Cytowanie/quotation:
D. Kaźmierczak , *Siły zbrojne RP w systemie przeciwdziałania terroryzmowi,* [w:] red. J. Kuck, Bezpieczeństwo w procesach globalizacji – dziś i jutro, UKiP J&D Gębka Gliwice, 2013, ISBN978-83-87296-49-0 str./p. 49 - 61

Danuta KAŹMIERCZAK
Wyższa Szkoła Zarządzania Marketingowego i Języków Obcych w Katowicach

SIŁY ZBROJNE RP W SYSTEMIE PRZECIWDZIAŁANIA TERRORYZMOWI

Streszczenie. Postęp naukowo-techniczny przynoszący radykalne zmiany w funkcjonowaniu społeczeństw XXI wieku, stawia je wobec nowych wyzwań ale też i zagrożeń. Dla bezpieczeństwa narodowego i międzynarodowego priorytetem stało się zwalczanie terroryzmu międzynarodowego, który ze względu na swą dynamikę i zdolności adaptacyjne do zmieniających się strategii obronnych państw stanowi jedno z trudniejszych celów. Omówienie charakteru współczesnego terroryzmu i określenie roli sił zbrojnych nakreśla pozycję Polski i stan polskiej obronności w kontekście zagrożeń bezpieczeństwa narodowego i międzynarodowego.

Abstract. Scientific and technological advances bringing about radical changes in functioning of societies in the XXIst century crate new challenges and threats to face. The priority for national and international safety is fighting terrorism, which is a goal hard to achieve because of the dynamic nature of terrorism and its adaptability to changing safety strategies of countries. Analyzing the character of terrorism and defining the role of the Polish Armed Forces identifies the position of Poland and condition of its defense capabilities in terms of threats to national and international safety.

„Partacze, którzy zniszczyli część nowojorskiego Word Trade Center, mogliby zmieść z powierzchni ziemi Wall Street, gdyby ktoś bardziej rozgarnięty wyposażył ich w taktyczną broń jądrową”[1].

To komentarz wydarzeń z 11 września 2001 r. z lekką nutą czarnego humoru, ale przez to skutecznie uruchamiający wyobraźnię o realnych zagrożeniach bezpieczeństwa XXI w. Rozwój cywilizacyjny i technologiczny wymusił przewartościowanie i zdefiniowanie na nowo pojęcia bezpieczeństwa. Bezpieczeństwo jako **gwarancja nienaruszalnego przetrwania danego podmiotu oraz swobody jego rozwoju** [2], wymaga ujęcia nie tylko w kategoriach militarnych, ale także ekonomicznych, kulturowych, moralnych, społecznych i edukacyjnych. Główne zjawiska lub **megatrendy**[3] kształtujące dzisiejszą rzeczywistość wraz ze wszystkimi konsekwencjami to między innymi :

- transformacja społeczeństwa prowadząca do podziału świata na trzy rywalizujące i odmienne cywilizacje, gdzie pierwsza ciągle jest pod znakiem rewolucji agrarnej, druga - rewolucji przemysłowej i trzecia - rewolucji informacyjnej zajmując dominującą pozycje dzięki nowym sposobom zdobywania i wykorzystywania wiedzy;
- globalizacja rozumiana jako budowanie sieci światowych powiązań politycznych, ekonomicznych, kulturowych i militarnych, która zwiększa znaczenie problemów gospodarczych poprzez alokację produkcji. Globalizacja to również płynność granic potęgująca masowe emigracje przynoszące ze sobą nienawiść, własne ruchy polityczne i terrorystyczne organizacje;

[1] Toffler A., Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s. 224.
[2] *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa, s. 15.
[3] Ibidem, s. 88.

- uniformizacja stylu życia i nacjonalizacja zmuszająca do życia w trzech kulturach jednocześnie: globalnej, narodowej i regionalnej;
- postęp w dziedzinie biologii dający nowe możliwości w zakresie budowania środków masowej „śmiercionośności”[4]: chemicznych, biologicznych i atomowych;
- wojna dwóch przeciwstawnych kulturowo światów islamskiego z zachodnim przy pomocy terroru. W 1998 roku Osama bin Laden na łamach dziennika Al Quds Al.-‘Arabi wypowiedział wojnę Stanom Zjednoczonym i zobligował wszystkich muzułmanów, żeby zabijali każdego Amerykanina, zarówno osoby cywilne jaki i członków armii USA po to, by osłabić to państwo w takim stopniu, aby nie było w stanie zagrozić żadnemu z państw muzułmańskich[5].

