grudnia 2008 r. (art 2): „infrastruktura krytyczna oznacza składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji".

W Polsce pojęcie IK pojawiło się najpierw w związku z rozszerzeniem kontaktów z NATO w 2002r. (Cichoń, 2007, s. 28). Na stałe weszło ono do systemu prawnego wraz przyjęciem przez Sejm 26 kwietnia 2007 r. Ustawy o zarządzaniu kryzysowym, w której dokonano zdefiniowania jej elementów.

Definicję pojęcia „infrastruktura krytyczna" zamieszczono w art. 3 pkt 2 wspomnianej Ustawy. Według jej zapisów, są to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców"(Dz.U. 2007, nr 89 poz. 590 z późn. zm.).

W dalszej części definicji ustawodawca podaje, że „infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,

k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych" (Dz.U. 2007 nr 89 poz. 590 z późn. zm.).

Tabela 1. Przykładowa klasyfikacja kategorii obiektów infrastruktury krytycznej.

System	Rodzaje obiektów
Zaopatrzenie w energię i paliwa	Elektrownie i inne obiekty elektroenergetyczne, bazy, składy i magazyny paliw, zakłady mające bezpośredni związek z wydobywaniem kopalin i ich pochodnych, sieci transportu, przesyłu i dystrybucji energii i paliw.
Łączność i sieci teleinformatyczne	Infrastruktura operatorów publicznych świadczących usługi pocztowe, sieci telekomunikacyjne i teleinformatyczne oraz związane z nimi obiekty, a także systemy teleinformatyczne służące do przetwarzania danych i związane z nimi obiekty. Obiekty Telewizji Publicznej oraz Polskiego Radia.
Finansowy	Obiekty NBP oraz BOK, PWPW S.A., Mennicy Państwowej S.A. oraz obiekty i systemy istotne dla zapewnienia stabilności systemu finansowego, systemy płatności, systemy rozliczeń i rachunku papierów wartościowych wraz z obsługującą infrastrukturą oraz rynki regulowane.
Zaopatrzenia w żywność i wodę	Obiekty bezpośrednio związane z produkcją żywności i gromadzeniem wody, a także infrastruktura związana z przechowywaniem i transportem do bezpośrednich odbiorców.
Ochrona zdrowia	Obiekty i systemy istotne ze względu na zapewnienie opieki i świadczeń zdrowotnych obywatelom (szpitale, placówki zdrowia), magazyny rezerw państwowych produktów leczniczych i wyrobów medycznych oraz zakłady i przedsiębiorstwa farmaceutyczne.
Transportowy i komunikacyjny	Obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, śródlądowego i morskiego.
Ratowniczy	Wytypowane obiekty Państwowej Straży Pożarnej oraz infrastruktura jednostek powołanych do ratowania życia i ochrony własności.
Zapewniający ciągłość funkcjonowania państwa	Obiekty urzędów wojewódzkich, obiekty jednostek organizacyjnych służb zespolonych, inspekcji i straży.
Administracji publicznej	Obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji lub przez niego nadzorowanych, obiekty podległe Ministrowi Spraw Zagranicznych, obiekty jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, obiekty Agencji Wywiadu, Agencji Bezpieczeństwa Wewnętrznego, Policji, Straży Granicznej, Biura Ochrony Rządu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, obiekty znajdujące się we właściwości Ministra Sprawiedliwości oraz ważne obiekty innych organów centralnych.
Produkcyjny sektora bezpieczeństwa	Zakłady produkujące, remontujące lub magazynujące uzbrojenie i sprzęt wojskowy oraz środki bojowe, a także zakłady, w których są prowadzone prace badawczo-rozwojowe lub konstruktorskie w zakresie produkcji na potrzeby bezpieczeństwa i obronności państwa.
Ochronne	Instalacje i urządzenia służące ochronie granicy państwowej, posterunki monitoringu.

Źródło: Sztab Generalny WP, Zarząd Planowania Operacyjnego – P3, *Materiały wyjściowe do Koncepcji Przestrzennego Zagospodarowania Kraju na lata 2008-2033,* P3/1061/08 z 9 maja 2008r.

Przedstawiona normatywna systematyka infrastruktury krytycznej jest prawnym uregulowaniem możliwości ingerencji państwa w pewien „system naczyń połączonych", w celu zapewnienia ciągłości funkcjonowania sfery niezbędnej człowiekowi do życia i zabezpieczenia jej przed różnego rodzaju niekorzystnymi zdarzeniami oraz ustalania stopnia ich zabezpieczenia na te zdarzenia. Podana lista ma bardzo szeroki kontekst znaczeniowy, co może wzbudzać pewne wątpliwości dotyczące precyzyjnego określenia poszczególnych komponentów (Walczak, 2009, s. 93-109). Dlatego, analizując infrastrukturę poszczególnych sektorów, w *Materiałach wyjściowych do Koncepcji Przestrzennego Zagospodarowania Kraju na lata 2008-2033 opracowanych w* Sztabie Generalnym Wojska Polskiego (2008) zaproponowano podział na grupy obiektów zakwalifikowane jako elementy infrastruktury krytycznej (Tabela 1).

Obszary, obiekty lub urządzenia wchodzące w skład infrastruktury krytycznej, a podlegające ochronie są umieszczane w ewidencji na podstawie decyzji administracyjnych odpowiednich organów.

W ramach ochrony obowiązkowej osoba odpowiedzialna za jej bezpieczeństwo (lub osoba przez nią upoważniona) opracowuje i uzgadnia z właściwym terytorialnie komendantem wojewódzkim policji planu ochrony tych obszarów, obiektów i urządzeń.

Zagrożenia infrastruktury krytycznej

Obiekty infrastruktury krytycznej są bardzo podatne na różnego rodzaju zagrożenia. W przeszłości elementy tworzące obecną infrastrukturę krytyczną funkcjonowały jako systemy niezależne, lub też zależne od siebie w niewielkim stopniu. Obecnie, systemy składające się na infrastrukturę krytyczną państwa cechuje coraz większe wzajemne powiązanie i uzależnienie. Postępująca konsolidacja, centralne sterowanie sieciocentryczne, informatyzacja zarządzania stwarzają nowe okoliczności zwiększające wrażliwość funkcjonowania w ramach systemów i uzależnienie ich prawidłowego funkcjonowania od elementów powiązanych. Postęp, poza sferą korzyści, powoduje również potencjalnie negatywne uwarunkowania. W dobie globalizacji i rozwoju technologicznego poszczególne obiekty infrastruktury są coraz bardziej współzależne nie tylko w wymiarze jednego państwa, ale również w wymiarze międzynarodowym. Powiązania ponadgraniczne powodują, że skutki ewentualnych zaburzeń mogą być bardzo istotne dla państw. Istniejąca sieć wzajemnych powiązań powoduje, że naruszenie sprawności części infrastruktury krytycznej, dotyczącej jednego sektora może powodować wadliwość funkcjonowania innych systemów, a nawet ich uszkodzenie (tak zwany efekt „klocka domino").

Inną kategorię problemów, zagrażających funkcjonowaniu infrastruktury krytycznej, jest uzależnienie od surowców zasilających, które pozostają w wyłącznej gestii dostawców. Do grupy tej zaliczyć należy również generowanie zagrożenia przez obiekty infrastruktury krytycznej na skutek ich specyficznej podatności konstrukcyjnej na uszkodzenie.

