dr Marcin Oskierko
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0003-3450-6037

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

dr Julia Kobets
Przykarpacki Uniwersytet Narodowy im. Wasyla Stefanyka
w Iwano-Frankiwsku
ORCID: 0000-0001-9492-6119

mgr Wiktoria Marcinek
ORCID: 0009-0009-0959-6182

https://doi.org/10.29316/9788368103205_14

METODY DZIAŁANIA I ŹRÓDŁA FINANSOWANIA WSPÓŁCZESNYCH ORGANIZACJI TERRORYSTYCZNYCH

METHODS OF OPERATION AND SOURCES OF FINANCING OF CONTEMPORARY TERRORIST ORGANIZATIONS

Streszczenie

Celem niniejszego rozdziału jest analiza metod działania współczesnych grup terrorystycznych oraz źródeł ich finansowania w kontekście rosnącego zagrożenia dla bezpieczeństwa państwowego i międzynarodowego. Problem badawczy ujęto w pytaniu: W jaki sposób współczesne organizacje

Summary

The aim of this chapter is to analyze the methods of operation of contemporary terrorist groups and the sources of their financing in the context of the growing threat to state and international security. The research problem is addressed in the question: How do contemporary terrorist organizations diversify

terrorystyczne różnicują swoje metody działania i pozyskiwania środków finansowych oraz jak wpływa to na skuteczność systemów przeciwdziałania terroryzmowi? Postawiono hipotezę, że im bardziej zróżnicowane i trudne do wykrycia są metody działania oraz finansowania organizacji terrorystycznych, tym większe wyzwania napotykają systemy bezpieczeństwa w zakresie przeciwdziałania terroryzmowi. W pracy wykorzystano metody teoretyczne, w tym analizę dokumentów źródłowych, przegląd literatury naukowej, analizę przypadków oraz studia porównawcze dotyczące działań terrorystycznych i mechanizmów ich finansowania. Główny wniosek wskazuje, że skuteczne przeciwdziałanie terroryzmowi wymaga zintegrowanego podejścia obejmującego działania legislacyjne, technologiczne i międzynarodową współpracę instytucjonalną, ze szczególnym uwzględnieniem nowych zagrożeń, takich jak cyberterroryzm czy finansowanie z użyciem kryptowalut.

Słowa kluczowe: terroryzm, finansowanie terroryzmu, cyberterroryzm, bezpieczeństwo narodowe, metody działań terrorystycznych

their methods of operation and obtaining funds, and how does it affect the effectiveness of counter-terrorism systems? It has been hypothesized that the more diverse and difficult to detect the methods of operation and financing of terrorist organizations, the greater the challenges faced by security systems in the field of counterterrorism. The paper uses theoretical methods, including the analysis of source documents, a review of scientific literature, case studies and comparative studies on terrorist activities and the mechanisms of their financing. The main conclusion is that effective counter-terrorism requires an integrated approach involving legislative, technological, and international institutional cooperation, with a particular focus on emerging threats such as cyberterrorism and cryptocurrency financing.

Keywords: terrorism, financing terrorism, cyberterrorism, national security, methods of terrorist activities

Wstęp

Terroryzm od dekad stanowi jedno z najpoważniejszych zagrożeń dla bezpieczeństwa międzynarodowego, narodowego i lokalnego. Jego ewolucja, zarówno w zakresie ideologii, jak i środków działania, sprawia, że współczesne państwa muszą nieustannie dostosowywać strategie przeciwdziałania oraz metody identyfikacji potencjalnych zagrożeń. W XXI wieku działalność grup terrorystycznych przybiera coraz bardziej zróżnicowane formy, obejmując zarówno klasyczne zamachy bombowe i porwania, jak i cyberataki, wykorzystanie broni biologicznej oraz działania prowadzone przez tzw. „samotne wilki". Kluczowym elementem skuteczności tych organizacji pozostaje jednak dostęp do źródeł finansowania – legalnych i nielegalnych – które umożliwiają realizację zamierzeń ideologicznych oraz prowadzenie działań operacyjnych.

Niniejszy rozdział ma na celu przybliżenie metod działania współczesnych grup terrorystycznych, z uwzględnieniem ich taktyki, środków przemocy oraz mechanizmów finansowania. Ukazuje także skalę zagrożeń wynikających z postępu technologicznego, jak również podejmowane środki przeciwdziałania, zarówno na poziomie krajowym, jak i międzynarodowym.

Metody i działania grup terrorystycznych

Zorganizowane grupy terrorystyczne nie tylko dokonują zamachów terrorystycznych, ale także prowadzą kampanie terrorystyczne. Zamachy mają charakter incydentalny, natomiast kampanie to umyślna i zamierzona seria ataków, które przeprowadzane są na dużą skalę w krótkim okresie. Grupy terrorystyczne działają w oparciu o metody działania, czyli charakterystyczne sposoby, za pomocą których dokonują zamachów[1].

Zamachy terrorystyczne, przeprowadzone w formie pojedynczego ataku czy też całej serii, różnią się przede wszystkim w zależności od zastosowanych środków przemocy. Wyodrębnia się:

- ataki bombowe,
- zamachy z wykorzystaniem broni palnej,
- zamachy z użyciem broni masowego rażenia – ładunku promieniotwórczego, środków chemicznych,
- ataki związane z cyberprzestrzenią – z wykorzystaniem sieci internetowej,
- ataki dokonane za pomocą wybranego środka transportu – powietrznego, lądowego lub nawodnego[2].

Działania terrorystyczne prowadzone przez zorganizowane grupy mogą być podejmowane nie tylko bezpośrednio wobec ludzi, ale również wobec infrastruktury. Szczególnie ataki skierowane w obiekty i systemy infrastruktury krytycznej powodują chaos i znaczną dezorganizację, co w konsekwencji prowadzi do zakłócenia minimalnego funkcjonowania państwa oraz jego gospodarki. Akty terrorystyczne wymierzone w obiekty infrastrukturalne przebiegają

[1] B. Bolechów, *Terroryzm w świecie podwubiegunowym,* Wydawnictwo Adam Marszałek, Toruń 2003, s. 39.

[2] P. Lubiewski, *Reguły i metody działania współczesnych organizacji terrorystycznych*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, Nr 29(4), 2018, s. 113-114.

zazwyczaj według podobnego schematu, zawierającego kolejno następujące po sobie fazy, takie jak:

- podejście do obiektu, który stanowi cel ataku,
- wejście na teren obiektu,
- dokonanie zniszczeń bądź uszkodzeń obiektu z możliwością uprowadzenia wybranej, zawartej w planie osoby,
- oddalenie się z miejsca ataku lub też dokonanie zamachu samobójczego[3].

Faktem jest, że organizacje terrorystyczne kierują swoje działania często bezpośrednio w ludzi, narażając ich zdrowie i pozbawiając życia w imię wyznawanej ideologii. Wykonawcy ataków terrorystycznych przyjmują w tym celu różną taktykę. Mogą zorganizować zasadzkę lub sieć zasadzek, przeprowadzić napad lub dokonać rabunku. Ich celem nierzadko są uprowadzenia, zabójstwa czy też przetrzymywanie zakładników, dzięki którym zamierzają wymusić określone zachowania[4].

Warto wspomnieć, że grupy terrorystyczne wykorzystują w swoich działaniach elementy psychologiczne, dzięki którym wywierają znaczący wpływ na stan psychiki przeciwnika oraz jego morale. Ponadto, działania te powodują wzrost poczucia przygnębienia oraz rezygnacji, a także wzmagają niepewność i osłabiają wolę walki wśród społeczeństwa będącego celem ataku. Terroryści do zrealizowania zamierzonych zadań wykorzystują techniki polegające na:

- szerzeniu propagandy poprzez rozpowszechnianie informacji, które kwestionują autorytet władz państwowych,
- przecenianiu znaczenia efektów realizacji swoich zadań, wzbudzaniu paniki, chaosu i niepewności, na przykład poprzez przekazywanie nieprawdziwych informacji za pomocą środków masowego przekazu[5].

Poza aspektem psychologicznym, strategie terrorystów, zawierają również inne elementy. Uogólniając, większość organizacji terrorystycznych, funkcjonuje w oparciu o takie zasady jak:

- nieprzestrzeganie ustanowionego prawa międzynarodowego w zakresie konfliktów zbrojnych,
- kierowanie ataków zazwyczaj w osoby niewinne i nieuzbrojone,

[3] Ibidem, s. 114.
[4] Ibidem.
[5] Ibidem.