Zmiany te niosą ze sobą nowe zagrożenia i nie eliminują dawnych. Według Lema wprowadzają świat w „…fazę wielkiego strachu….”, jak tłumaczy H. Kissinger .. bo istota współczesnego zagrożenia polega na tym, że jest ono niespodziewane, że uderza w cywilów, że nie wiadomo jak nad nim zapanować.[6]

Tak zarysowana sytuacja świata XXI w prowadzi do podjęcia analizy terroryzmu, jako jednego z głównych niebezpieczeństw. To właśnie strach jest jego znaczącym składnikiem. W tradycyjnym rozumieniu terroryzm jest to przemyślane użycie przemocy lub zagrożenia w celu wywołania strachu; przemyślane wymuszanie lub zastraszania rządów lub społeczeństw w celach nacisku politycznego, religijnego lub ideologicznego[7]. Historycznie terroryzm jako działania nieregularne były podejmowane podczas II wojny światowej w walce o wyzwolenie spod okupacji hitlerowskiej, przez Żydów w czasie budowania współczesnego państwa izraelskiego, przy czym w tej konfrontacji jedna ze stron była strukturą państwa.

Wojskowa definicja określa terroryzm jako działaniem dywersyjnym (sabotażem) na szczeblu strategicznym, realizowanym głównie taktycznymi sposobami, środkami i metodami w ramach działań precyzyjnych. Natomiast obrona przed nim ma wymiar działań antydywersyjnych[8]. Różni się od typowego wojskowego sabotażu tym, ze wymierzony jest w państwo: na osłabienie jego systemu bezpieczeństwa i destrukcję władzy. Wojskowe działania antyterrorystyczne polegają na: ochronie ważnych obiektów i stanowisk dowodzenia, osłonie strefy tyłowej - infrastruktury logistycznej, składów materiałów, likwidacji skutków ataków i zwalczania grup terrorystycznych.

Rozbudowaną definicje terroru podaje T. Jordan. Terror to polityka czy strategia stosowana przez wielu aktorów sceny politycznej. …na atak terrorystyczny składają się następujące elementy: premedytacja, aspekt polityczny, aspekt psychologiczny i przemoc[9]. Akt terrorystyczny jest częścią celowej z góry zaplanowanej strategii stworzonej na potrzeby agendy politycznej, kierującej się motywami religijnymi, etnicznymi, narodowymi. Skutek psychologiczny działań ma być niewspółmiernie większy od rzeczywistych skutków materialnych, chociaż stosowana przemoc ma również wymiar materialny. T. Jordan podkreśla również, ze terroryzm może mieć sprawców państwowych i niepaństwowych, że nie można porównywać go z partyzanckimi działaniami wojennymi, gdyż te pomimo tego, że zawierają elementy terroryzmu zdecydowanie więcej jest w nich czynników pokrewnych wojnie, np. geograficznie określone granice. Terrorystą może być bojownik o wolność i żołnierz państwa narodowego. Terroryzm jest strategią, czy też polityką[10], która może być realizowana przez wiele autonomicznych jednostek. Czynniki decydujące o sile i skuteczności tej strategii to :

- dostępność do środków masowego rażenia;
- swoboda poruszania się w każdym państwie zachodniej demokracji;
- bezbronność i wrażliwość na atak obiektów infrastruktury krytycznej[11] i miejsc gromadzenia się osób cywilnych (miękkich celów);

---

[4] Toffler A., Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s.

[5] Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2010, s.31.

[6] *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa, s.8.

[7] Ibidem, s.103.

[8] Ibidem, s.104.

[9] Jordan T., *Hakerstwo*, PWN, Warszawa 2011, s.106.

[10] Ibidem, s.107.

[11] **Infrastruktura krytyczna** - systemy i dobra fizyczne i wirtualne, żywotne dla państwa, których zniszczenie lub destrukcja mogłyby osłabić bezpieczeństwo gospodarki narodowej, narodowej służby zdrowia i opieki społecznej lub innych dziedzin. *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa, s 99.

- powszechna dostępność systemów komputerowych;
- anonimowość i bezkarność sprawców;
- niskie koszty przeprowadzenia operacji;
- medialność wzmacniająca ich psychologiczne oddziaływanie na społeczeństwo.

Ponadto, współczesny terroryzm międzynarodowy charakteryzuje się dużą dynamiką zmiennością form i stosowanych narzędzi i co najistotniejsze, brakiem podmiotowości prawnej, przez co walka z nim staje się wręcz niemożliwa. Cytując A. i H. Tofflerów, jak można wziąć masowy odwet na terrorystycznym gangu albo na zbrojnych przywódcach narkokartelu, albo na małym państwie, pozbawionym rozwiniętej infrastruktury i centrum dowodzenia, które można by zaatakować[12] Jak rozprawić się z grupą infoterrorystów lub jednym infoterrorystą, który wdziera się do sieci, uszkadza infrastrukturę krytyczną państwa leżącego na drugim końcu świata?