Zagrożenia dla infrastruktury krytycznej obejmują następujące obszary:

- zagrożenia obszaru środowiskowego (katastrofy naturalne, zawodność systemów energetycznych oraz zasilania zapasowego, sabotaż oraz zagrożenia terrorystyczne instalacji i obiektów fizycznych, odporność na włamania i szczelność systemów kontroli dostępu);

- zagrożenia obszaru technologicznego (brak alternatywnych torów transmisyjnych, występowanie błędów produkcyjnych lub konstrukcyjnych – szczególnie niebezpieczne w przypadku monopolu jednego dostawcy, zła jakość stosowanego oprogramowania i jego bezpieczeństwo, czyli możliwość przejęcia w przypadku wystąpienia błędu lub usterki, odporność technologii transmisji na przechwycenie lub zakłócenia elektromagnetyczne oraz warunki środowiskowe, okres funkcjonowania urządzeń do pierwszej awarii oraz odporność na warunki pracy),
- zagrożenia obszaru danych i sieci poprzez techniki transmisji oraz protokoły przesyłania danych, projektowanie i skalowanie, standardy implementowania sprzętu różnych dostawców, brak synchronizacji sieci z elementami toru transmisji, stopień skomplikowania;
- zagrożenia obszaru czynnika ludzkiego (kradzież, sabotaż, terroryzm, zemsta, niezadowolenie obywateli lub pracowników, nieświadome szkodliwe działanie wynikające z niewiedzy użytkownika, brak polityki bezpieczeństwa oraz nierealistyczne regulacje prawne lub luki prawne, brak wykwalifikowanej kadry menedżerskiej oraz brak szkoleń i kampanii uświadamiającej).

Analiza poszczególnych obszarów wskazuje, że atak terrorystyczny stanowi zagrożenie mające niezwykle istotne znaczenie dla bezpieczeństwa państwa. Jak wynika z dotychczasowych przypadków zamachów terrorystycznych, celem ataków mogą stać się ośrodki władzy oraz infrastruktury gospodarczej i publicznej, a także obiekty, których zniszczenie stanowi poważne zagrożenie dla bezpieczeństwa, głównie takie jak: zapory wodne, zakłady przechowujące toksyczne środki przemysłowe i ujęcia wody (Lidwa, Krzeszowski, Więcek, Kamiński, 2012, s. 31).

Każdy z systemów zaliczanych do infrastruktury krytycznej może być potencjalnym obiektem ataku terrorystycznego, choć cel ataku może być różny. Skuteczność przeciwdziałania zamachom w dużej mierze zależy od przyjęcia za wysoce prawdopodobną możliwość zaatakowania każdego z tych systemów oraz podjęcia działań zapobiegawczych mających na celu zmniejszenie prawdopodobieństwa dokonania zamachu. Jedną z najistotniejszych cech współczesnego terroryzmu jest jego nieprzewidywalność co do miejsca oraz formy ataku, użytych środków oraz skutków, jakie mogą wywołać. Dlatego też, zagrożenia ze strony organizacji terrorystycznych należy rozpatrywać w odniesieniu do systemów oraz tworzących je obiektów infrastruktury krytycznej.

- System zaopatrzenia w energię, surowce energetyczne i paliwa

Jednym z podstawowych systemów infrastruktury krytycznej jest system zaopatrzenia w energię, surowce energetyczne i paliwa, który składa się z trzech podsystemów:

a) wytwarzania (pozyskiwania) energii,
b) przesyłu energii i paliw,
c) dystrybucji i dostaw energii i paliw do odbiorców.

W odniesieniu do jednego z podsystemów, jakim są elektrownie, możliwe są następujące formy ataku terrorystycznego (Lidwa at al., 2012, s. 32):

a) bezpośredni atak na system – celem ataku jest fizyczna infrastruktura systemu. Mogą zostać zaatakowane stacje elektroenergetyczne lub kluczowe linie w celu wywołania awarii na dużym obszarze sieci;

b) atak poprzez system elektroenergetyczny – mogą zostać użyte niektóre instalacje w systemie elektroenergetycznym do zaatakowania innych elementów jego infrastruktury, wywołany silny impuls elektromagnetyczny w sieci w celu uszkodzenia komputerów i infrastruktury telekomunikacyjnej.

Jako przykład ataku terrorystycznego na obiekty systemu energetycznego można przedstawić zamach roku na elektrownię wodną w Republice Kabardo-Bałkarii na rosyjskim Kaukazie w 2010r. W wyniku ataku zginęło dwóch strażników oraz uszkodzone zastały dwa z trzech generatorów elektrowni (Newsweek.pl, 2010). Atak nie miał istotnego znaczenia ekonomicznego, jednak pokazał, że takie obiekty mogą stanowić cel działania terrorystów.

Niezwykle istotnym zagadnieniem bezpieczeństwa obiektów infrastruktury energetycznej jest zagrożenie potencjalnym atakiem elektrowni jądrowych. Obecnie w Europie pracuje około 220 reaktorów (Zięba, 1999, s. 112-114). Najbardziej rozbudowane systemy pozyskiwania energii atomowej mają państwa najbardziej zagrożone terroryzmem: Francja, Wielka Brytania, Niemcy i Rosja.

Polska nie posiada obecnie elektrowni jądrowej, jednak w jej bliskim sąsiedztwie w promieniu do ok. 300 km od granic, pracuje 10 elektrowni tego typu (Litwa – 1, Ukraina – 2, Słowacja – 2, Węgry – 1, Czechy – 2, Niemcy – 1, Szwecja – 1) z 23 blokami energetycznymi, które w przypadku awarii mogą znacząco zagrozić ludności zamieszkującej obszar naszego kraju.

Najlepszy przykład zagrożenia skażeniami radiologicznymi środowiska naturalnego, w kontekście ich transgranicznego przemieszczania, stanowi awaria elektrowni jądrowej w Czarnobylu. W wyniku emisji radionuklidów, będącej następstwem awarii elektrowni, doszło do skażenia państw na terenie całej Europy. Największe skażenie objęło tereny państw Półwyspu Skandynawskiego, Polski, Czechosłowacji, a także części Niemiec i Włoch.

Elektrownie jądrowe wraz z instalacjami zawsze podlegały szczególnej ochronieze względu na zagrożenie, z jakim wiązało się przejęcie kontroli nad systemami sterowania pracą reaktorów.

Obecnie najbardziej prawdopodobne zagrożenie dla elektrowni to:

- możliwość przeprowadzenia sabotażu wewnątrz elektrowni przez osobę kierującą się korzyściami materialnymi lub ideologią,
- przejęcie systemu sterowania pracą reaktorów z poziomu sterowni przez uzbrojoną grupę terrorystyczną, która przeprowadziła udany atak i obezwładniła ochronę elektrowni,
- uderzenie dużego samolotu (samolotu pasażerskiego lub transportowego) w reaktor elektrowni. Jest to szczególnie niebezpieczne dla elektrowni starego typu, których reaktory nie zostały zabezpieczone przed taką ewentualnością (Wójtowicz, 2006,

s.21)[1]. Reaktory nowego typu konstruowane są w sposób chroniący je przed tego rodzaju atakiem.

Stan bezpieczeństwa nowoczesnych elektrowni jądrowych nie budzi zastrzeżeń, jednak przeprowadzenie skutecznego ataku terrorystycznego na jedną z elektrowni jądrowych na terenie sąsiednich państw może mieć znaczenie dla bezpieczeństwa i funkcjonowania naszego kraju. Należy mieć nadzieję, że jest to zadanie niezwykle trudne dla terrorystów, ze względu na ochronę i istniejące systemy zabezpieczeń, jednak nie oznacza to, że jest niemożliwe.