- dokonywanie zamachów na terenach miejskich, wysoce zurbanizowanych, z uwagi na gęstość zaludnienia oraz obecność atrakcyjnych celów, na przykład ważnych kulturowo lub strategicznie budynków,
- odrzucenie wszelkich norm moralnych,
- działanie w celu zadania możliwie największych strat wśród ofiar i zyskania rozgłosu,
- wybieranie odpowiednich środków przemocy, które pokażą bezwzględność organizacji,
- planowanie tak zwanych sieci konspiracyjnych, na przykład ukrytych magazynów środków pieniężnych czy broni, lokali zajmowanych przez członków organizacji i wykonawców zamachu,
- stosowanie przemocy i siły w sposób jak najbardziej efektowny i spektakularny, z zamiarem zwrócenia uwagi społeczeństwa i osiągnięcia zamierzonych celów[6].

Jeden z punktów strategii dotyczy nieprzestrzegania przez terrorystów prawa międzynarodowego. Przejawia się to między innymi w świadomym dokonywaniu zamachów na osoby cywilne, chronione prawem międzynarodowym, w tym na dyplomatów, braniu zakładników i pozbawianiu ich życia. W ramach przyjętej przez poszczególne organizacje strategii, jej członkowie wykorzystują różne metody przeprowadzania zamachów. Jedną z najpopularniejszych technik stosowanych przez terrorystów w XXI wieku stanowią zamachy samobójcze. Osoby dokonujące takiego zamachu zazwyczaj ukrywają materiały wybuchowe pod ubraniem – jako tak zwany *pas szahida* lub w bagażach podręcznych, na przykład w plecakach czy torbach. Odnotowano również przypadki, kiedy ładunki wybuchowe w dużej ilości ukryte były w pojazdach, którymi poruszali się zamachowcy. Ataki te są szczególnie niebezpieczne, ponieważ powodują śmierć bardzo dużej ilości osób. Z tego względu są uważane przez terrorystów za efektowne i spektakularne, dlatego też ich powtarzalność jest coraz częstsza[7].

Z początkiem XXI wieku, między innymi islamscy fundamentaliści powrócili do znanej od tysięcy lat metody pozbawiania życia poprzez dekapitację, czyli uśmiercanie ofiary przez ścięcie głowy. Niegdyś była ona stosowana

[6] G. Nowacki, *Zagrożenia terrorystyczne na świecie*, Nierówności Społeczne a Wzrost Gospodarczy, Nr 44(4), 2015, s. 416-17.

[7] K. Karolczak, *Terroryzm XXI wieku – wybrane aspekty*, Terroryzm – Studia, Analizy, Prewencja 2022, Nr 1(1), s. 12.

nie tylko jako kara za faktycznie dokonane przestępstwa lub zbrodnie wyimaginowane, ale również jako forma ostrzeżenia dla osób planujących przeciwstawienie się ówcześnie panującej władzy. Terroryści wykorzystują tą metodę także jako ultimatum w sprawie uwolnienia więzionych terrorystów w zamian za darowanie życia przetrzymywanej przez nich ofiary[8].

Za przykład wyżej wymienionej techniki stosowanej przez terrorystów może posłużyć historia Daniela Pearl'a, amerykańskiego dziennikarza, pracującego dla Wall Street Journal. Mężczyzna został uprowadzony z własnego samochodu 23 stycznia 2002 r. w Pakistanie. Zabójstwa dziennikarza dokonano 1 lutego tego samego roku. Porywacze zamieścili w Internecie film, który ukazuje ostatnie minuty jego życia oraz drastyczną scenę przedstawiającą dekapitację. Ciało mężczyzny zostało odnalezione i zidentyfikowane kilka miesięcy później – 16 maja 2002 r. Mimo że do porwania i pozbawienia życia dziennikarza przyznała się organizacja National Movement for the Restoration of Pakistani Sovereignty, to pakistański rząd skierował oskarżenia ku członkom Al-Kaidy, których później aresztowano[9].

Warto pamiętać, że podobny los spotkał polskiego geologa, pracownika Geofizyki Kraków, Piotra Stańczaka. Tymczasowo przebywał on w Pakistanie w związku z kontraktem realizowanym przez krakowską firmę dla pakistańskiego przedsiębiorstwa Oil & Gas Development Company Limited. W momencie porwania, we wrześniu 2008 r., mężczyzna podróżował samochodem w rejonie Pind Sultani, miejscowości oddalonej około 100 km od stolicy Pakistanu. Jego porywaczami okazali się Talibowie, którzy żądali między innymi zwolnienia z pakistańskich więzień 110 talibów. W zamian za to, Piotr Stańczak, miał odzyskać wolność. Pakistański Rząd nie spełnił ultimatum, w związku z czym w lutym 2009 r. Talibowie powiadomili o zabójstwie Polaka poprzez dekapitację. Jego ciało z początkiem maja 2009 r., zgodnie z wolą rodziny, spoczęło na cmentarzu w Krośnie[10].

Wykorzystanie dekapitacji jako środka służącego do zastraszania przeciwnika i zmuszania go do wypełniania żądań stawianych przez ugrupowania

[8] Ibidem, s. 13.

[9] Ibidem.

[10] *Prezydent odznaczył zabitego przez talibów geologa*, 04 października 2010 r., https://www.prezydent.pl/kancelaria/archiwum/archiwum-bronislawa-komorowskiego/aktualnosci/ordery-i-odznaczenia/prezydent-odznaczyl-zabitego-przez-talibow-geologa,18399, [dostęp: 25.04.2025].

terrorystyczne nie dotyczy tylko pojedynczych jednostek. Przed dekadą, do globalnej opinii publicznej dotarły informacje o egzekucjach przeprowadzonych w taki sposób w okresie między 25 lipca 2014 r. a 10 sierpnia 2015 r. Ofiarami byli między innymi:

- żołnierze kurdyjscy oraz syryjscy,
- chrześcijańscy uchodźcy pochodzący z Etiopii,
- pracownicy organizacji humanitarnych,
- dziennikarze z różnych części świata[11].

Ogółem, w tym czasie, w 24 egzekucjach dokonanych przez Państwo Islamskie, śmierć poniosło co najmniej 300 osób. Jedną z kategorii terrorystów stanowią *samotne wilki,* czyli zamachowcy, którzy:

- nie są członkami żadnej organizacji,
- nie dążą do realizacji konkretnego, ogólnoświatowego planu,
- nie są zobligowani do wypełniania rozkazów dowódcy,
- planują i przeprowadzają zamachy samodzielnie[12].

Ofiarami *samotnych wilków* są najczęściej osoby przypadkowe i nieznane sprawcom. Należy jednak pamiętać, że nie każdy pojedynczy atak, przeprowadzony przez zamachowca w sposób samodzielny, jest atakiem o charakterze terrorystycznym. Warunkiem uznania go za czyn terrorystyczny jest fakt działania sprawcy w myśl określonej idei, kiedy przyczyną ataku jest na przykład motyw polityczny lub radykalny światopogląd.

Przykładem ataku terrorystycznego, dokonanego przez „samotnego wilka" jest zamach z 22 lipca 2011 r. Norweg Anders Breivik, najpierw w dniu zamachu opublikował w sieci internetowej swojego autorstwa manifest, noszący tytuł 2083 – Europejska Deklaracja Niepodległości. Stanowił on zbiór tekstów o charakterze ksenofobicznym, islamofobicznym, rasistowskim i antyfeministycznym. Następnie przeprowadził zamach bombowy na siedzibę norweskiego premiera w Oslo, w której śmierć poniosło 8 osób. Tego samego dnia, przemieścił się na wyspę Utøya, gdzie trwał obóz młodzieżowej sekcji norweskiej Partii Pracy. Anders Breivik za pomocą broni palnej dokonał masowej strzelaniny, w wyniku której zginęło 69 osób. Sprawcę uznano za poczytalnego w momencie dokonywania czynu. Zastosowano wobec niego najwyższy możliwy wymiar kary, skazując go na 21 lat pozbawienia wolności, z zachowaniem

[11] K. Karolczak, *Terroryzm XXI wieku – wybrane aspekty*, op. cit., s. 14.