Jak zauważa K. Liedel, [13] brak jednoznacznej definicji prawnej terroryzmu skutkuje brakiem mechanizmów umożliwiających pociągniecie do odpowiedzialności ugrupowania terrorystycznego jako samodzielnego aktora stosunków międzynarodowych. Terroryzm traktowany jest jako działanie zbiorowe formalnych organizacji, jednak współcześnie obserwuje się zmianę form tych działań i wzmożenie ataków terrorystycznych dokonywanych przez pojedyncze jednostki. Wyróżnia się dwa typy zamachów indywidualnych: Solo Terrorism i Lone Wolf Terrorism[14] Zamachy typu Solo Terrorism dokonywane są przez indywidualne osoby szukające kontaktu z organizacjami terrorystycznymi, ale nie są ich członkami. Solo terrorysta planuje i dokonuje ataków po wcześniejszym przeszkoleniu w obozach treningowych, jednak działa samodzielnie i bez powiązań z grupą. Przykłady ataków to: próba zamachu samobójczego na samolot lecący z Detroit do USA – 25 grudnia 2009 r. Umar Farouk Abdulmutallab był w kontakcie z Al. Qaida Arabian Peninsula, przeszkolony w obozie treningowym w Jemenie, działał według planu przygotowanego przez organizację terrorystyczną. Abdulhakim Mujahid Muhammad – sprawca zamachu z użyciem broni palnej w biurze rekrutacji w Little Rock w USA w 2009 roku działał z własnej inicjatywy i nie otrzymał wsparcia od organizacji, ale być może został przeszkolony podczas studiów w Jemenie.

Taktyka Lone Wolf stosowana jest przez indywidualnych zamachowców którzy nie są w żaden sposób powiązani z organizacjami terrorystycznymi. Inspirację i wiedzę na temat metod czerpią z zasobów internetowych. Przykładem może być zamach w amerykańskiej bazie wojskowej w Fort Hood w USA - 5 listopada 2010 roku przeprowadzony przez Nidal Hassana. Prawdopodobnie nie miał kontaktów z innymi terrorystami. Arid Uka przeprowadził samodzielny atak na amerykańskich żołnierzy na lotnisku we Frankfurcie 2 marca 2011 roku. Podkreślmy jeszcze raz, że walka z terroryzmem to walka z metodą działania i nie można dopuścić do tego, aby państwo zastosowało te same metody - a więc przekroczyło tą cienką granicę norm i zasad, w których obronie występuje. Nowoczesne technologie, osiągnięcia naukowe sprzyjają rozwojowi i specjalizacji terroryzmu: bioterroryzm wykorzystujący broń bakteriologiczną, terror jądrowy - broń jądrową, czy też cyberterror – Internet.

Bioterroryzm

Uważany za najbardziej podstępny i niebezpieczny rodzaj terroryzmu, utożsamiany jest z bezprawnym, nielegalnym użyciem **czynników biologicznych** wobec ludzi, z zamiarem wymuszenia jakiegoś działania lub zastraszania rządu, ludności cywilnej, lub jakiejkolwiek jej części, dla osiągnięcia celów osobistych, politycznych, społecznych lub religijnych[15]

Biologiczny czynnik jest ładunkiem bojowym mogącym wywoływać ostre i przewlekłe choroby, doprowadzając do epidemii u ludzi i zwierząt. Środki wykorzystywane jako broń biologiczna to:

- **bakterie** - małe, wolnożyjące organizmy, hodowane na stałej lub ciekłej pożywce. Choroby wywołane bakteriami są wrażliwe na określoną terapię antybiotykową;

[12] Toffler A.,Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s.121.
[13] Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2010, s. 39.
[14] Liedel K., P. Piasecka, T.R. Aleksandrowicz, *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie*, Difin, Warszawa 2011, s.44.
[15] Kępka P., Bioterroryzm. Polska wobec użycia broni biologicznej, Difin, Warszawa 2009, s.23.

- **wirusy** - uzależnione są od komórek gospodarza, które zakażają. Choroby wywołane nie są wrażliwe na antybiotyki, są zwalczane lekami antywirusowymi;
- **riketsje** - to organizmy pośrednie między bakteriami i wirusami. Są wrażliwe na antybiotykoterapię ale rozmnażają się tylko w organizmach żywych;
- **chlamydie** - to pasożyty rozmnażające się w komórkach żywych, wrażliwe na antybiotyki
- **grzyby** - prymitywne rośliny;
- **toksyny** - toksyczne substancje chemiczne pochodzenia roślinnego, zwierzęcego lub chemicznego. Mogą być zwalczane za pomocą przeciwciał lub środków farmakologicznych.

Podział broni biologicznej zaproponowany przez specjalistów z Uniwersytetu w Waszyngtonie wyróżnia:

- **drobnoustroje**, które zakażają „gospodarza", wywołują choroby, które go niszczą;
- **bioaktywne substancje** pochodzenia biologicznego - produkty metabolizmu drobnoustrojów, które zabijają „gospodarza";
- **nowo-wytworzone** substancje biologiczno - mimetyczne - wyprodukowane substancje o działaniu biologicznym, np. gazy działające na układ nerwowy.