Z pewnością, plany budowy elektrowni jądrowej w naszym kraju muszą uwzględniać jej zabezpieczenie również przed taką ewentualnością.

- System łączności oraz sieci teleinformatycznych

Systemy łączności oraz sieci teleinformatycznych to systemy i sieci, których nieprawidłowe funkcjonowanie lub uszkodzenie – niezależne od przyczyn i zakresu – może spowodować istotne zagrożenie dla życia lub zdrowia ludzi, interesów obronności oraz bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę. Wynika stąd, że chodzi o codzienne sprawne działanie systemów: energetycznego, finansowego, wodociągów, transportu, służby zdrowia, ale także o sytuacje nadzwyczajne (kryzysowe). We współczesnej gospodarce od tego rodzaju infrastruktury zależy prawidłowe funkcjonowanie państwa. Infrastruktura ta pozostaje przeważnie w rękach prywatnych (sieci komórkowe, sieci dostępowe do Internetu, korporacyjne sieci bankowe, itp.). Wynika stąd, że warunkiem zapewnienia bezpieczeństwa tej infrastruktury na poziomie krajowym jest współpraca pomiędzy zarządcami poszczególnych jej części (tzw. partnerstwo publiczno-prywatne).

Wraz z rozwojem globalnej sieci internetowej, negatywne zjawiska świata realnego, takie jak przestępczość i terroryzm, zaczęły przenikać do świata wirtualnego. Cyberterroryzm to dokonywanie aktów terroru przy pomocy zdobyczy technologii informacyjnej. Ma na celu wyrządzenie szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. Polega na celowym zakłóceniu interaktywnego, zorganizowanego obiegu informacji w cyberprzestrzeni. Należy go odróżnić od innych nielegalnych aktów, takich jak przestępczość komputerowa, szpiegostwo gospodarcze, czy też wojna informacyjna. Terroryzm cybernetyczny musi skutkować pewnym stopniem przemocy w stosunku do ludzi lub ich własności, a przynajmniej wywoływać strach.

O terroryzmie cybernetycznym możemy mówić jedynie wtedy, kiedy mamy do czynienia z politycznie motywowanym atakiem przy użyciu sieci teleinformatycznych. W pozostałych przypadkach takie ataki klasyfikuje się zazwyczaj jako przestępstwa cybernetyczne bez podtekstu politycznego. Z kolei chęć zwrócenia uwagi opinii publicznej na określony problem społeczny, bądź polityczny poprzez niedozwolone działania w sieci, określa się jako haktywizm.

[1] Szwajcarska elektrownia jądrowa KKL Leibstadt po przeprowadzeniu symulacji prawdopodobnych skutków ataku przesłoniła reaktor specjalną kopułą znoszącą uderzenia i eksplozje.

Cyberterroryzm jest atrakcyjną opcją dla współczesnych terrorystów z kilku powodów. Po pierwsze, jest tańszy niż tradycyjne metody terrorystyczne. Wszystko, co jest potrzebne, to komputer osobisty i połączenie on-line. Nie potrzeba kupować broni czy materiałów wybuchowych, zamiast tego, mogą tworzyć i dostarczać wirusy komputerowe poprzez linię telefoniczną, kabel, lub połączenie bezprzewodowego. Po drugie, cyberterroryzm jest bardziej anonimowy niż tradycyjne metody terrorystyczne. Tak jak wielu internautów, terroryści korzystają z „nicków" internetowych lub mogą zalogować się na stronie internetowej jako „niezidentyfikowany użytkownik, gość", co jest bardzo trudne dla wytropienia prawdziwej tożsamości terrorysty. W cyberprzestrzeni brakuje barier fizycznych, takich jak punkty kontrolne, nie ma również granic dla poruszania się Po trzecie, różnorodność i liczba celów jest ogromna. Cyberterrorysta może kierować komputerem i sieciami komputerowymi rządów, osób prywatnych, obiektów użyteczności publicznej, prywatnych linii lotniczych, itd. Sama liczba i złożoność potencjalnych celów gwarantuje, że terroryści mogą znaleźć niedociągnięcia i słabości oraz je wykorzystać. Liczne badania wykazały, że obiekty infrastruktury krytycznej, takie jak sieci elektroenergetyczne są szczególnie narażone na ataki cyberterrorystyczne, ponieważ struktury i systemy komputerowe służące do ich uruchomienia są wysoko złożone i próba wyeliminowania wszystkich słabości wydaje się niemożliwa. Po czwarte, działania mogą być prowadzone zdalnie. Cyberterroryzm wymaga mniej szkoleń fizycznych, psychologicznych, inwestycji, podróży, niż konwencjonalny terroryzm (Weimann, 2004).

Działaniami nagłośnionymi publicznie nazywanymi powszechnie cyberterroryzmem były ataki typu DoS (*Denial of Service*) na komputery NATO w czasie wojny w Kosowie w 1999r. W stanie wojny, ale wojny elektronicznej, znalazły się Stany Zjednoczone i ChRL w maju 2001r., kiedy amerykańscy hackerzy zaatakowali masowo chińskie strony internetowe. W odpowiedzi, Chińczycy włamali się na strony amerykańskiej administracji i wielkiego biznesu. Obyło się bez wielkich strat materialnych, ale efekt pozwolił zdać sobie sprawę z tego, jak mogą wyglądać wojny w przyszłości (Pietrzak, 2002).

- System finansowy

Kolejny potencjalny cel ataków terrorystycznych stanowi system finansowy państwa. Do obiektów w tej grupie ryzyka zaliczyć można siedziby główne banków i ich placówki terenowe, siedziby giełd finansowych, mennice i wytwórnie papierów wartościowych, systemy płatnicze, centra rozliczeniowe dla kart płatniczych oraz sieci bankomatowe i POS. Atak terrorystyczny może przybrać formę zamachu bombowego mającego na celu zniszczenie infrastruktury i spowodowanie strat w personelu i klienteli lub formę cyberataku na finansowe systemy informatyczne.

Cyberterrorystyczne ataki skierowane na wymienione elementy sektora bankowego mogą skutkować (Syta, 2009, s. 698):

- zakłóceniem swobodnego przepływu środków pieniężnych,
- zafałszowaniem danych dotyczących bieżącej sytuacji gospodarczej i finansowej,
- manipulowaniem notowaniami kursowymi bądź giełdowymi,
- odebraniem firmom i osobom prywatnym bieżącego dostępu do zgromadzonych środków,
- zafałszowaniem informacji dotyczących poziomu zadłużenia,

– kradzieżą i legalizacją znacznych sum.

Wszystkie z powyższych ataków stanowią potencjalne zagrożenie dla stabilności gospodarki. W niesprzyjających okolicznościach mogłyby stać się pretekstem do histerii i związanych z nią gwałtownych ruchów jak na przykład przecena akcji, czy masowe wypłacanie środków z rachunków bankowych.

- System zaopatrzenia w żywność

Zaopatrzenie społeczeństwa w żywność to potrzeba z rzędu elementarnych potrzeb egzystencjalnych. Zakłócenia w tym względzie wywołać mogą nie tylko niezadowolenie społeczne, ale mogą być przyczyną powstania groźnych chorób, a nawet epidemii. W systemie zaopatrzenia w żywność do celowych zakłóceń dojść może na różnych poziomach przygotowania żywności. Może to mieć miejsce w fazie (Zięba, 1999, s. 33):

– produkcji rolnej (uprawa i hodowla),
– transportu i przechowywania surowców,
– produkcji i przechowywania żywności,
– dystrybucji,
– sieci gastronomicznej.