[12] Ibidem.

możliwości nieograniczonego jej przedłużenia. Zamachowiec, wyznający poglądy skrajnie prawicowe, w trakcie procesu przyznał, że do ataku skłoniły go pobudki polityczne. Ponadto, wykonywał również charakterystyczne gesty faszystowskiego pozdrowienia. Zachowania oraz motyw sprawcy pozwalają uznać, że czyn, jakiego się dopuścił, miał charakter terrorystyczny[13].

Charakterystyczne metody stosują organizacje, działające w ramach bioterroryzmu. Stosowana przez nich broń biologiczna jest niezwykle niebezpieczna. Do przeprowadzenia ataków z jej użyciem wykorzystuje się patogenne mikroorganizmy, takie jak laseczki wąglika, wirusy albo toksyny pochodzenia biologicznego, na przykład rycynę czy botulinę. Produkcja broni biologicznej pochłania stosunkowo niskie koszty, a materiały wykorzystywane w procesie wytworzenia są łatwo dostępne, ponieważ niektóre z nich można pozyskać nawet z surowców naturalnych[14].

Broń biologiczna jest nie tylko wysoce skuteczna, ale także trudna do wykrycia. Wpływa na to między innymi szybkość rozprzestrzeniania się patogenu zakaźnego oraz szerokie możliwości jego transportu. Ponadto, nawet niewielka dawka środka biologicznego jest w stanie wywołać infekcje i choroby o ciężkim przebiegu, często odporne na podejmowane przez medyków leczenie. Ataki z wykorzystaniem broni biologicznej ukierunkowane są na wywołanie epidemii, nierzadko bardzo śmiercionośnej, która w konsekwencji doprowadzi do strat społecznych i gospodarczych, poczucia niepokoju w społeczeństwie, dezorganizacji władzy, a nawet destabilizacji sfery finansowej państwa[15].
Sprawcy zamachów, noszących znamiona bioterroryzmu, wybierają różne metody działania. Ataki mogą być przeprowadzone między innymi poprzez:

- skażenie powietrza,
- skażenie ujęć wody lub artykułów żywnościowych,
- ukrycie i przekazanie środków biologicznych w przesyłkach pocztowych[16].

Ponadto, dzięki rozwojowi inżynierii genetycznej i biotechnologii, bioterroryści zyskują nowe możliwości dostępu do broni biologicznej, co w przyszłości

[13] Ibidem, s. 15-16.
[14] P. Nowak, *Bioterroryzm i chemoterroryzm jako formy współczesnego terroryzmu. Zapobieganie atakom w Rzeczypospolitej Polskiej,* Kultura Bezpieczeństwa 2019, Nr 36, s. 48-49.
[15] Ibidem, s. 48-50.
[16] Ibidem, s. 50.

może spowodować, że staną się samowystarczalni w zakresie produkcji tego rodzaju broni. Zagrożenie wykorzystania badań, odkryć i eksperymentów naukowych z zakresu medycyny w sposób niewłaściwy, przez osoby do tego nieuprawnione, może spowodować, że potencjalne ataki z użyciem środków biologicznych osiągną w przyszłości zasięg globalny[17].

Cyberprzestrzeń postrzegana jest jako olbrzymia cyfrowa biblioteka[18], z której mogą korzystać wszyscy użytkownicy, również terroryści. Terroryści w ten sposób mają dostęp do ogromnej ilości informacji, których uzyskanie było wcześniej niezwykle utrudnione, choćby ze względu na ich rozproszenie geograficzne, jak i różnorodność form występowania[19]. Zwiększająca się dynamicznie liczba stron internetowych zapewnia dostęp do wiedzy, która może być wykorzystana zarówno w legalnych, jak i bezprawnych zamiarach również w aktach bezprawnej ingerencji[20]. W literaturze możemy odnaleźć dwa główne obszary wykorzystania Internetu jako źródła pozyskiwania przez terrorystów informacji[21]. Pierwszym obszarem są wszelkie legalnie dostępne w Internecie dane, które mogą posłużyć do rozpoznania potencjalnych obiektów ataku oraz pozwalają zapoznać się z ich otoczeniem, a także informacje, które mogą ułatwić planowanie i przygotowanie zamachu terrorystycznego. Źródła te mogą być różne[22]. Na przykład, na stronach internetowych często znajdują się szczegółowe mapy, zdjęcia oraz opisy infrastruktury krytycznej, takich jak lotniska, elektrownie, budynki rządowe czy obiekty wojskowe. Media społecznościowe umożliwiają monitorowanie działań osób, które mogą być celem ataków, oraz zdobycie informacji na temat rutynowych działań i zabezpieczeń stosowanych w różnych miejscach.

---

17 Ibidem.

18 M. Ranstorp, *The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation*, [w:] *International Relations and Security in the Digital Age*, J. Eriksson, G. Giacomello (red.), Routledge. London 2007, s. 40.

19 M. Conway, *Terrorist 'Use' of the Internet and Fighting Back*, Information & Security. An International Journal, vol.19, 2006, s. 16.

20 R. Hennig, *Cyberterroryzm miękki. Cz. 1, Internet jako źródło informacji i funduszy*, Przegląd Naukowo-Metodyczny, Edukacja dla bezpieczeństwa, Rok IX, nr 4 (29), 2015, s. 46.

21 D. Thelesklaf, M. Gercke, *Terrorist Use of the Internet and Legal Response.* F3 – Freedom From Fear Magazine, Issue 7, July 2010, s. 18.

22 B.W. Don et al., *Network Technologies for Networked Terrorists*, *Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, RAND Technical Report, 2007, s. 25.

Kolejnym źródłem są bazy danych i rejestry publiczne, które zawierają informacje o firmach, instytucjach oraz osobach prywatnych. Rejestry te mogą dostarczyć cennych informacji na temat struktury organizacyjnej, danych kontaktowych oraz lokalizacji potencjalnych celów. Dostęp do takich danych może być uzyskany legalnie, co utrudnia ich monitorowanie i kontrolę przez organy ścigania. Dodatkowo, informacje geolokalizacyjne dostępne poprzez usługi, takie jak Google Maps czy Bing Maps, pozwalają na dokładne zapoznanie się z topografią terenu oraz szczegółami dotyczącymi infrastruktury. Umożliwiają one terrorystom przygotowanie szczegółowych planów operacyjnych bez konieczności fizycznego rozpoznania terenu.

Warto również wspomnieć o publikacjach akademickich oraz raportach branżowych, które często zawierają szczegółowe analizy dotyczące zabezpieczeń oraz potencjalnych słabych punktów w różnych sektorach infrastruktury. Tego typu dokumenty, dostępne w bibliotekach i repozytoriach internetowych, mogą być wykorzystane do zdobycia specjalistycznej wiedzy niezbędnej do przeprowadzenia zamachu.

Wszystkie te źródła informacji są legalnie dostępne, co sprawia, że ich monitorowanie i kontrola są dużym wyzwaniem dla służb wywiadowczych i organów ścigania. Właśnie dlatego, w celu przeciwdziałania wykorzystywaniu tych danych przez terrorystów, konieczna jest współpraca międzynarodowa oraz wprowadzenie odpowiednich regulacji prawnych, które ograniczą dostęp do wrażliwych informacji oraz zwiększą świadomość społeczną na temat zagrożeń związanych z udostępnianiem danych w Internecie.

Organizacjami terrorystycznymi kierują różne motywy. Działają głównie w oparciu o przemoc w celu wywołania chaosu, niepokoju czy podważenia autorytetu władzy. Wykorzystywane przez terrorystów środki to najczęściej broń palna lub bomby, jednak rozwój technologiczny obserwowany w ciągu ostatnich lat powoduje pojawienie się nowych rozwiązań, za pomocą których zamachowcy mogą realizować stawiane im cele. Modyfikacje i ciągłe ulepszanie stosowanej broni wpływają na wzrost jej skuteczności. Stwarza to zagrożenie, że przyszłe potencjalne ataki terrorystyczne będą jeszcze tragiczniejsze w skutkach[23].

[23] J. Horgan, *Psychologia terroryzmu,* Wydawnictwo Naukowe PWN, Warszawa 2015, s. 28-29.

Źródła finansowania terroryzmu

Terroryzm jest złożonym zjawiskiem, którego istotnym elementem jest finansowanie. Bez odpowiednich środków finansowych organizacje terrorystyczne nie byłyby w stanie przeprowadzać operacji, rekrutować członków ani realizować swojej ideologii. Zrozumienie źródeł finansowania terroryzmu jest kluczowe dla skutecznego przeciwdziałania temu zagrożeniu.