Natomiast Ośrodek Kontroli Chorób (CDC) dzieli niebezpieczne czynniki biologiczne na 3 kategorie:

- **kategoria A** - patogeny najwyższego priorytetu o dużej łatwości rozprzestrzeniania się wywołujące wysoką śmiertelność;
- **kategoria B** - to patogeny o umiarkowanie łatwym rozsiewaniu wymagające wzmożonego nadzoru;
- **kategoria C** - to nowe patogeny, które mogą być przedmiotem manipulacji genetycznej, łatwo dostępne i łatwo rozprzestrzeniające się, powodują wysoką zachorowalność i śmiertelność.

Bioterroryzm jest podstępny i niebezpieczny. Broń biologiczna to broń masowego rażenia (BMR), składa się z czynnika aktywnego, (np. bakterii, wirusów), pojemnika, w którym ten czynnik się znajduje oraz środka przenoszenia i dyspersji. Podczas ataku terrorystycznego drobnoustroje mogą być łatwo rozprzestrzeniane przez wiatr po ich rozpyleniu (np. z samolotów), zarażone wcześniej insekty; pchły, kleszcze, muchy. W stanie nieaktywnym broń biologiczna jest trudna do rozpoznania więc łatwa do ukrycia i transportu. Niewielka ilość wystarczy by osiągnąć zamierzony efekt. Jest łatwa do rozpylenia. Kilkudniowy okres utajnienia pozwala zamachowcom bezpiecznie oddalić się z miejsca zdarzenia. Jest trudna do wykrycia u bezobjawowych nosicieli. Szybko rozprzestrzenienia się z powodu swobodnego przemieszczania się dużych grup zakażonych ludzi na znaczne odległości. Sygnały użycia broni biologicznej to:

- pojawienie się nietypowych objawów chorobowych w szczególności na skórze, błonach śluzowych;
- uszkodzenia układu nerwowego, oddechowego, pokarmowego;
- nagły wzrost zachorowalności lub umieralności z powodu nieznanych chorób;
- nieskuteczność leczenia w rutynowej terapii;
- pojedynczy przypadek choroby spowodowany egzotycznym czynnikiem u osoby nie opuszczającej kraju;
- nietypowe dla danego czynnika zakaźnego objawów chorobowych;
- jednoczesne wystąpienie zachorowań na podobne choroby w ogniskach nie połączonych terytorialnie w kraju lub zagranicą;
- nietypowy sposób transmisji chorób (aerozol, woda, żywność).

Atak terrorystyczny na danym terytorium może mieć skutki w odległym kraju w postaci:

- błyskawicznego rozprzestrzeniania się drobnoustrojów;
- psychozy strachu;
- braku skuteczności lekarstw;
- trudności zdiagnozowania przyczyny;
- mylące objawy.

Od zakończenia okresu „zimnej wojny" odnotowano szereg przykładów użycia broni biologicznej. W roku 1884 w Dallas 750 osób jednocześnie zachorowało po spożyciu posiłków w czterech restauracjach w Dallas – przyczyną było zatrucie bakterią Salmonella, którą zakażono szklanki i pojemniki. Atak ten przeprowadzony został przez członków sekty Bhagwan Shree Rajneesh. W 1986 terroryści iraccy wysyłają zarodniki wąglika i jadu kiełbasianego Judith Miller, współautorce książki „Zarodniki. Biologiczna broń i amerykańska tajna wojna." W 1990 roku Członkowie sekty Najwyższa Prawda rozsiewają jad kiełbasiany

wokół budynku japońskiego parlamentu. W 2001 roku po ataku na WTC pierwszą śmiertelną ofiarą użycia broni biologicznej był Bob Stevens fotoreporter czasopisma „The Sun" – odosobniony przypadek zapalenia opon mózgowych o ciężkim przebiegu. W ciągu kolejnych dni odnotowano siedem kolejnych przypadków zakażenia wąglikiem i ślady zarodników tej bakterii na redakcyjnych komputerach. W październiku 2001 na Kapitolu otwarcie listu do lidera większości demokratycznej Toma Daschle spowodowało zakażenie 28 osób. 14 dni później kolejny list otworzyła jego asystentka co spowodowało kolejne zakażenia wąglikiem. Oba listy wysłane zostały z dwóch różnych miejsc z Trenton i Brentwood.

Podsumowując, akty terroryzmu z użyciem wąglika spowodowały 5 ofiar śmiertelnych w USA i psychozę strachu we wszystkich krajach cywilizacji zachodniej. W Polsce żadne z odnotowanych podejrzanych zdarzeń nie było atakiem terrorystycznym.