Celem działań terrorystycznych w stosunku do tego sektora gospodarki może być wywołanie znacznych strat w ludziach, wywołanie stanu paniki, bądź spowodowanie strat gospodarczych poprzez zahamowanie eksportu, jako efektu skażenia żywności na którymś z poziomów jej produkcji. Do środków, które mogą zostać wykorzystane przez terrorystów w tej działalności, zalicza się szczególnie środki biologiczne, chemiczne lub radioaktywne. Przy pomocy tych środków terroryści wpływać mogą na (Zięba, 1999, s. 33):

– zaburzenia w systemie dystrybucji żywności,
– wywołanie zaburzeń ekonomicznych w sektorze rolno-spożywczym przez wprowadzenie patogenów niszczących plony lub powodujących choroby zwierząt (np. pryszczycy), a w najgorszym przypadku do wywołania klęski głodu (w przypadku wywołania epidemii roślin lub zwierząt na znacznym obszarze,
– poczucie bezpieczeństwa obywateli poprzez celowe podważanie zaufania konsumentów do wytwarzanej żywności, a tym samym władz, które rzekomo nie troszczą się o stan zdrowia obywateli.

Szczególnie wrażliwymi elementami systemu produkcji i dystrybucji żywności są zakłady przemysłowe, wytwarzające gotowe produkty oraz zakłady gastronomiczne, w których istnieje dostęp osób postronnych do przygotowywanych potraw.

Prowadzenie ataków terrorystycznych przeciwko sektorowi rolniczemu określa się mianem agroterroryzmu. Stanowi on rodzaj terroryzmu, a ściślej rzecz biorąc bioterroryzmu i może być definiowany, jako celowe uwolnienie patogenów zwierzęcych lub roślinnych do wywołania strachu, strat ekonomicznych oraz destabilizacji państwa.

Znane są przypadki użycia trucizn i broni masowego rażenia przeciwko sektorowi rolniczemu w atakach terrorystycznych:

– w 1978 roku Arabska Rada Rewolucyjna doprowadziła do zatrucia transportu pomarańczy z Jaffy, próbując w ten sposób osłabić gospodarkę Izraela (Żuber, 2003, s. 205-211).

- w 1984 roku w niewielkim miasteczku Dalles w stanie Oregon, grupa wyznawców Bhagwana Shree Rajneesha zatruła lokalny zbiornik wody i zakaziła bary sałatkowe w restauracjach bakterią *Salmonella,* w nadziei „ogłupienia" miejscowej populacji i przechylenia szali ważnych wyborów lokalnych na korzyść sekty (Hoffman, 2001, s. 116), (Chalk, 2004, s. 28; Żuber, Sawczak, 2004, s. 54-64).
- w latach 1983–87 Tamilowie stosowali środki biologiczne przeciwko Syngalezom, w tym ok. do niszczenia upraw herbaty na Sri Lance (Narayan Swamy, 1994; O'Balance, 1989; Gunaratna, 1987, s. 51-52).
- w 1997 roku osadnicy izraelscy ze Strefy Gazy użyli chemikaliów w celu zniszczenia palestyńskich upraw winogron. W wyniku ataku zniszczono ok. 17.000 ton winogron (Karasik, 2002, s. 19).
- w 2000 roku, w Wielkiej Brytanii pojawiła się wśród trzody chlewnej epidemia pryszczycy. Niektóre źródła podały, że mógł to być atak terrorystyczny osób powiązanych z osobą Osamy bin Ladena. Niektórzy wiązali epidemię z odwetem za ataki rakietowe wojsk amerykańskich i brytyjskich na obiekty irackie.

To tylko niektóre z przypadków ataków agroterrorystycznych, jednak stanowią one spektakularne przykłady słabo chronionej dziedziny gospodarki, jaką jest rolnictwo. Wiadomo, iż jest ono żywotną gałęzią gospodarki wszystkich krajów. Dlatego też atak biologiczny na sektor rolny może okazać się brzemienny w skutki, takie jak (Żuber, 2006, s. 158):

- głęboka dezorganizacja życia społecznego,
- bezpośrednie straty w plonach lub hodowli zwierząt, które z kolei mogą doprowadzić do niedoborów żywności, drastycznych podwyżek cen żywności i bezrobocia,
- destabilizacja struktur społecznych i politycznych,
- straty wynikające z działań ograniczania skutków wybuchów zachorowań odżywnościowych (interwencyjne wybijanie stad i niszczenie plonów), które mogą przekraczać o kilka rzędów wielkości straty wynikające bezpośrednio z samych zachorowań,
- straty wynikające z wprowadzenia ograniczeń fitosanitarnych w handlu międzynarodowym,
- straty wynikające ze skutków pośrednich (destabilizacja rynku).

Atak na sektor rolny może zostać zainicjowany przez:

- kraje działające z motywów militarnych, politycznych, ideologicznych lub gospodarczych,
- korporację rolną łączącą producentów, przetwórców oraz dostawców produktów rolnych, liczących na korzyści wynikające ze skutków finansowo-rynkowych udanego ataku biologicznego,
- zorganizowaną przestępczość, ze względu na wysoką stawkę, jaką dla przestępców stanowi sektor rolny, w związku z umiejscowieniem przemysłu narkotykowego w hodowli upraw,
- organizacje terrorystyczne, dążące do zadania ciosu przeciwstawiającym się im państwom i narodom,
- innych osobników (szaleńcy, osoby zawiedzione określonymi działaniami).

Przeprowadzenie ataku na sektor rolny jest relatywnie łatwe, ponieważ ataki tego typu wyróżniają pewne szczególne cechy:

- czynniki te nie stanowią zagrożenia dla sprawców (z wyjątkiem kilku czynników wywołujących choroby odzwierzęce),
- trudności techniczne w konwersji tych czynników w narzędzia agresji są niewielkie,
- liczne potencjalne cele ataku są słabo chronione (istnieje wiele słabo strzeżonych obiektów, gdzie może potencjalnie nastąpić uwolnienie zwierzęcych lub roślinnych czynników chorobotwórczych),
- bariery moralne są łatwiejsze do pokonania (reakcja na atak biologiczny przeciw uprawom lub inwentarzowi żywemu byłaby mniej zdecydowana, niż na atak powodujący natychmiastowe straty w ludziach, natomiast prawdopodobieństwo wykrycia sprawców i odwetu na nich jest mniejsze),
- maksymalizacja skutków nie wymaga wielu ognisk inicjujących (jeśli celem jest wywołanie zakłóceń w handlu międzynarodowym poprzez wprowadzenie choroby wysoce zaraźliwej),
- wystarczy jedno źródło punktowe w celu stworzenia wrażenia, że zachorowania zostały wywołane przez czynniki naturalne,
- stosunkowo łatwo jest, nie przekraczając granic, osiągnąć wielopunktowość ognisk zachorowań poprzez zanieczyszczenie importowanych pasz lub nawozów.

Skutkiem udanego ataku terrorystycznego na przemysł spożywczy będą nie tylko liczne zachorowania i zgony, lecz także wysokie straty ekonomiczne rolników, zakładów przetwórczych, firm transportowych, dystrybutorów żywności, właścicieli sklepów, restauracji i punktów gastronomicznych, co może spowodować poważne zakłócenie funkcjonowania państwa.