Organizacje terrorystyczne finansują swoją działalność ze środków pochodzących z przestępstwa, jak również ze źródeł legalnych[24]. Do najważniejszych należą:

- przestępczość zorganizowana,
- przestępstwa finansowe,
- wsparcie państwowe,
- donacje i datki,
- własne działalności gospodarcze,
- zasoby naturalne[25].

W związku z koniecznością finansowania swojej działalności organizacje terrorystyczne w dużym stopniu współpracują z grupami przestępczymi zajmującymi się działalnością kryminalną[26].

Jednym z głównych źródeł finansowania jest przestępczość zorganizowana. Organizacje terrorystyczne często angażują się w handel narkotykami, przemyt broni, fałszerstwa oraz inne formy przestępczości, które dostarczają im znaczących środków finansowych[27]. Handel narkotykami, na przykład, jest szczególnie dochodowy, zwłaszcza w regionach takich jak Afganistan, gdzie produkcja opium stanowi istotne źródło dochodów dla grup terrorystycznych.

Przestępstwa finansowe również odgrywają istotną rolę w finansowaniu terroryzmu. Pranie pieniędzy, oszustwa podatkowe oraz cyberprzestępczość to popularne metody uzyskiwania funduszy. Organizacje terrorystyczne korzystają z zaawansowanych technik prania pieniędzy, aby legalizować swoje dochody i unikać wykrycia przez organy ścigania. Do zaistnienia przestępstwa

[24] K. Izak, M. Kluczyński, *Handel Narkotykami jako źródło finansowania terroryzmu*, Przegląd Bezpieczeństwa Wewnętrznego, nr 10, 2014, s. 38.

[25] T. Bąk, *Oblicza terroryzmu*, Wydawnictwo Konsorcjum Akademickie, Kraków-Rzeszów-Zamość 2011, s. 103-113.

[26] J. W. Wójcik, *Przeciwdziałanie finasowaniu terroryzmu*, Wolters Kluwer, Warszawa 2007, s. 82-83.

[27] K. Izak, M. Kluczyński, *Handel Narkotykami …*, op. cit., 39.

finansowania terroryzmu nie jest koniecznie występowanie przestępstwa bazowego. Ta różnica może być istotna dla systemów wykrywania obu przestępstw[28]. Jedną z kluczowych różnic między praniem pieniędzy a finansowaniem terroryzmu jest to, że w wypadku pierwszego chodzi o źródło funduszy, a drugiego o ich miejsce przeznaczenia[29].

W ostatnich latach rośnie także rola cyberprzestępczości, gdzie kradzież tożsamości, phishing oraz inne formy oszustw internetowych stają się coraz bardziej powszechne, co może się przerodzić w ataki terrorystyczne.

Cyberprzestępczość stała się popularną metodą uzyskiwania funduszy przez organizacje terrorystyczne, ze względu na anonimowość i globalny zasięg, które oferuje internet. Grupy terrorystyczne stosują różne techniki cyberprzestępcze, aby zdobyć środki finansowe na swoją działalność. Poniżej w tabeli przedstawiono rzeczywiste przykłady i źródła wykorzystywania cyberprzestępczości do finansowania swoich operacji.

Tabela 1. Rzeczywiste przykłady i źródła wykorzystywania cyberprzestępczości do finansowania operacji terrorystycznych.

Rodzaj i forma przestępstwa	Przykład wykorzystania
Ransomware (oprogramowanie wymuszające okup)	Grupa Lazarus (podejrzewana o powiązania z Koreą Północną): Grupa ta jest znana z ataków ransomware, takich jak atak WannaCry w 2017 roku, który zainfekował komputery na całym świecie, żądając okupu w Bitcoinach[30].
Phishing i kradzież tożsamości	ISIS: Grupy powiązane z ISIS przeprowadzały kampanie phishingowe, aby kraść dane osobowe i finansowe, które następnie były wykorzystywane do wyłudzania pieniędzy lub przeprowadzania oszustw finansowych[31].

[28] Ł. Krupa, *Przeciwdziałanie finansowaniu terroryzmu*, Cybersecurity and Law, nr 7, 2022, s. 98.

[29] Przeciwdziałanie praniu pieniędzy: Podstawy, https://www.pibr.org.pl/static/items/publishing/AML_cz.8_Trendy%20w%20przest-opczoCcci.pdf>, [dostęp: 24.04.2025].

[30] *Globalny atak ransomware WannaCry może być powiązane z grupą cyberprzestępczą Lazarus – komentarz Kaspersky Lab*, https://itreseller.com.pl/globalny-atak-ransomware-wannacry-moze-byc-powiazane-z-grupa-cyberprzestepcza-lazarus-komentarz-kaspersky-lab/, [dostęp: 16.05.2025].

[31] *Cyberarmia kalifatu*, https://polska-zbrojna.pl/Mobile/ArticleShow/30080, [dostęp: 16.05.2025].

Rodzaj i forma przestępstwa	Przykład wykorzystania
Oszuści finansowi (fraud):	Al-Kaida: Członkowie Al-Kaidy angażowali się w różne oszustwa finansowe, takie jak kartowe oszustwa bankowe, które przynosiły organizacji znaczne zyski[32].
Krypto-waluty:	Hezbollah: Używa kryptowalut do unikania tradycyjnych systemów finansowych i sankcji, ułatwiając transfery pieniędzy między sympatykami i członkami organizacji[33].

Źródło: opracowanie własne.

Przestępcy celowo szukają giełd o niskich wymaganiach w zakresie AML w przekonaniu, że można je bez większych przeszkód wykorzystać do transakcji między pieniędzmi FATF, a kryptowalutami lub pomiędzy różnymi kryptowalutami[34]. Cechy takich giełd są następujące:

- celowe lekceważenie przepisów i wymogów rejestracyjnych;
- umożliwienie klientom zakładania rachunków przy jednoczesnym niewielkim lub żadnym wymogu przedstawienia informacji identyfikacyjnych;
- klienci otwierający rachunki nie muszą przestrzegać przepisów w żadnej jurysdykcji;
- siedziba giełdy w kraju wysokiego ryzyka, do których należą:
  - kraje z wysokim ogólnym ryzykiem prania pieniędzy i finansowania terroryzmu – zwykle w Afryce, Europie Wschodniej lub na Bliskim Wschodzie,
  - kraje podlegające międzynarodowym sankcjom, embargu i innym ograniczeniom,
  - kraje na liście jurysdykcji wysokiego ryzyka i braku współpracy FATF,
  - kraje bez regulacji AML/CTF obejmujących kryptowaluty lub z nieefektywnymi ramami regulacyjnymi.

[32] L. Lisiecki, K. Kucharski, *Źródła finasowania Al-Kaidy*, Studia bezpieczeństwa narodowego, vol. 4, nr 1, 2013, s. 298.

[33] N. Malik, *Jak przestępcy i terroryści używają kryptowaluty: i jak to powstrzymać*, Forbes 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/, [dostęp: 16.05.2025].

[34] J. Wróblewski, C. Martysz, *Kryptowaluty a finansowanie przestępczości i pranie pieniędzy*, Studia i Prace Kolegium Zarządzania i Finansów, nr 193, 2023, s. 215.

Waluty cyfrowe mogą pomóc zarówno przestępcom, jak i terrorystom kupującym towary i usługi w Darknecie, którzy w przeciwnym razie byliby narażeni na oszustwa ze strony rywalizujących organizacji przestępczych[35].

Wsparcie państwowe jest kolejnym istotnym źródłem finansowania. Niektóre państwa, kierując się własnymi celami politycznymi lub ideologicznymi, świadomie wspierają organizacje terrorystyczne, dostarczając im funduszy, broni oraz zapewniając schronienie i logistykę. Pomoc finansowa dla terrorystów zapewniana przez państwa jest naturalną przyczyną politycznych aspektów działalności wywrotowej. Organizacje terrorystyczne przy definiowaniu swoich postulatów jasno wskazują, przeciwko komu walczą i co jest ich celem, zyskując przy tym sympatię jednych oraz wrogość innych krajów[36]. Przykłady takich działań można znaleźć w historii współpracy Iranu z Hezbollachem czy innych podobnych przypadków. W corocznych raportach Departamentu Stanu USA są wymieniane państwa oskarżane o sponsorowanie terroryzmu, przy czym lista tych państw zmieniała się przez ponad 40 lat. Obecnie są na niej cztery kraje:

- Syria – od 29 grudnia 1979 r.,
- Iran – od 16 stycznia 1984 r.,
- Koreańska Republika Ludowo-Demokratyczna – od 20 listopada 2017 r.,
- Kuba – od 12 stycznia 2021 r.