Terror jądrowy

W epoce trzeciej fali o sile stanowi dostęp do informacji i „know-how" – jest on wolny i demokratyczny. Możemy bez większego wysiłku dotrzeć do instrukcji… jak skonstruować bombę Manchester Manual - publikacji na potrzeby islamskich ekstermistów[16], zasobów banku danych Międzynarodowej Agencji Energii Atomowej, International Nuclear Information System, podziemnego podręcznika Basement Nukes.

Carl Builder, specjalista w korporacji RAND twierdzi, że „tak jak proch strzelniczy, broń nuklearna będzie się rozprzestrzeniać… Poszedłbym jeszcze dalej i powiedział, ze choć nie za mojego życia, lecz w przewidywalnej przyszłości, broń jądrowa stanie się osiągalna dla poszczególnych jednostek. Jednostka będzie mogła skonstruować własną broń atomową, korzystając z materiałów znajdujących się w handlu[17]. Tymi jednostkami mogą być rodziny mafijne, grupki ortodoksyjnych trockistów, somalijscy kondotierzy, serbscy naziści, prywatne armie na usługach biznesmenów, mafiopodobnne grupy przedsiębiorców, czy działający w pojedynkę szaleńcy.

Przykładem działającego w pojedynkę szaleńca, czy ujmując inaczej – pojedynczej zradykalizowanej jednostki jest Anders Breivik, sprawca zamachów w Oslo i na wyspie Utoya, w których łącznie zginęło 77 osób. Sam określa siebie jako obrońcę wartości europejskich przed islamizacją. Jako materiału wybuchowego Breivik nie użył prochu strzelniczego ani broni atomowej, ale saletrę amonową - powszechnie dostępny środek do pielęgnacji roślin. Niemniej jednak, Thomas Schelling twierdzi, że w roku 1999 nie będziemy zdolni lepiej kontrolować broni nuklearnej, niż dziś kontrolujemy heroinę i pornografię – atrakcje sobotnich wieczorów.[18]

Proliferacja broni jądrowej stanowi już realny problem. Korea Północna dostarczyła fabryczną technologię budowy rakiet krajom Środkowego Wschodu. Charls Homer, szef US Air Force Space Command ostrzega, że technologia wykorzystywana przy konstrukcji SS-25 (wielkie przewoźne rakiety radzieckie) w przeciągu ośmiu do dziesięciu lat… będzie dostepna tym wszystkim, którzy bardzo chcą ją nabyć[19].

Potencjalni klienci takiej czy innej bomby mogą szantażować całe narody bo jako przeciwnik nie stanowią określonego społeczeństwa. Więc jak i kogo powstrzymać, odstraszyć groźbą użycia broni jądrowej?

Cyberterroryzm

Jutro terrorysta może wyrządzić większe szkody posługując się klawiaturą komputera niż bombą.[20] T. Jordan daje przykład terrorystów 11 września, którzy dobrze wykorzystali sieć – dwóch z nich meldując się w hotelu zażądało 24-ro godzinnego dostępu do Internetu. Wykorzystanie Internetu do komunikacji nawet w celu zorganizowania ataku terrorystycznego nie jest jeszcze atakiem. Jakie zatem działania w cyberprzestrzeni są atakiem terrorystycznym – cyberatakiem? Terroryści idąc śladami hakerów mogą włamywać się do rządowych i prywatnych systemów komputerowych paraliżując wojskowe, finansowe i usługowe sektory gospodarki, narodowe systemy obrony i systemy kontroli ruchu lotniczego. Innymi słowy cyberterroryzm jest to groźba lub bezprawny atak wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom

[16] Liedel K., Piasecka P., Aleksandrowicz T.R., *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie*, Difin, Warszawa 2011, s.27.
[17] Toffler A.,Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s. 225.
[18] Ibidem, s.224.
[19] Ibidem, s.118.
[20] Ibidem, s. 171.

teleinformatycznym w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów[21].

W 1997 roku Narodowa Agencja Bezpieczeństwa USA przeprowadziała symulacje cyberataku na systemy Pentagonu. Zamówieni krakerzy wykorzystując jedynie dostępne w Internecie narzędzia zdobyli dostęp do tuzinów newralgicznych systemów. Pomimo braku potwierdzonych aktów cyberterroryzmu potencjalne zagrożenie staje się coraz bardziej realne wraz z coraz większym uzależnieniem krajów od technologii informacyjnej. Cyberterroryzm ma przed sobą możliwości, ale nie stoi za nim dzisiejsza praktyka w przeciwieństwie do kilku przykładów cyberwojny, wielu – hackerstwa, czy cyberprzestępczości. Cyberwojna to „krakopodobny" atak na infrastrukturę sieciową państwa narodowego, przeprowadzony przez inne państwo narodowe[22]. Hacki to materialne praktyki, które wywołują zamiany w technologiach komputerowych i sieciowych, to cracki są hackami, które zajmują się niedozwolonym przekazaniem kontroli nad komputerami i sieciami. Cracki nie wytwarzają niczego nowego w infrastrukturze rzeczywistości wirtualnej[23].