- System zaopatrzenia w wodę

Nie mniej wrażliwym systemem jest system zaopatrzenia w wodę zwłaszcza dużych aglomeracji miejskich. Tworzą go ujęcia wody pitnej i wodociągi. Atak na ten system polegać może na skażeniu ujęć wody przy pomocy środków biologicznych lub chemicznych. Celem ataku terrorystycznego z użyciem tego rodzaju broni będzie spowodowanie na znacznym obszarze śmierci lub schorzeń mogących przybrać rozmiar epidemii, co spowodować może utratę zaufania do władz oraz destabilizację struktur społecznych i politycznych.

- System ochrony zdrowia

Niezmiernie istotnym systemem infrastruktury krytycznej bezpośrednio wpływającym na poczucie bezpieczeństwa przez obywateli jest system ochrony zdrowia.

Zakłócenie funkcjonowania tego systemu spowodować może wzrost niezadowolenia społecznego wynikającego z poczucia zagrożenia oraz troski o losy ludzi słabych i chorych niezdolnych do samodzielnego zapewnienia sobie bezpieczeństwa. I choć dotychczas brakuje dowodów na takie działanie, to nie można go wykluczać z uwagi na łatwość dostępu do obiektów służących ochronie zdrowia. Atak na te obiekty może być wykonany przy pomocy środków chemicznych (niekoniecznie trujących), lub też groźby

podłożenia ładunku materiału wybuchowego zmuszającego personel szpitala do ewakuacji chorych, zaangażowania służb ratowniczych i porządkowych. Działania takie mogą stanowić element odwracający uwagę wspomnianych służb od zamachu terrorystycznego w innym obiekcie lub utrudniać udzielanie pomocy osobom poszkodowanym podczas innego zamachu.

- System transportu i komunikacji

Analiza zamachów terrorystycznych przeprowadzonych w ostatnich latach wskazuje, że infrastruktura krytyczna związana z transportem i komunikacją jest jednym z głównych celów ataków terrorystycznych. Narażone są wszystkie rodzaje transportu i komunikacji: lotnicza, kolejowa, drogowa i morska oraz infrastruktura z nią związana.

Obiektem ataku terrorystycznego mogą więc być elementy infrastruktury lotniskowej oraz samoloty zarówno na lotniskach, jak i podczas wykonywania operacji startu i lądowania, a także podczas lotu. Zagrożenie atakiem terrorystycznym na lotnisku jest ciągle zagrożeniem aktualnym. Terroryści, dążąc do zniszczenia infrastruktury portu lotniczego lub samolotów (zarówno na ziemi, jak i w powietrzu), mogą wnosić na teren lotniska oraz do samolotów ładunki wybuchowe. Mogą również dążyć do uprowadzenia samolotu pasażerskiego celem użycia go do ataku z powietrza na ważny, wybrany obiekt (np. budynek administracji rządowej, duży port lotniczy). Mogą też uprowadzić cywilny statek powietrzny, a następnie użyć go do ataku samobójczego na samolot pasażerski będący na lotnisku lub w powietrzu. Nie wyklucza się także użycia środków rażenia do zniszczenia (uszkodzenia) infrastruktury lotniska lub samolotu na lotnisku podczas wykonywania startu lub lądowania. Innym rodzajem zagrożenia terrorystycznego jest atak wymierzony w systemy kierowania ruchem powietrznym i zarządzania lotniskiem za pomocą sieci komputerowych przez cyberterrorystów.

Liczba ataków terrorystycznych na lotniczą infrastrukturę transportową jest znaczna i w historii zamachów terrorystycznych budziła zawsze wiele emocji, ze względu na tragiczną liczbę ofiar, z jaką wiązało się zniszczenie samolotu w powietrzu. Wśród najbardziej znanych przypadków ataków terrorystycznych można wymienić (Encyklopedia terroryzmu, 2004, s. 683-708):

- 1 listopada 1958r. – podczas pierwszego na świecie przypadku uprowadzenia samolotu, terroryści z Ruchu 26 czerwca porwali kubański samolot pasażerski i zmusili pilota do próby lądowania na opuszczonym lotnisku na Kubie; samolot rozbił się, w wyniku czego zginęło 17 spośród 20 osób obecnych na pokładzie;
- 22 lipca 1968r. – Ludowy Front Wyzwolenia Palestyny (LFWP) dokonał pierwszego w swej historii uprowadzenia samolotu; terroryści porwali w Rzymie samolot Boeing 707 izraelskich linii lotniczych El Al i skierowali go do Algierii. W charakterze zakładników przez 5 tygodni przetrzymywano 32 żydowskich pasażerów;
- 6 września 1970r. – „Niedziela Porwań" – LFWP uprowadził 3 samoloty z ponad 400 zakładnikami na pokładzie. Dwa z nich wylądowały w Jordanii, gdzie zostały wysadzone w powietrze, natomiast trzeci został wysadzony w Egipcie. Inny zespół terrorystów usiłował porwać nad Londynem samolot linii El Al, jednak bez powodzenia. Jedna z terrorystek, Leila Chaled, została schwytana przez policję. Kolejny samolot

linii El Al został porwany do Jordanii 9 września. Rządy Niemiec, Szwajcarii i Wielkiej Brytanii zgodziły się na spełnienie żądań LFWP i wypuściły z więzień wielu terrorystów, w tym Leilę Chaled;

- 8 maja 1972r. – izraelscy komandosi przeprowadzili szturm na lotnisku Lod w Izraelu na porwany samolot pasażerskich belgijskich linii lotniczych Sabena. W wyniku akcji zginęło 3 palestyńskich terrorystów z grupy Czarny Wrzesień, 5 izraelskich żołnierzy i 1 zakładnik. Pozostali pasażerowie zostali uwolnieni;
- 17 września 1973r. – palestyńscy terroryści podłożyli bombę w biurze linii lotniczych PanAm na lotnisku Fiumicino w Rzymie, zabijając 32 i raniąc 50 osób. Następnie terroryści, biorąc jako zakładników 7 włoskich policjantów, porwali samolot do Aten. Po zabiciu jednego z zakładników Palestyńczycy odlecieli do Kuwejtu, gdzie oddali się w ręce policji;
- 27 czerwca 1976r. – samolot pasażerski linii lotniczych Air France został porwany przez grupę terrorystów z grupy Baader-Meinhof oraz Ludowego Frontu Wyzwolenia Palestyny. Pilot został zmuszony do lądowania na lotnisku w Entebbe w Ugandzie. Terroryści przetrzymywali około 258 pasażerów i członków załogi jako zakładników, jednak wszystkich pasażerów, niebędących Żydami lub obywatelami Izraela, uwolniono. Terroryści byli wspierani przez rząd Ugandy. Trzeciego lipca izraelscy komandosi wylądowali w Ugandzie i uwolnili pozostałych zakładników. Podczas operacji zginęli wszyscy terroryści i 3 zakładników;
- 6 czerwca 1985r. – wybuch bomby podłożonej przez Frakcję Czerwonej Armii na lotnisku we Frankfurcie nad Menem spowodował śmierć 3 osób;
- 14 czerwca 1985r. – dwaj terroryści z libańskiego ugrupowania Hezbollah uprowadzili samolot Boeing 727 linii TWA lecący z Rzymu do Aten i zmusili pilotów do skierowania go do Bejrutu. Przez 17 dni przetrzymywali 8 członków załogi i 145 pasażerów. Zakładnicy zostali uwolnieni po tym, jak rząd Izraela w wyniku nacisków Stanów Zjednoczonych, spełnił żądania porywaczy i wypuścił 435 więźniów libańskich i palestyńskich;
- 21 grudnia 1988r. – samolot pasażerski należący do linii lotniczych PanAm eksplodował nad miasteczkiem Lockerbie w Szkocji, w wyniku wybuchu bomby umieszczonej na jego pokładzie na lotnisku we Frankfurcie nad Menem. Zginęło 259 osób znajdujących się na pokładzie. Zamachu dokonali dwaj agenci służb specjalnych Libii, którzy zostali po kilkunastu latach wydani przez władze Libii i w 2003 roku stanęli przed sądem w Holandii, a następnie skazani na kary wieloletniego więzienia;
- 17 lipca 1996r. – samolot pasażerski Boeing 747 należący do linii TWA eksplodował tuż po starcie z lotniska im. J.F. Keneddy'ego w Nowym Jorku i spadł do Oceanu Atlantyckiego u wybrzeży Long Island. Śmierć poniosło 230 pasażerów i członków załogi;
- 11 września 2001r. – dokonano największego w historii ataku terrorystycznego. Dziewiętnastu członków Al-Kaidy porwało 4 samoloty z pasażerami: dwa z nich uderzyły w wieżowce Światowego Centrum Handlu (World Trade Center), powodując ich pożar i zawalenie się, jeden uderzył w Pentagon, a czwarty, na pokładzie którego pasażerowie próbowali obezwładnić porywaczy, rozbił się pod Pittsburghiem. Zginęło