Wcześniej na liście zamieszczono również Libię, Irak, Jemen Południowy i Sudan[37].

Donacje i datki od sympatyków również odgrywają znaczącą rolę. Organizacje terrorystyczne często korzystają z darowizn od osób prywatnych oraz funduszy zbieranych pod pretekstem działalności charytatywnej. Fundacje i organizacje charytatywne mogą służyć jako przykrywki do zbierania funduszy na działalność terrorystyczną, co utrudnia ich wykrywanie i neutralizację. Również publikacja informacji dotyczących swojej działalności służy prowadzonej propagandzie i może wzmacniać źródło dochodu, jakim są dotacje od osób zewnętrznych[38].

---

[35] N. Malik, *Jak przestępcy i terroryści używają kryptowaluty: i jak to powstrzymać*, Forbes 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/, [dostęp: 16.05.2025].

[36] L. Lisiecki, K. Kucharski, *Źródła finasowania*…, op. cit., s. 290.

[37] *State sponsors of terrorism*, U.S. Department of State, https://www.state.gov/state-spon-sors-of-terrorism/, [dostęp: 16.05.2025].

[38] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Bezpieczeństwo w XXI Wieku. Asymetryczny świat*, Difin, Warszawa 2011, s. 69

Ponadto, organizacje terrorystyczne często prowadzą własne działalności gospodarcze. Mogą to być zarówno małe przedsiębiorstwa, jak i duże firmy działające na skalę międzynarodową.

Firmy, które wydają się całkowicie legalne – komisy samochodowe, firmy zajmujące się nieruchomościami, organizacje charytatywne, a nawet banki – czasami służą jako legalna twarz organizacji terrorystycznych i stanowią istotny składnik aparatu pieniężnego, centralny kanał prania ogromnych sum, które organizacje terrorystyczne zarabiają na działalności przestępczej[39]. Legalne przedsięwzięcia biznesowe generują dochody, które są następnie wykorzystywane do finansowania działań terrorystycznych.

Ten system sieci służący transferowaniu pieniędzy dla Hamasu zakłada istnienie pracowników sektora finansowego czy nawet całych banków, które pośredniczą w przekazywaniu pieniędzy terrorystom. Na przykład w 2020 roku Sąd okręgowy wschodniego okręgu USA w Nowym Jorku orzekł, że mający siedzibę w Stambule bank Kuveyt Türk Katilim Bankasi m.in. prowadził konta klientów powiązanych z Hamasem, wiedząc, że pomaga transferować pieniądze[40].

Tymi klientami w bankach najczęściej są organizacje non-profit, czy firmy i korporacje działające w państwach Bliskiego Wschodu, w których Hamas posiada ukryte aktywa. Najczęściej są to firmy z sektora nieruchomości z Turcji, Arabii Saudyjskiej, Algierii, a nawet Sudanu.

Jak już wspomniano organizacje terrorystyczne korzystają również z pieniędzy pochodzących z legalnych źródeł, w tym ze wsparcia finansowego prywatnych darczyńców i organizacji charytatywnych. Organizacje charytatywne mogą być wykorzystywane przez ugrupowania terrorystyczne na trzy sposoby:

- organizacja charytatywna prowadzi działalność statutową, ale część pozyskiwanych środków przekazuje terrorystom,
- organizacja charytatywna jest jedynie kamuflażem, całość zaś pozyskiwanych przez nią środków przekazywana jest na działania ugrupowań terrorystycznych,

[39] *Najbogatsze organizacje terrorystyczne na świecie*, https://forbes.co.il/rankings/2021terrororganizations/intro/, [dostęp: 16.05.2025].

[40] *Terroryści z milionami na koncie. Skąd Hamas ma pieniądze na wojnę?*, https://geekweek.interia.pl/militaria/news-terrorysci-z-milionami-na-koncie-skad-hamas-ma-pieniadze-na-,nId,7085873#google_vignette, [dostęp: 16.05.2025].

- organizacja prowadzi działalność charytatywną, jednak pomoc udzielana jest przez punkty kontrolowane przez członków ugrupowania terrorystycznego, dzięki czemu beneficjenci mają wrażenie, że otrzymują ją od ugrupowania terrorystycznego, co przynosi wymierne efekty propagandowe[41].

Kontrola nad surowcami naturalnymi stanowi dodatkowe źródło finansowania. Niektóre grupy terrorystyczne przejmują kontrolę nad złożami ropy naftowej, diamentów, drewna czy innych surowców, które następnie sprzedają na czarnym rynku, generując znaczne zyski. Przykładem może być działalność ISIS, która finansowała się z handlu ropą naftową z kontrolowanych przez siebie terenów.

Poniżej w tabeli przedstawiono klasyfikacje grup terrorystycznych z uwzględnieniem źródeł finansowania.

Tabela 2. Klasyfikacja grup terrorystycznych z uwzględnieniem źródeł finansowania

Typy grup lub scenariuszy (działań)	Źródła finansowania
Terroryzm wewnętrzny	
• antykolonialne (nacjonalistyczne); • mniejszości etniczne, religijne i kulturowe; • mniejszości ideologiczne, lewicowe; • mniejszości ideologiczne, prawicowe; • grupy sponsorowane przez rząd; • partyzantka miejska, tj. grupy wystarczająco; duże, by miały szansę na obalenie rządu.	• sponsorowanie przez państwo, donacje; • donacje, uprowadzenia, działalność kryminalna; • rabowanie banków; • indywidualni sponsorzy; • rządowi „pracodawcy"; • donacje, podatek rewolucyjny.
Terroryzm międzynarodowy	
• emigracyjne; • wspierając emigrację; • internacjonalistyczne; • Odgrywające rolę parawanu dla innych; • kontrrewolucyjne; • Islamskie grupy fundamentalistyczne; • niezorganizowani naśladowcy.	• rabowanie banków i donacje. • finansowane przez „emigrantów"; • Starające się korzystać z tzw. war chest (skrzyń wojennych); • sponsorowane przez państwo; • sponsorowane przez państwo, również przez bogate osoby prywatne; • wiernych, osoby prywatne; • finansowani przez wszystkich, rzeczywiście nie-zorganizowani, ale wielu wyszkoliło się w Afganistanie w oszustwach z użyciem kart kredytowych i upodabniają się w małej skali do przestępców w „białych kołnierzykach".

Źródło: funding of terrorist groups compared, https://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/.

[41] P. Pomianowski, E. Maćkowiak, *Zwalczanie finansowania terroryzmu w świetle prawa obowiązującego w Polsce i we Francji*, Przegląd Bezpieczeństwa Wewnętrznego, 4(6), 2012, s. 75.

Rzeczywiście, większość najtragiczniejszych zamachów ostatnich lat nie miało tak skomplikowanych planów jak ataki na Nowy Jork, a więc mogły mieć znacznie szczuplejsze budżety. ONZ szacuje, że zorganizowanie zamachu bombowego na turystów na Bali kosztowało około 50 tysięcy dolarów. Zginęło ponad 200 osób. Na bomby użyte do zamachów w Madrycie terroryści wydali między 10 a 15 tysięcy dolarów. 191 ofiar śmiertelnych.

Zorganizowanie zamachów w londyńskim metrze w 2005 r. kosztowało około dwóch tysięcy dolarów. „Zwrot z inwestycji" był imponujący: na każdego wydanego dolara przypadło 1,27 mln dolarów strat. Bomby, które wybuchły w godzinach szczytu w metrze i autobusie zabiły ponad 50 osób. Profesor Lomborg szacuje, że materiały wybuchowe zamachowiec-samobójca może kupić za 150 dolarów. Siła wybuchu takiego ładunku może zabić 12 osób[42]. W tabeli 3 przedstawiono przykłady kosztów zamachów terrorystycznych.