Cyberprzestępczość wykorzystuje techniki hakerskie, ale w służbie korzyści osobistych. Rodzaj korzyści nie różni się od innych przestępstw natury finansowej, informacyjnej, seksualnej[24]. Cyberprzestrzeń rozumiana jest jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jako cyberprzestrzeń państwa przyjmuje się przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa.

Rola Sił Zbrojnych RP w systemie przeciwdziałania terroryzmowi

Zwalczanie terroryzmu na płaszczyźnie militarnej to newralgiczny obszar działania państwa. Organy i służby odpowiedzialne za bezpieczeństwo narodowe to Policja, Straż Graniczna, Żandarmeria Wojskowa, Służby Więzienne, Biura Ochrony Rządu, służby rozpoznania SZ RP, organy celne i skarbowe. Zgodnie z art. 3 Ustawy z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej Siły Zbrojne RP stoją na straży suwerenności i niepodległości narodu polskiego oraz jego bezpieczeństwa i pokoju. Mogą one też brać udział w zwalczaniu klęsk żywiołowych, działaniach antyterrorystycznych[25]. Ważne, by działania wymienionych podmiotów w podejmowanych akcjach antyterrorystycznych były skoordynowane.

Głównym organem organizującym współpracę wymienionych służb jest Kolegium do Spraw Służb Specjalnych. Prace Kolegium mają charakter normatywny i opiniotwórczy co do kierunku i planu działania służb Specjalnych. W jego skład wchodzą: minister właściwy do spraw zagranicznych, minister obrony narodowej, minister właściwy do spraw wewnętrznych, szef Biura Bezpieczeństwa Narodowego, minister właściwy do spraw finansów z przewodniczącym Prezesem RM. Międzyresortowy Zespół ds. Przeciwdziałania Zagrożeniom Terrorystycznym (w podstawowym składzie: Minister Spraw Wewnętrznych i Administracji - przewodniczący, Minister Finansów, Minister Obrony Narodowej, Minister Spraw Zagranicznych) ma za zadanie:
- monitorować zagrożenia o charakterze terrorystycznym i przedstawiać opinie Radzie Ministrów;
- opracować standardy i procedury w zakresie zwalczania terroryzmu;
- występować z wnioskami do właściwych ministrów w celu podjęcia działań legislacyjnych;
- współpracować z innymi państwami;
- organizować szkolenia i konferencje.

Prace Zespołu wspierane są przez Grupę Ekspercką, która sporządza opinie i rekomendacje bazując na wymianie informacji i doświadczeń. Natomiast Centrum Antyterrorystyczne (CAT) powołane Zarządzeniem nr 102 Prezesa Rady Ministrów z dnia 17 września 2008 roku, jest pomostem między poziomem strategicznym (Międzyresortowy Zespół ds. Przeciwdziałania Zagrożeniom Terrorystycznym i Grupa Ekspercka) a poziomem wykonawczym, na którym zadania realizują służby. Zadania CAT to głównie przetwarzanie informacji o charakterze operacyjnym, dystrybucji tych informacji na potrzeby wewnętrzne i społeczeństwa. CAT ma również koordynować współpracę na poziomie międzynarodowym.

---

[21] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia*, Warszawa, marzec 2009, s. 4. http://www.cert.gov.pl/portal/cer/30/Rzadowy_program_ochrony_cyberprzestrzeni. html (20.03.2013)
[22] Jordan T., *Hakerstwo*, PWN, Warszawa 2011, s 101.
[23] Ibidem, s. 43.
[24] Ibidem, s. 116.
[25] Tekst jednolity DzUz 2004 nr 241, poz. 2416 z późn. zm.

W całym systemie przeciwdziałania terroryzmowi wyróżnia się następujące obszary zadaniowe: **rozpoznanie, profilaktyka, zwalczanie, minimalizacja i likwidacja skutków** ataków terrorystycznych. Siły Zbrojne RP a rozpoznanie zagrożeń terrorystycznych. Walka z terroryzmem to również zadanie Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego. SKW ma za zadanie między innymi wykrywanie popełnianych przez żołnierzy i pracowników jednostek organizacyjnych MON przestępstw przeciwko pokojowi, ludzkości, przestępstw wojennych, związanych działalnością terrorystyczną i innych godzących w bezpieczeństwo Sił Zbrojnych i podejmowanie działań określonych umowami międzynarodowymi, które Polska ratyfikowała.