ponad 3 tys. osób, a kilka tysięcy zostało rannych. Straty finansowe na całym świecie liczone były w miliardach dolarów. O dokonanie zamachu oskarżono organizację terrorystyczną Al-Kaida.

To tylko wybrane przykłady działań terrorystów przeciwko lotniczej infrastrukturze transportowej. W historii współczesnego terroryzmu można wymienić ich znacznie więcej.

Bardzo wrażliwymi obiektami ataku terrorystycznego są dworce kolejowe i pociągi, w tym także metro. Dotychczasowe zamachy terrorystyczne na terenie tych obiektów, bądź próby ich dokonania, przeprowadzane były w godzinach szczytu komunikacyjnego i wymierzone były w podróżnych. Do ataków wykorzystywano zamachowców-samobójców. Oprócz ładunków bombowych, terroryści używali także broni chemicznej. Szczególnie narażone na ten rodzaj ataku są stacje podziemne i ich systemy wentylacyjne.

Wśród najbardziej znanych przypadków ataków na tego typu infrastrukturę transportową można wymienić:

- 8 sierpnia 1983r. – zginęło 12 osób, a 48 zostało rannych, kiedy neofaszyści zdetonowali ładunek wybuchowy w pociągu w pobliżu Bolonii we Włoszech;
- 23 maja 1977r. – trzynastu terrorystów z Moluków Południowych wzięło jako zakładników 85 pasażerów pociągu w Assen, w Holandii. Po 19 dniowym oblężeniu, przeprowadzono atak holenderskich komandosów, wyniku czego zginęli dwaj zakładnicy i wszyscy terroryści;
- 20 marca 1995r. –zamach z użyciem bojowego środka paraliżującego – sarinu, na zatłoczoną stację metra w centrum Tokio, 12 osób poniosło śmierć, a ponad 5 tys. osób zostało porażonych. Atak przeprowadziła sekta religijna Aum Shinrikyo (Najwyższa Prawda) kierowana przez Shoko Asaharę. Został on aresztowany dwa miesiące później, a po procesie sadowym skazany na karę śmierci;
- 11 marca 2004 r. – Największy zamach terrorystyczny w historii Europy. W podmiejskich pociągach jadących w kierunku centrum Madrytu wybuchło 10 bomb. Śmierć poniosło 2000 osób, a ponad 1400 zostało rannych. Początkowo rząd oskarżył o dokonanie zamachów ETA, lecz wkrótce okazało się, że za atakami stała Al-Kaida.
- 7 lipca 2005r. – Kolejny atak Al-Kaidy przeprowadzony na metro w Londynie oraz miejski autobus w porannych godzinach szczytu. Bomby wybuchły w tym samym czasie, kiedy w Gleneagles w Szkocji odbywał się szczyt państw G8 oraz w dzień po decyzji Międzynarodowego Komitetu Olimpijskiego o organizacji Letnich Igrzysk Olimpijskich w 2012 w Londynie, a także podczas procesu Abu Hamzy al-Masriego. W wyniku eksplozji zginęło 56 osób, a ponad 700 osób było rannych. Atak przeprowadziło czterech Brytyjczyków pochodzenia pakistańskiego oraz jeden Jamajczyk. Grupa ta przeprowadziła ataki w imieniu Al-Kaidy.

Zagrożenie stwarzające szczególne niebezpieczeństwo dla obywateli stanowi uszkodzenie lub zniszczenie, zwłaszcza w rejonach zaludnionych, wagonów, transportujących substancje niebezpieczne, w celu przedostania się ich do atmosfery, co może spowodować znaczną liczbę ofiar.

Porty morskie i nabrzeża, szczególnie w części dotyczącej ruchu pasażerskiego, mogą stanowić kolejny cel ataków terrorystów. Oprócz takich form ataku jak zamach bombowy, czy ostrzał osób z użyciem broni palnej i granatów, do zniszczenia infrastruktury

portowej mogą być użyte statki wypełnione materiałami wybuchowymi (gazowce) lub łatwopalnymi (tankowce i zbiornikowce), które zostaną zniszczone w strefie portowej. Dodatkowym niebezpieczeństwem jest zatopienie tankowca wypełnionego dużą ilością ropy u wybrzeży, co może spowodować katastrofę ekologiczną i blokadę komunikacyjną danego obszaru morskiego.

- System ratowniczy

Celem ataku terrorystycznego na obiekty infrastruktury systemu ratowniczego (centra zarządzania kryzysowego, strażnice Państwowej Straży Pożarnej, obiekty Państwowego Ratownictwa Medycznego, pogotowia techniczne) będzie destabilizacja centrów zarządzania i kierowania akcją ratowniczą, wyeliminowanie ratowników oraz zniszczenie pojazdów i sprzętu ratunkowego, lub też uniemożliwienia przeprowadzenia akcji ratunkowej, dotyczącej zamachu równoległego.

- System administracji publicznej

System zapewniający ciągłość funkcjonowania administracji publicznej stanowią obiekty administracji państwowej, zwłaszcza te, w których urzędują organy państwa odpowiedzialne za przeciwdziałanie, zwalczanie, rozpoznawanie terroryzmu, czy zarządzanie kryzysowe. Stanowią one jeden z głównych celów zamachów terrorystycznych na całym świecie, ze względu na swój strategiczny i symboliczny charakter. Zagrożone mogą być także bazy danych znajdujące się w tych obiektach.

Przykładem najbardziej spektakularnego ataku terrorystycznego na budynek rządowy jest wysadzenie 19 kwietnia 1995r. budynku federalnego w Oklahoma City, który został całkowicie zniszczony w wyniku eksplozji furgonetki wypełnionej nawozami sztucznymi i olejem napędowym. W zamachu zginęło 169 osób, a setki innych odniosły obrażenia. Wybuch miał miejsce w drugą rocznicę masakry na farmie Waco z 1993 roku. Sprawcą zamachu byli: Timothy Mc Veigh – weteran wojny w Zatoce Perskiej, oraz Terry Nichols. Mc Veigh został skazany na karę śmierci i wyrok wykonano.