Tabela 3. Koszty ataków terrorystycznych

Atak	Szacowany koszt
Atak w Nicei w 2016 roku	2 000 dolarów
Zamachy w Paryżu w listopadzie 2015 roku	30 000 euro
Atak w Bamako w 2015 roku	10 000 dolarów
Zamach w Mumbaju w 2008 roku	50 000 dolarów
Londyn 7 lipca 2005 roku	8 000 funtów
Madryt 11 marca 2004 roku	10 000 dolarów
Stambuł 15 i 20 listopada 2003 roku	40 000 dolarów
Dżakarta 5 sierpnia 2003 roku	30 000 dolarów
Bali 12 października 2002 roku	50 000 dolarów
USS Cole 12 października 2000 roku	10 000 dolarów

Źródło: opracowane na podstawie: Raport Financial Action Task Force, Terrorist Financing, Raport EMCDDA, Raport Europol.

Główne zagrożenia terrorystyczne pochodzą od osób inspirowanych ideologią Al-Kaidy, ISIS lub krajowego brutalnego ekstremizmu, które pragną przeprowadzać śmiertelne ataki bez wskazówek ze strony obcej grupy. Zagrożenia w dalszym ciągu w dużej mierze finansują się ze środków własnych, co stwarza poważne wyzwania.

[42] *Zamachy w Paryżu. Zorganizowanie ataku kosztuje grosze*, https://www.money.pl/gospodarka/wiadomosci/artykul/zamachy-w-paryzu-zorganizowanie-ataku,187,0,1955003.html, [dostęp: 16.05.2025].

Znacznym problemem jest to, iż grupy terrorystyczne w USA nadal przebywają w USA i wspierają Al-Kaidę lub ISIS, którzy chcą wysyłać pieniądze za granicę lub finansują podróże osób fizycznych, w dużej mierze wykorzystując sprawdzone metody, takie jak rejestracja i niezarejestrowanie MSB, gotówka, a w niektórych przypadkach aktywa wirtualne. Dodatkowo irańskie grupy zastępcze, takie jak Hamas i Hezbollah mogą wyszukać luki we wdrażaniu sankcji, aby wykorzystać formalny system finansowy. Hamas również do tego przyłącza zwolenników na całym świecie i wykorzystuje różnorodne wyrafinowane metody w celu gromadzenia funduszy na swoją sprawę[43].

Finansowanie terroryzmu jest złożonym i wielowymiarowym procesem, który obejmuje szeroki wachlarz źródeł i metod uzyskiwania funduszy przez organizacje terrorystyczne. Kluczowe źródła finansowania obejmują przestępczość zorganizowaną, handel narkotykami, przemyt ropy naftowej, porwania dla okupu oraz różnorodne przestępstwa finansowe, takie jak pranie pieniędzy i oszustwa. Organizacje terrorystyczne również korzystają z darowizn i datków, często zbieranych za pośrednictwem fałszywych organizacji charytatywnych, oraz z handlu zasobami naturalnymi, takimi jak diamenty i złoto. W ostatnich latach rosnącą rolę odgrywa cyberprzestępczość, w tym ataki ransomware, phishing oraz wykorzystanie kryptowalut do ukrywania i transferu środków. W tabeli 4 przedstawiono ranking najbogatszych organizacji terrorystycznych na świecie.

Tabela 4. Ranking najbogatszych organizacji terrorystycznych na świecie

Organizacja	Budżet
Hezbollah	1.1 miliarda dolarów
Talibowie	800 milionów dolarów
Hamas	700 milionów dolarów
Al-Kaida	300 milionów dolarów
ISIS	200 milionów dolarów
PKK – Partia Pracujących Kurdystanu	180 milionów dolarów
Kata'ib Hezbollah	150 milionów dolarów
Palestyński Islamski Dżichad	100 milionów dolarów
Lashkar-e-Taiba	75 milionów dolarów

[43] *2024 National Strategy for Combating Terrorist and Other Illicit Financing*, Department of the Treasury, 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf, [dostęp: 16.05.2025].

Organizacja	Budżet
Prawdziwa IRA	50 milionów dolarów

Źródło: The Richest Terror Organizations in the World, Forbes International, https://www.forbes.com/sites/forbesinternational/2018/01/24/the-richest-terror-organizations-in-the-world/, [16.05.2025].

Z analizy źródeł finansowania wynika, że organizacje terrorystyczne są niezwykle elastyczne i innowacyjne w swoich metodach pozyskiwania funduszy. Wykorzystują legalnie dostępne informacje w Internecie do planowania i realizacji działań przestępczych, co czyni ich operacje trudnymi do wykrycia i śledzenia. Anonimowość zapewniana przez kryptowaluty oraz globalny zasięg cyberprzestępczości dodatkowo utrudniają działania organom ścigania.

W związku z powyższym, kluczowe jest wprowadzenie i utrzymanie zintegrowanych działań na poziomie międzynarodowym, które obejmują współpracę między rządami, organami ścigania, sektorem prywatnym oraz organizacjami międzynarodowymi. Istotne jest również wprowadzenie bardziej rygorystycznych regulacji dotyczących przejrzystości finansowej oraz monitorowania transakcji, zwłaszcza tych związanych z kryptowalutami. Ponadto, zwiększenie świadomości społecznej na temat zagrożeń związanych z udostępnianiem wrażliwych informacji w Internecie może przyczynić się do ograniczenia możliwości wykorzystywania tych danych przez organizacje terrorystyczne.

Przeciwdziałanie finasowaniu terroryzmu

Momentem przełomowym w walce z terroryzmem były wydarzenia z 11 września 2001 r. Niezwykle istotne było oświadczenie przewodniczącego Parlamentu, szefów i rządów państw Unii Europejskiej, mówiące, że atak na Stany Zjednoczone był atakiem przeciwko wszystkim państwom Wspólnoty. W oświadczeniu tym wezwano również do globalnej walki z terroryzmem oraz przyjęcia planu działania przeciw terroryzmowi[44].

Termin „zwalczanie finansowania terroryzmu" odnosi się w szczególności do wszystkich zbiorów zasad i aktów prawnych, które zmuszają instytucje finansowe do aktywnego monitorowania swoich klientów w celu zapobiegania

[44] K. Bartosz, *Prawne aspekty walski z terroryzmem*, Security, Economy & Law, Nr 1(XVIII), 2018, s. 23.

finansowaniu terroryzmu[45]. Długoterminowym, strategicznym celem zwalczania finansowania terroryzmu jest odcięcie terrorystów od ich źródeł funduszy oraz przerwanie kanałów dystrybucji środków. Jest to jednak cel, którego pełne osiągnięcie nie wydaje się możliwe[46].

Przeciwdziałanie finansowaniu terroryzmu jest kluczowym elementem globalnej strategii zwalczania terroryzmu. Efektywne działania wymagają skoordynowanych wysiłków na wielu frontach, w tym legislacji, technologii, międzynarodowej współpracy i edukacji.

Wprowadzenie i egzekwowanie rygorystycznych przepisów prawnych jest fundamentalne w walce z finansowaniem terroryzmu. Rządy na całym świecie wdrażają przepisy dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT), które wymagają od instytucji finansowych, firm i organizacji pozarządowych ścisłego monitorowania i raportowania podejrzanych transakcji. Organizacje międzynarodowe, takie jak Financial Action Task Force (FATF), opracowują i promują globalne standardy w tej dziedzinie.

Terroryzm jest problemem transnarodowym, dlatego międzynarodowa współpraca jest niezbędna. Kraje współpracują poprzez wymianę informacji wywiadowczych, wspólne operacje policyjne i wspieranie międzynarodowych sankcji finansowych wobec organizacji terrorystycznych i ich sympatyków. Organizacje międzynarodowe, takie jak ONZ i Interpol, odgrywają kluczową rolę w koordynowaniu tych działań.

Zaawansowane technologie analityczne i systemy monitoringu transakcji finansowych pomagają wykrywać podejrzane operacje finansowe. Instytucje finansowe wykorzystują systemy do monitorowania przepływów pieniędzy, które mogą być związane z finansowaniem terroryzmu, a także raportują nietypowe transakcje do odpowiednich władz. Wykorzystanie sztucznej inteligencji i analizy big data zwiększają skuteczność tych narzędzi.

Kryptowaluty, ze względu na swoją anonimowość, stanowią wyzwanie dla tradycyjnych metod monitorowania finansowania terroryzmu. Wiele krajów i organizacji międzynarodowych wprowadza regulacje dotyczące giełd kryptowalut i portfeli cyfrowych, aby zapewnić większą przejrzystość

[45] *Zwalczanie finansowania terroryzmu*, https://help.revolut.com/pl-PL/business/help/more/security-and-personal-data/what-is-terrorism-financing/, [dostęp: 16.05.2025].