SWW zaś realizuje następujące zadania ukierunkowane na zwalczanie terroryzmu:

- rozpoznawanie i przeciwdziałanie międzynarodowym akcjom terrorystycznym;
- przeciwdziałanie międzynarodowemu obrotowi bronią, towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa;
- przeciwdziałanie proliferacji broni masowej zagłady;
- rozpoznawanie i eliminowanie zagrożeń w rejonach napięć, konfliktów i sytuacji kryzysowych mających wpływ na obronność kraju;
- gromadzenie, analizowanie i przekazywanie odpowiednim organom informacji istotnych dla bezpieczeństwa państwa.

W zakresie profilaktyki podejmowane są pewne działania, głównie przez Policję i MENiS, jednak nie są one ustrukturyzowane ani standaryzowane, a przez to nieskuteczne na skalę społeczną.

Siły Zbrojne RP a zwalczanie terroryzmu

Zgodnie z aktami prawnymi zwalczanie aktów terroryzmu to zadanie sił policyjnych i służb specjalnych, które mogą być wspomagane przez oddziały SZ na podstawie Rozporządzenia RM z dnia 19 lipca 2005 roku w sprawie szczegółowych warunków i sposobu użycia oddziałów i pododdziałów Policji oraz Sił Zbrojnych RP w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego.

Do zadań oddziałów SZ należy: ochrona, izolacja określonych obiektów infrastruktury krytycznej, dróg lub części miast, wspieranie działań oddziałów Policji przywracających bezpieczeństwo, odbijanie zakładników, wsparcie logistyczne oddziałów Policji.

Odziały wyspecjalizowane w tym zakresie to:

- Wojskowa Formacja Specjalna GROM (JW 2305)
- Sekcja Działań Specjalnych Marynarki Wojennej RP FORMOZA,
- Pułk Specjalny Komandosów (JW 4101)
- Oddziały specjalne ŻW

Siły Zbrojne RP w systemie zarządzania kryzysowego

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym określa struktury systemu zarządzania i zadania. Zarządzanie kryzysowe realizowane jest na poziomach: krajowym, wojewódzkim, powiatowym i gminnym. Na terytorium RP zarządzanie kryzysowe sprawuje Rada Ministrów i funkcjonujący przy niej Rządowy Zespół Zarządzania Kryzysowego jako organ doradczy. W skład Zespołu wchodzą: Prezes RM (przewodniczący), Minister Obrony Narodowej, minister właściwy do spraw wewnętrznych, Minister Spraw Zagranicznych, oraz, jeżeli powołany, Minister Koordynator Służb Specjalnych. Obsługę RM, Prezesa RM i Zespołu zapewnia Rządowe Centrum Bezpieczeństwa, które:

- wykonuje zadania planistyczne;
- monitoruje potencjalne zagrożenia;
- uruchamia procedury związane z zarządzaniem kryzysowym;
- współpracuje z jednostkami organizacyjnymi NATO i UE;
- zapewnia obieg informacji;
- realizuje zadania z zakresu przeciwdziałania, zapobiegania i likwidacji skutków ataków terrorystycznych.

Na terenie województwa zadania w zakresie zarządzania kryzysowego wykonuje wojewoda:

- monitoruje, planuje, reaguje i likwiduje skutki zagrożeń na terenie województwa;
- wnioskuje o użycie pododdziałów i oddziałów SZ RP do wykonywania zadań w sytuacji zagrożenia;
- zapobiega, przeciwdziała atakom terrorystycznym i usuwa ich skutki.

Minister Obrony Narodowej, na wniosek wojewody, przekazuje do jego dyspozycji oddziały i pododdziały sił zbrojnych do zadań z zakresu zarządzania kryzysowego, jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub niewystarczające. Oddziały SZ mogą być przekazane w składzie etatowym lub jako doraźne zgrupowania zadaniowe. Ich obowiązki to:

- współudział w monitorowaniu zagrożeń;
- udział w akcjach poszukiwawczo-ratowniczych;
- ewakuowanie ludności i mienia i przygotowanie warunków do tymczasowego przebywania tej ludności w określonych miejscach;
- izolowanie obszaru występowania zagrożeń;
- usuwanie materiałów niebezpiecznych i likwidowanie skażeń chemicznych, zakażeń biologicznych i skażeń promieniotwórczych;
- naprawa i odbudowa infrastruktury technicznej;
- udzielanie pomocy medycznej, w tym zadań przeciwepidemiologicznych.