- System produkcji, składowania, przechowywania oraz stosowania substancji chemicznych i promieniotwórczych

Systemy produkcji, składowania, przechowywania oraz stosowania substancji chemicznych i promieniotwórczych, stanowią opłacalne obiekty ataków terrorystycznych Skutki ataków przy użyciu ładunków wybuchowych lub artyleryjskich środków rażenia mogą powodować rozległe pożary lub uwolnienie do atmosfery znacznych ilości substancji trujących, tzw. toksycznych środków przemysłowych (TŚP) powodujących masowe zatrucia ludzi lub skażenie środowiska.

Przeniknięcie małych grup terrorystycznych lub pojedynczych terrorystów jest dość łatwe ze względu na niezbyt szczelny system ochrony zakładów przemysłowych, co wynika z rozległości terenu na którym je rozlokowano, a ponadto, brakuje możliwości skutecznego weryfikowania dokumentów uprawniających do wejścia na teren zakładu, które mogą posiadać terroryści. Dokumenty takie z pewnością byłyby doskonale sfałszowane, przy użyciu najnowszych technik komputerowych.

Źródłem takich skażeń mogą być również TŚP przewożone środkami transportu kolejowego i drogowego, na które przeprowadzenie ataku jest znacznie łatwiejsze.

Szczególną uwagę zwraca się na ochronę obiektów, w której przechowywane są materiały promieniotwórcze. Przejęcie takich materiałów może być niezwykle niebezpieczne, gdyż mogą posłużyć do wyprodukowania tzw. „brudnej bomby", będącej rodzajem broni radiologicznej. Detonacja tego typu ładunku może spowodować skażenie na znacznym obszarze, a przy dużych stężeniach radionuklidów wywołać chorobę popromienną u osób narażonych na oddziaływanie promieniowania jonizującego.

Ochrona infrastruktury krytycznej

W związku z obecnością całej gamy potencjalnych zagrożeń nie jest możliwe przewidzenie wszelkich możliwości i okoliczności ich wystąpienia. Celowe jest zatem przygotowanie możliwie dużej liczby scenariuszy reagowania, umożliwiających elastyczne modelowanie i działanie modułowe w zależności od rozwoju sytuacji. System ochrony powinien również przewidywać działania naprawcze, odtwarzające sprawność infrastruktury krytycznej lub jej zastąpienie.

Zgodnie z ustawą o zarządzaniu kryzysowym (art. 3 pkt. 3) ochrona infrastruktury krytycznej obejmuje „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie" (Dz.U. 2007, nr 89, poz. 590 z późn. zm.).

Według opinii Rządowego Centrum Bezpieczeństwa, ochrona infrastruktury krytycznej to proces związany ze znaczną liczbą obszarów zadaniowych i kompetencji oraz angażujący wiele zainteresowanych stron. Proces ten obejmuje wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej, zakłada również stopniowe dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie. Zadania w tym zakresie obejmują zapobieganie zagrożeniom i ograniczanie ich skutków, zmniejszanie podatności infrastruktury krytycznej na zagrożenia oraz szybkie przywrócenie jej prawidłowego funkcjonowania na wypadek wszelkich zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Ochronę infrastruktury krytycznej można prowadzić, przy użyciu różnych metod, do których można zaliczyć (Narodowy Program Ochrony Infrastruktury Krytycznej, 2013), (Ochrona infrastruktury transportowej, 2012, s. 65):

1. Ochronę fizyczną – czyli zespół przedsięwzięć minimalizujących ryzyko zakłócenia funkcjonowania infrastruktury krytycznej przez osoby, które znalazły się na terenie infrastruktury krytycznej w sposób nieautoryzowany. Składają się na nią ochrona osób, rozumiana jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej oraz ochrona mienia, czyli działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony.

2. Ochronę techniczną – czyli zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania infrastruktury krytycznej, związanego z technicznymi aspektami budowy i eksploatacji obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, w tym również techniczne środki ochrony. Oznacza to, że ochrona techniczna infrastruktury krytycznej obejmuje sprawy związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi normami (np. budowlanymi) oraz innymi przepisami (np. przeciwpożarowymi), co ma zagwarantować bezpieczne użytkowanie infrastruktury krytycznej oraz zabezpieczenie techniczne obiektu, czyli wykorzystanie w ochronie obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych itp. środków.

3. Ochronę osobową – czyli zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które poprzez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu. Ochronę tę należy zatem powiązać z pracownikami oraz innymi osobami czasowo przebywającymi w obrębie infrastruktury krytycznej (usługodawcy, dostawcy, goście).

4. Ochronę teleinformatyczną – czyli zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania infrastruktury krytycznej, związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych. Oznacza to również ochronę przed cyberprzestępstwami i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom.

5. Ochronę prawną – czyli zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością innych podmiotów gospodarczych, państwowych lub prywatnych, których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług infrastruktury krytycznej. Oznacza zastosowanie narzędzi prawnych niedopuszczających, poprzez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów do na przykład wrogiego przejęcia, fuzji, czy też sprzedaży niektórych elementów infrastruktury, której efektem mogą być zakłócenia w jej funkcjonowaniu.

Zatem, ochrona obiektu obejmuje zespół przedsięwzięć organizacyjnych, taktycznych, technicznych i fizycznych zapobiegających przestępstwom i wykroczeniom przeciwko niemu, a także przeciwdziałających powstaniu szkody wynikającej z tych zdarzeń oraz niedopuszczających do wstępu osób nieuprawnionych na teren danego obiektu, co zostało zawarte w Ustawie o ochronie osób i mienia z 22 sierpnia 1997r.

Wymienione elementy ochrony infrastruktury krytycznej są ze sobą wzajemnie powiązane i tylko stosowane łącznie mogą dać zadowalające rezultaty. Aby ochrona infrastruktury krytycznej mogła być skuteczna, powinna być realizowana na każdym poziomie i stanowić wspólny wysiłek zarówno administracji rządowej, samorządowej oraz operatorów i właścicieli infrastruktury krytycznej, co pozwoli na zwiększenie poziomu bezpieczeństwa i niezawodności infrastruktury krytycznej.

Biorąc pod uwagę definicję ochrony infrastruktury krytycznej, należy ją rozumieć jako proces składający się z kilku podstawowych elementów (Szewczyk, Pyznar, 2009, s. 14):

1. identyfikacji infrastruktury krytycznej w ramach systemu, określenia sieci powiązań oraz roli w danym systemie,
2. oceny ryzyka zakłócenia działania lub zniszczenia infrastruktury krytycznej,
3. rozwoju i wdrażania programów ochrony infrastruktury krytycznej, w tym planów ochrony, jak i planów odtwarzania,
4. doskonalenia rozumianego jako pomiar postępów na drodze do osiągnięcia celu i wprowadzania, w wyniku tego pomiaru, modyfikacji i korekt.

Nie mniej ważne niż ochrona infrastruktury krytycznej jest jej ewentualne odtwarzanie, a w związku z tym plany odtwarzania, należy rozumieć jako odtwarzanie nie tyle samej infrastruktury krytycznej, co funkcji przez nią realizowanych.