[46] C. Sońta, G. Szczuciński, *Wybrane zagadnienia przeciwdziałania Terroryzmu w Polsce*, Studia Bezpieczeństwa Narodowego, nr 1, 2011, s. 51.

i możliwość śledzenia transakcji. Firmy specjalizujące się w analizie blockchain, takie jak Chainalysis, odgrywają kluczową rolę w identyfikowaniu podejrzanych działań.

Wielu terrorystów korzysta z luk prawnych i słabości ekonomicznych w niektórych krajach. Wsparcie międzynarodowe dla państw o słabszych systemach prawnych i finansowych może pomóc w budowaniu ich zdolności do przeciwdziałania finansowaniu terroryzmu. Inwestycje w rozwój infrastruktury prawnej, szkolenia dla służb oraz wsparcie technologiczne są kluczowe.

Wprowadzanie sankcji finansowych i zamrażanie aktywów osób i organizacji powiązanych z terroryzmem to skuteczne narzędzia przeciwdziałania. Międzynarodowe listy sankcyjne, takie jak te prowadzone przez ONZ i różne państwa, pomagają w identyfikowaniu i blokowaniu zasobów finansowych terrorystów. Zaangażowanie sektora prywatnego, zwłaszcza instytucji finansowych i firm technologicznych, jest kluczowe. Banki, firmy technologiczne i giełdy kryptowalutowe muszą aktywnie uczestniczyć w wykrywaniu i zgłaszaniu podejrzanych transakcji. Publiczno-prywatne partnerstwa mogą znacząco zwiększyć skuteczność działań prewencyjnych.

Walka Unii Europejskiej (UE) z praniem pieniędzy i finansowaniem terroryzmu jest priorytetem w polityce bezpieczeństwa i gospodarczej. UE stosuje złożony system regulacji, nadzoru i współpracy międzynarodowej w celu przeciwdziałania tym zagrożeniom. Unia Europejska wprowadziła szereg dyrektyw dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT). Najważniejsze z nich to:

- Czwarta Dyrektywa AML (2015): Wprowadziła wymogi dotyczące identyfikacji klientów, zgłaszania podejrzanych transakcji i prowadzenia rejestrów beneficjentów rzeczywistych. Ustanowiła centralne rejestry beneficjentów rzeczywistych w państwach członkowskich[47].
- Piąta Dyrektywa AML (2018): Zwiększyła przejrzystość poprzez publiczny dostęp do rejestrów beneficjentów rzeczywistych. Nałożyła nowe obowiązki na giełdy kryptowalut i portfele cyfrowe w zakresie

[47] Dyrektywa 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

AML. Zwiększyła wymogi dotyczące współpracy i wymiany informacji między państwami członkowskimi[48].

- Szósta Dyrektywa AML: Obecnie trwające prace dotyczą regulacji będących częścią tzw. Pakietu AML, w skład, którego wchodzą trzy rozporządzenia (w tym AMLAR i AMLR) oraz tzw. 6 Dyrektywa. Celem 6 Dyrektywy AML ma być przede wszystkim ujednolicenie praktyk państw członkowskich Unii[49].

Jeśli chodzi o normatywne aspekty przeciwdziałania tytułowemu procederowi, należy wskazać, że na polski system prawny wpływ wywarło wiele aktów prawnych o charakterze międzynarodowym[50].

Jednym z pierwszych aktów prawnych, który zobowiązywał Polskę do wprowadzenia penalizacji finansowania terroryzmu, była Międzynarodowa Konwencja o Zwalczaniu Finansowania Terroryzmu[51]. Na podstawie niniejszego aktu prawnego każde Państwo-Strona zobowiązało się do uznania w prawie wewnętrznym finansowania terroryzmu za czyn karalny.

Drugim w tym zakresie aktem prawnym jest także Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu[52].

Kształt polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu wyznaczają przede wszystkim przepisy prawne, zarówno krajowe, jak i Unii Europejskiej (UE). Podstawowym aktem prawnym w tym obszarze jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu

[48] Dyrektywa 2018/843 zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

[49] *Jakie zmiany wprowadzi 6 Dyrektywa AML*, https://www.prawo.pl/podatki/co-zmieni-6-dyrektywa-aml,527059.html, [dostęp: 16.05.2025].

[50] W. Goleński, *Proceder prania pieniędzy – zarys problematyki*, Kontrola Państwowa, nr 4, 2023, s. 107.

[51] Międzynarodowa Konwencja o Zwalczaniu Finansowania Terroryzmu przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r. (Dz. U. z 2004 r. Nr 263, poz. 2620), która to została ratyfikowana za zgodą wyrażoną w Ustawie z dnia 9 stycznia 2003 r. o ratyfikacji Międzynarodowej Konwencji o zwalczaniu finansowania terroryzmu, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych w dniu 9 grudnia 1999 r. (Dz. U. z 2003 r. Nr 44, poz. 374).

[52] Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie dnia 16 maja 2005 r. (Dz. U. z 2008 r. Nr 165, poz. 1028), ratyfikowana za zgodą wyrażoną w ustawie z dnia 27 października 2006 r.

praniu pieniędzy oraz finansowaniu terroryzmu. Ustawa określa zasady i tryb przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu[53]. 13 grudnia 2023 r. Rada i Parlament uzgadniały wspólnie powołanie nowego urzędu ds. przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AMLA). To kluczowe osiągnięcie pakietu dotyczącego przeciwdziałania praniu pieniędzy przedstawionego przez Komisję Europejską w lipcu 2021 r. Nowe przepisy mają chronić obywateli UE i unijny system finansowy przed praniem pieniędzy i finansowaniem terroryzmu. AMLA będzie miał bezpośrednie i pośrednie kompetencje w zakresie nadzoru nad podmiotami zobowiązanymi stwarzającymi największe ryzyko w sektorze finansowym[54].

Doskonały przykład działania w tej materii stanowi realizowana przez ONZ Globalna Strategia Zwalczania Terroryzmu (A/RES/60/288): jest to unikatowy światowy instrument, który umacnia krajowe, regionalne i międzynarodowe wysiłki na rzecz zwalczania terroryzmu. Poprzez jej przyjęcie w drodze konsensusu w 2006 r. wszystkie państwa członkowskie ONZ zgodziły się na wspólne podejście strategiczne i operacyjne do walki z terroryzmem. Globalna Strategia Zwalczania Terroryzmu ONZ składa się z 4 filarów. Są to:

- eliminowanie okoliczności sprzyjających rozprzestrzenianiu się terroryzmu,
- środki na rzecz zapobiegania terroryzmowi i jego zwalczania,
- środki mające na celu zwiększanie skuteczności państw w zapobieganiu terroryzmowi i jego zwalczaniu oraz wzmocnienie roli systemu ONZ w tym zakresie,
- środki mające na celu zapewnienie poszanowania praw człowieka wszystkich osób oraz praworządności jako podstawy walki z terroryzmem.

Przeciwdziałanie finansowaniu terroryzmu wymaga kompleksowych działań. Monitorowanie przepływów finansowych, zamrażanie aktywów podejrzanych podmiotów, a także wdrażanie regulacji przeciwdziałających praniu pieniędzy są kluczowymi elementami w walce z finansowaniem terroryzmu. Skuteczna walka z tym zjawiskiem jest niezbędna dla zapewnienia globalnego bezpieczeństwa i stabilności.

[53] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, (Dz. U. z 2018 r. poz. 723), art. 1.

[54] *Walka UE z praniem pieniędzy i finansowaniem terroryzmu*, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/fight-against-terrorist-financing/timeline/, [dostęp: 16.05.2025].

Walka z praniem pieniędzy i finansowaniem terroryzmu wymaga również ciągłej adaptacji i współpracy na poziomie krajowym, regionalnym i międzynarodowym. Unia Europejska podejmuje liczne kroki w celu wzmocnienia regulacji, nadzoru i współpracy, aby skutecznie przeciwdziałać tym zagrożeniom. Inicjatywy takie jak centralne rejestry beneficjentów rzeczywistych, regulacje dotyczące kryptowalut oraz utworzenie Europejskiego Urzędu ds. Zwalczania Prania Pieniędzy stanowią kluczowe elementy tej strategii. Jednak skuteczność tych działań zależy od konsekwentnego wdrażania i egzekwowania przepisów w państwach członkowskich oraz od zdolności do szybkiej adaptacji do nowych zagrożeń.