Zadania na etapie likwidowania skutków ataków terrorystycznych wykonują jednostki wojskowe inżynieryjne, chemiczne, logistyczne i medyczne. Zadania Sił Zbrojnych RP w walce z terroryzmem poza obszarem kraju obejmują: ochronę własnych obywateli i ewakuację, uwolnienie własnych obywateli przetrzymywanych jako zakładnicy na terytorium innego państwa, likwidację infrastruktury szkoleniowej i logistycznej oraz kadry kierowniczej grup terrorystycznych. Do tego celu wyznaczone są siły Żandarmerii Wojskowej, oddziały wojsk inżynieryjnych i chemicznych. Siły Zbrojne RP na rzecz przeciwdziałania terroryzmowi na arenie międzynarodowej

Dla polskiej polityki międzynarodowej kluczowym wydarzeniem było ratyfikowanie aktu przystąpienia Polski do Traktatu Północnoatlantyckiego 12 marca 1999 roku. Polska przyjęła zadanie aktywnie uczestniczyć w działaniach podejmowanych na rzecz stabilizacji i pokoju na kontynencie. Wydarzenia z 11 września 2001 roku dopełniły i dookreśliły role Polski w układzie sił międzynarodowych. Artykuł 5 Traktatu Północnoatlnatyckiego wydany 12 września 2001 roku[26] w skutek katastrofy dnia poprzedniego zobowiązuje wszystkich jego członków, by traktować atak na jednego lub kilku z nich na terenie Europy lub Ameryki Północnej jako atak przeciwko wszystkim, co w konsekwencji ma doprowadzić do jednomyślnego potępienia i zwalczenia wszelkiej przemocy i aktów terroru. Kolejny dokument wytyczający kierunek polskiego bezpieczeństwa to Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007 roku. Uwzględnia i ostro zarysowuje charakter zagrożeń, w tym terroryzmu, jakim Polska musi stawić czoło w dynamicznie zmieniającym się układzie sił międzynarodowych. Podkreśla, ze ataki terrorystyczne mogą zostać skierowane przeciwko Polsce w odwecie za udział w międzynarodowej koalicji antyterrorystycznej. Siły Zbrojne RP mają więc za zadanie wspierać działania prewencyjne na terytorium RP, i z zakresu zarządzania kryzysowego z udziałem wojsk specjalnych. Wyrazem polityki państwa w tym zakresie jest obecność polskich żołnierzy w rejonach konfliktów w Bośni i Hercegowinie, Kosonie, Syrii, Libanie, Kongo Czadzie, Iraku, i Afganistanie.

Powołując się na opinię K. Liedla

Siły Zbrojne to jeden z nielicznych komponentów polskiego systemu bezpieczeństwa, który już przed 11 września 2001 roku przystosowany był do przeciwdziałania zagrożeniom terrorystycznym nie tylko na mocy uprawnień i zadań związanych z innymi zagrożeniami bezpieczeństwa państwa, ale także jako autonomicznie identyfikowanego zagrożenia, jakim jest terroryzm[27]. Stan ten odzwierciedla kierunek polityki państwa polskiego i rzeczywisty stan obronności państwa. Uwarunkowania geopolityczne i geostrategiczne wymuszają poniekąd traktowanie wszelkich zagrożeń z największą ostrożnością i uwagą. Nie mamy jako społeczeństwo możliwości kontrolowania intencji nawet tych najbardziej przerażających jakim jest atak terrorystyczny ale jako część społeczeństwa europejskiego musimy wyciągać wnioski z wydarzeń września 2011, aby śmiech w infosferze[28] nie był śmiechem z Polski zaskoczonej przemocą.

[26] NATO Handbook, Public Diplomacy Division, NATO, 1110 Brussels, Belgium 2006, s.372.
[27] Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2010, s.81.
[28] Toffler A., Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s.104.

Bibliografia

Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie, Bellona, Warszawa.
Jordan T., *Hakerstwo*, PWN, Warszawa 2011.
Irak 2004 ku przyszłości. Materiału z konferencji naukowej zorganizowanej z inicjatywy i pod patronatem Ministra Obrony Narodowej, AON, Warszawa 2004.
Kępka P., *Bioterroryzm. Polska wobec użycia broni biologicznej*, Difin, Warszawa 2009.
Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*. Zarządzanie bezpieczeństwem, Difin, Warszawa 2010.
Liedel K., Piasecka P., Aleksandrowicz T.R., *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmen w Europie*, Difin, Warszawa 2011.
NATO Handbook, *Public Diplomacy Division*, NATO, 1110 Brussels, Belgium 2006.
Toffler A., Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006.
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007.
Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, Warszawa, marzec 2009, str. 4 – http://www.cert.gov.pl/portal/cer/30/Rzadowy_program_ochrony_ cyberprzestrzeni.html.
Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej, Rok XLVI, nr 1 (160), 2005, str. 175 i n.www.amw.gdynia.pl/library/File/Zeszyty Naukowe/2005/Szubrycht_T.pdf.
Współczesne operacje reagowania kryzysowego – wymóg regionalnego bezpieczeństwa czy operacje przyszłości. Materiały z konferencji naukowej, AON, Warszawa 2005.

Recenzent: doc. dr Zbigniew GRZYWNA