Podsumowanie

Zagrożenie terrorystyczne w ostatnich dziesięcioleciach przybrało na sile i stało się jednym z najpowszechniejszych zagrożeń współczesnego świata. Zamach terrorystyczny nie jest celem samym w sobie. Stanowi element przemyślanej i konsekwentnie realizowanej strategii – strategii walki biednych z bogatymi. Podstawowym zadaniem ataków terrorystycznych jest naruszenie wewnętrznej równowagi politycznej lub gospodarczej państwa, by w konsekwencji uzyskać odpowiednie warunki do wprowadzenia w życie swoich żądań.

Infrastruktura krytyczna, jako element systemu utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności, którego zakłócenie lub zniszczenie miałoby istotny wpływ na państwo w wyniku utraty tych funkcji, jest szczególnie podatna na zagrożenia ze strony ugrupowań terrorystycznych. Ich identyfikacja jest poza zakresem kompetencji i możliwości operatorów oraz gospodarzy systemów IK. W tym obszarze muszą oni polegać na informacjach otrzymanych w ramach współpracy ze służbami ochrony państwa, w szczególności wykorzystując mechanizm opisany w art. 12a ustawy o zarządzaniu kryzysowym (Rządowe Centrum Bezpieczeństwa, 2013).

Zagrożenia wybrane do analizy pod względem ochrony powinny dotyczyć konkretnego obiektu, urządzenia, instalacji lub systemu IK i są podstawą do opracowania scenariuszy rozwoju niekorzystnych zdarzeń. Scenariusze w kontekście ochrony IK mają wskazać obszary niepewności i czynniki, które wpływają na decyzje dotyczące systemu ochrony IK, które muszą zostać podjęte teraz i w przyszłości.

Bibliografia

Chalk, P. (2004). *Hitting America' Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against U.S. Agricultural and Food Industry*. Santa Monica: RAND National Defense Research Institute.

Cichoń, B. (2007). *System zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego.* W: B. Kosowski, A. Włodarski (red.). *I Międzynarodowa konferencja naukowa. Wyzwania bezpieczeństwa cywil-*

nego XXI wieku – inżynieria działań w obszarach nauki, badań i praktyki (s. 28). Warszawa: Szkoła Główna Służby Pożarniczej.

Dyrektywa Rady UE 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.

Encyklopedia terroryzmu (2004), Warszawa: Bellona–Muza S.A.

Gunaratna, R. (1987). *War and Peace in Sri Lanka*. Sri Lanka: Institute of Fundamental Studies.

Hoffman, B. (2001). *Oblicza terroryzmu*. Warszawa: Bertelsman Media sp. z o.o.

Karasik, T. (2002). *Toxic Warfare*. Santa Monica: RAND National Defense Research Institute.

Lidwa, W., Krzeszowski, W., Więcek, W., Kamiński, P. (2012). *Ochrona infrastruktury krytycznej*, Warszawa: Akademia Obrony Narodowej.

Materiały wyjściowe do Koncepcji Przestrzennego Zagospodarowania Kraju na lata 2008-2033, P3/1061/08 z 9 maja 2008 r. Sztab Generalny WP, Zarząd Planowania Operacyjnego - P3.

Narayan Swamy, M.R. (1994). *Tigers of Lanka, From Boys to Guerrillas*, Delhi: Konark Publishers.

Narodowy Program Ochrony Infrastruktury Krytycznej (2013). Rządowe Centrum Bezpieczeństwa. Pobrano 23 maja 2013 z: http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf.

O'Balance, E. (1989). *The Cyanide War: Tamil Insurrection in Sri Lanka 1973-88,* Washington: Brassey's U.K.

Ochrona krytycznej infrastruktury transportowej. Zeszyt Problemowy TWO Nr 1/2012, 65.

Pietrzak, A. (2002). Światowy terroryzm. *Magazyn globalizacji i integracji europejskiej nr 6/listopad 2002r. – Glob@lizator.* Niezależna Inicjatywa Naukowa PARADYGMAT.

Syta, J. (2009). Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego. W: T. Jemioła, J. Kisielnicki i K. Rajchel (Red.) *Cyberterroryzm - nowe wyzwania XXI wieku* (s. 696-703). Szczytno: Wyższa Szkoła Policji.

Szewczyk, T., Pyznar M. (2009). Ochrona infrastruktury krytycznej – polskie podejście, *Terroryzm 1*, 14.

Newsweek.pl. (2010). *Terroryści zaatakowali elektrownię na Kaukazie*. Pobrano 23 maja 2013 z: http://swiat.newsweek.pl/terrorysci-zaatakowali-elektrownie-na-kaukazie,62191,1,1.html.

Ustawa z dnia 22 sierpnia 1997 roku *o ochronie osób i mienia* (Dz. U. 1997, nr 114, poz. 740), tekst jednolity z dnia 26 lipca 2005 roku, (Dz. U. 2005, nr 45, poz. 1221).

Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. 2007, nr 89, poz. 590, z późn. zm.).

Walczak, W. (2009). Zarządzanie kryzysowe – rola i zadania organów administracji państwowej. *Przedsiębiorczość i zarządzanie*, *X(8),* 93–109.

Weimann, G. (2004). Cyberterrorism, how Real is the threat? *US Institute of Peace, Special Report*. Pobrano 20 września 2012, z www.usip.org.

Wójtowicz, W. (2006). *Bezpieczeństwo infrastruktury krytycznej,* Warszawa: MON.

Zięba, R. (1999). *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje, struktury, funkcjonowanie*. Warszawa: WN Scholar.

Żuber, M. (2006). *Agroterroryzm – zagrożenie sektora rolniczego.* W: M. Żuber (red.), *Katastrofy naturalne i cywilizacyjne. Terroryzm współczesny. Aspekty polityczne, społeczne i ekonomiczne* (s. 155-161). Wrocław: WSOWL.

Żuber, M. (2003). Bioterroryzm – refleksja historyczno-filozoficzna. W: K. Pająk, A. Zduniak (red.). *Edukacyjne zagrożenia początku XXI wieku* (s. 205-211). Poznań–Warszawa: Wydaw. ELIPSA.

Żuber, M., Sawczak, S. (2004). Zagrożenie bronią masowego rażenia w aspekcie działań terrorystycznych. W: D. Kozerawski (red.). *Udział jednostek Wojska Polskiego w międzynarodowych operacjach pokojowych w latach 1973-2003: wybrane problemy* (s. 54-64). Warszawa: Akademia Obrony Narodowej.

State critical infrastructure as an area of potential terrorist acts

Summary: The term "critical infrastructure" describes those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic well-being of the nation or affect ability to conduct national defence and ensure national security.
In the article the author presents terrorist threats to the objects of critical infrastructure, which include assassinations, kidnappings, hijackings, bomb scares and bombings, cyber attacks (computer-based), and the use of chemical, biological, nuclear and radiological weapons.
High-risk targets for acts of terrorism include military and civilian government facilities, international airports, large cities, and high-profile landmarks. Terrorists might also target large public gatherings, water and food supplies, utilities and corporate centers. Furthermore, terrorists are capable of spreading fear by sending explosives or chemical and biological agents through the mail.
The paper describes examples of the terrorist attacks on the elements of critical infrastructure in the history of modern international terrorism. In the end of the article the author presents methods of protecting the critical infrastructure against threats, especially against terrorists attacks.

Keywords: national security, critical infrastructure, international terrorism, terrorists attack.