Podsumowanie

Współczesny terroryzm to zjawisko złożone, dynamiczne i trudne do jednoznacznego zdefiniowania, zarówno pod względem form działania, jak i mechanizmów finansowania. Organizacje terrorystyczne wykazują się dużą elastycznością i zdolnością adaptacji do zmieniających się warunków geopolitycznych, technologicznych i społecznych. Wykorzystują zarówno konwencjonalne formy przemocy, jak i nowoczesne narzędzia, takie jak cyberataki, propaganda internetowa czy transakcje kryptowalutowe, co znacznie utrudnia skuteczne przeciwdziałanie ich działalności. Zróżnicowanie źródeł finansowania – od przestępczości zorganizowanej po legalne podmioty gospodarcze – powoduje, że konieczne staje się tworzenie coraz bardziej kompleksowych i interdyscyplinarnych mechanizmów kontroli oraz współpracy między państwami i instytucjami międzynarodowymi. Skuteczna walka z terroryzmem wymaga integracji działań służb wywiadowczych, instytucji finansowych, podmiotów prywatnych i społeczeństwa obywatelskiego. Wnioski płynące z przeprowadzonej analizy jasno wskazują, że tylko całościowe, skoordynowane podejście – łączące działania prewencyjne, edukacyjne, legislacyjne i technologiczne – może skutecznie ograniczyć potencjał organizacji terrorystycznych oraz minimalizować ryzyko kolejnych zamachów.

Literatura

1. Bąk T., *Oblicza terroryzmu*, Wyd. Konsorcjum Akademickie, Kraków-Rzeszów-Zamość 2011.
2. Bartosz K., *Prawne aspekty walski z terroryzmem*, Security, Economy & Law, Nr 1(XVIII), 2018.
3. Bolechów B., *Terroryzm w świecie podwubiegunowym*, Wydawnictwo Adam Marszałek, Toruń 2003.
4. Conway M., *Terrorist 'Use' of the Internet and Fighting Back*, Information & Security. An International Journal, vol.19, 2006.
5. Dyrektywa 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.
6. Dyrektywa 2018/843 zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.
7. Don B. W. et al., *Network Technologies for Networked Terrorists. Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, RAND Technical Report, 2007.
8. Goleński W., *Proceder prania pieniędzy – zarys problematyki*, Kontrola Państwowa, nr 4, 2023.
9. Hennig R., *Cyberterroryzm miękki. Cz. 1, Internet jako źródło informacji i funduszy*, Przegląd Naukowo-Metodyczny, Edukacja dla bezpieczeństwa, Rok IX, nr 4(29), 2015.
10. Horgan J., *Psychologia terroryzmu*, Wydawnictwo Naukowe PWN, Warszawa 2015.
11. Izak K., Kluczyński M., *Handel Narkotykami jako źródło finansowania terroryzmu*, Przegląd Bezpieczeństwa Wewnętrznego, nr 10, 2014.
12. Karolczak K., *Terroryzm XXI wieku – wybrane aspekty*, Terroryzm – Studia, Analizy, Prewencja 2022, Nr 1(1), 2022.
13. Krupa Ł., *Przeciwdziałanie finansowaniu terroryzmu*, Cybersecurity and Law nr 7, 2022.
14. Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie dnia 16 maja 2005 r. (Dz.U. 2008 nr 165 poz. 1028), ratyfikowana za zgodą wyrażoną w ustawie z dnia 27 października 2006 r.
15. Liedel K., Piasecka P., Aleksandrowicz T., B*ezpieczeństwo w XXI Wieku. Asymetryczny świat*, Wydawnictwo Difin, Warszawa 2011.
16. Lisiecki L., Kucharski K., *Źródła finasowania Al-Kaidy*, Studia bezpieczeństwa narodowego, vol. 4, nr 1, 2013.
17. Lubiewski P., *Reguły i metody działania współczesnych organizacji terrorystycznych*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, Nr 29(4), 2018.

18. Międzynarodowa Konwencja o Zwalczaniu Finansowania Terroryzmu przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r. (Dz.U. 2004 nr 263 poz. 2620), która to została ratyfikowana za zgodą wyrażoną w Ustawie z dnia 9 stycznia 2003 r. o ratyfikacji Międzynarodowej Konwencji o zwalczaniu finansowania terroryzmu, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych w dniu 9 grudnia 1999 r. (Dz.U. 2003 nr 44 poz. 374).
19. Nowacki G., *Zagrożenia terrorystyczne na świecie*, Nierówności Społeczne a Wzrost Gospodarczy, Nr 44, 2015.
20. Nowak P., *Bioterroryzm i chemoterroryzm jako formy współczesnego terroryzmu. Zapobieganie atakom w Rzeczypospolitej Polskiej*, „Kultura Bezpieczeństwa", Nr 36, 2019.
21. Pomianowski P., Maćkowiak E., *Zwalczanie finansowania terroryzmu w świetle prawa obowiązującego w Polsce i we Francji*, Przegląd Bezpieczeństwa Wewnętrznego, nr 6, 2012.
22. Ranstorp M., *The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation,* [w:] J. Eriksson, G. Giacomello (red.), International Relations and Security in the Digital Age, Routledge, London 2007.
23. Sońta C., Szczuciński G., *Wybrane zagadnienia przeciwdziałania finansowaniu terroryzmu w Polsce*, „Studia Bezpieczeństwa Narodowego", nr 1, vol, 1, 2011.
24. Thelesklaf D., Gercke M., *Terrorist Use of the Internet and Legal Response*, F3 – Freedom From Fear Magazine, Issue 7, July 2010.
25. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2018 poz. 723.
26. Wójcik J. W., *Przeciwdziałanie finasowaniu terroryzmu*, Wolters Kluwer, Warszawa 2007.

Netografia

1. *Cyberarmia kalifatu*, https://polska-zbrojna.pl/Mobile/ArticleShow/30080
2. *Globalny atak ransomware WannaCry może być powiązane z grupą cyberprzestępczą Lazarus – komentarz Kaspersky Lab*, https://itreseller.com.pl/globalny-atak-ransomware-wannacry-moze-byc-powiazane-z-grupa-cyberprzestepcza-lazarus-komentarz-kaspersky-lab/
3. *Jakie zmiany wprowadzi 6 Dyrektywa AML*, https://www.prawo.pl/podatki/co-zmieni-6-dyrektywa-aml,527059.html
4. Malik N., *Jak przestępcy i terroryści używają kryptowaluty: i jak to powstrzymać*, Forbes 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/
5. *Najbogatsze organizacje terrorystyczne na świecie*, https://forbes.co.il/rankings/2021terrororganizations/intro/
6. *Prezydent odznaczył zabitego przez talibów geologa*, https://www.prezydent.pl/kancelaria/archiwum/archiwum-bronislawa-komorowskiego/aktualnosci/ordery-i-odznaczenia/prezydent-odznaczyl-zabitego-przez-talibow-geologa,18399
7. *Przeciwdziałanie praniu pieniędzy: Podstawy*, https://www.pibr.org.pl/static/items/publishing/AML_cz.8_Trendy%20w%20przest-opczoCcci.pdf

8. *State sponsors of terrorism*, U.S. Department of State, https://www.state.gov/state-spon-sors-of-terrorism/
9. *Terroryści z milionami na koncie. Skąd Hamas ma pieniądze na wojnę?* https://geekweek.interia.pl/militaria/news-terrorysci-z-milionami-na-koncie-skad-hamas-ma-pieniadze-na-,nId,7085873#google_vignette
10. *The Richest Terror Organizations in the World*, Forbes International, https://www.forbes.com/sites/forbesinternational/2018/01/24/the-richest-terror-organizations-in-the-world/
11. *Walka UE z praniem pieniędzy i finansowaniem terroryzmu*, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/fight-against-terrorist-financing/timeline/
12. *Zamachy w Paryżu. Zorganizowanie ataku kosztuje grosze*, https://www.money.pl/gospodarka/wiadomosci/artykul/zamachy-w-paryzu-zorganizowanie-ataku,187,0,1955003.html
13. *Zwalczanie finansowania terroryzmu*, https://help.revolut.com/pl-PL/business/help/more/security-and-personal-data/what-is-terrorism-financing/
14. *2024 National Strategy for Combating Terrorist and Other Illicit Financing*, Department of the Treasury, 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf