Nowoczesne Systemy Zarządzania
Zeszyt 19 (2024), nr 3 (lipiec-wrzesień)
ISSN 1896-9380, s. 41-64
DOI: 10.37055/nsz/203230

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 19 (2024), No. 3 (July-September)
ISSN 1896-9380, pp. 41-64
DOI: 10.37055/nsz/203230

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Jak wykorzystać modele Markowa na potrzeby przeciwdziałania praniu pieniędzy oraz w walce z terroryzmem? (Część 2)

How to use Markov models for the purposes of counteracting money laundering and in the fight against terrorism? (Part 2)

Maciej Aleksander Kędzierski
Radca prawny, Okręgowa Izba Radców Prawnych, Warszawa, Polska
sulawezi.mk@onet.eu; ORCID: 0000-0003-3074-1355

Abstrakt.
Cel badań i hipotezy/pytania badawcze
Przyjęto założenie, że przedmiotowe rozwiązanie, korzystające z uniwersalnej metody HMM, pozwala na jej zastosowanie w IO wobec potrzeby wyłonienia z wielości cechowanych danych – metadanych – wzorców postępowania określonych jako „negatywny impuls" (anomalia kierunkowa).
Metody badawcze
Dokonanie przeglądu dotychczasowych badań nad problematyką HMM i możliwości wdrożenia tej metody na potrzeby walki z przestępczością, w tym na rzecz walki z praniem pieniędzy i terroryzmem.
Główne wyniki
W związku z brakiem pozyskiwania bezpośrednich danych o działaniach terrorystycznych, ich niekompletności oraz potrzeby przewidywania możliwości powstania zdarzeń godzących w bezpieczeństwo publiczne czy finansowe istnieje potrzeba budowania wiedzy o terrorystach na podstawie danych niezwiązanych bezpośrednio z tym rodzajem przestępczości (jako pośrednie wyniki obserwacyjne). Ma to też swoje przełożenie na tworzenie zbiorów uczących dla matematycznych modeli przeciwdziałania. W konsekwencji prowadzenie badań opartych na niskiej liczbie danych i dostępnych w większych przedziałach czasowych może dawać nieadekwatne wyniki. Ponadto zastosowanie podejścia probabilistycznego stwarza możliwości projektowania przeciwdziałań wobec typowanych negatywnych zachowań.
Implikacje dla teorii i praktyki
Możliwości zastosowania matematycznych modeli przeciwdziałania w zakresie prowadzenia analizy rozpoznania przez instytucje obowiązane oraz na potrzeby prowadzenia czynności analitycznych w ramach stosowania analizy kryminalnej w służbach policyjnych i specjalnych.
Słowa kluczowe: finansowanie terroryzmu, pranie pieniędzy, ukryte modele Markowa, ukryty stan (ukryty model), proces rozpoznania anomalii

Abstract.
Research objectives and hypothesis/research questions
The assumption is that the solution in question, using the universal HMM method, allows its application in IO, in view of the need to select from the multitude of characterized data – metadata – patterns of conduct defined as a "negative impulse" (directional anomaly).
Research methods
Reviewing the existing research on HMM issues and the possibilities of implementing this method for the purposes of combating crime, including money laundering and terrorism.
Main results
Due to the lack of obtaining direct data on terrorist activities, their incompleteness and the need to predict the possibility of events that threaten public or financial security – there is a need to build knowledge about terrorists based on data not directly related to this type of crime (as indirect observational results). This also translates into the creation of training sets for mathematical models of counteracting. As a consequence, conducting research based on a small amount of data and available in larger time intervals may give inadequate results. In addition, the use of a probabilistic approach creates opportunities to design counteracting typified negative behaviors.
Implications for theory and practice
The possibility of using mathematical models of counteraction in the scope of conducting reconnaissance analysis by obligated institutions and for the purposes of conducting analytical activities as part of the application of criminal analysis in the police and special services.
Keywords: financing terrorism, money laundering, Hidden Markov Models (HMM), hidden state (hidden model), anomaly recognition process

Wprowadzenie

W części drugiej artykułu, w odróżnieniu od pierwszej, zaprezentowano wykorzystanie metody ukrytego modelu Markowa (dalej jako: HMM) w charakterze instrumentu do ujawniania ukrytych (grup) sprawców przestępstw prania pieniędzy do identyfikacji ryzyka/zagrożenia oraz ujawniania potencjalnych terrorystów poza systemem AML/CFT. Za przedmiot oceny przyjęto pewne symptomatyczne zachowania, których analiza pozwala zidentyfikować zagrożenie ML/FT, mające wpływ nie tylko na jego identyfikację, lecz także na możliwość włączenia w skalę ocenną instrumentów stosowanych w identyfikacji finansowej związanej z zachowaniem potencjalnego klienta i transakcji w systemie AML/CFT. Co istotne, zasobem danych do określenia zagrożenia i wykorzystania HMM są zwłaszcza dane niegenerowane z systemu AML/CFT, lecz z zachowań „zewnętrznych", identyfikowalnych w strukturach zarządczych sklasyfikowanych finansowo, społecznie i fizycznie. Dane te mogą dotyczyć zarówno generowania środków pochodzących z przestępstw pierwotnych wobec ML/FT, jak i z czynności sprawczych identyfikowanych jako fizyczne zachowania kryminalne. Nadal istotą pomocniczego zastosowania metody HMM pozostaje potrzeba „ujawnienia" powiązań między analizowanymi elementami przy braku pełnej wiedzy na temat wszystkich relacji pomiędzy podmiotami przestępczego procederu.

1. HMM jako instrument do ujawniania ukrytych (grup) sprawców przestępstw prania pieniędzy

Yuhua Li, Dongsheng Duan, Guanghao Hu oraz Zhengding Lu, opierając się na ukrytym modelu Markowa (ang. Hidden Markov Model, HMM), uznają, że przestępstwa finansowe, takie jak pranie pieniędzy, są często popełniane przez współpracujące osoby w ukryty sposób. Wskazali, że odkrycie tych grup w sieciach transakcji finansowych może pomóc także w znalezieniu osób podejrzanych o pranie pieniędzy (Li, Duan, Hu, Lu, 2009). Przedstawiono metodę „odkrywania" grupy ukrytej opartą na ukrytym modelu Markowa i algorytmie genetycznym. Ten algorytm genetyczny to rodzaj algorytmu przeszukującego przestrzeń alternatywnych rozwiązań problemu w celu wyszukania najlepszych rozwiązań. W tym przypadku HMM posłużył do opisu sieci transakcji finansowych, które wyrażono na podstawie przetworzonych prawdziwych danych. Przyjęto zasadę największej wiarygodności, aby przekształcić wykrywanie grup ukrytych w problem optymalizacji kombinacyjnej. Autorzy opracowali algorytm genetyczny umożliwiający rozwiązanie problemu optymalizacyjnego opartego na charakterystyce możliwych rozwiązań. Pewne dane dotyczące transakcji finansowych zostały wstępnie przetworzone z uwzględnieniem wielu relacji między rachunkami. Przyjęto, że sieci finansowe są określane jako ważone wykresy, w których węzły reprezentują konta, krawędzie – transakcje między rachunkami, a wagi krawędzi – częstotliwość lub intensywność transakcji (określenia pochodzą z teorii grafów). Skuteczność i wydajność tej metody została potwierdzona eksperymentami przeprowadzanymi zarówno na syntetycznym, jak i rzeczywistym zbiorze danych. W ramach prac przyjęto pewne założenia:

- konta w sieci finansowej mogą należeć do jednej grupy lub większej liczby grup;
- konta w tej samej grupie mają tendencję do relacji handlowych częściej niż pomiędzy różnymi (innymi) grupami. Im więcej grup jest wspólnych dla dwóch kont, tym częściej mogą ze sobą wchodzić w tego typu relacje;
- istnieje transmisja pomiędzy ukrytą grupą członków i jest to istotna cecha różniąca się od funkcjonowania normalnych grup;
- struktura grupy zmienia się w czasie, jako struktura grupy w następnym kroku czasowym *t+1* jest wyłącznie regulowana przez *1* w momencie kroku *t* z prawdopodobieństwem $P(G_{(t+1)} \mid G_{(t)})$, czyli tworzy łańcuch Markowa;
- macierz transakcji $I_{(t)}$, która wskazuje, kto handluje z kim i z jaką intensywnością, regulowana jest przez obecną strukturę grupy z prawdopodobieństwem $P(I_{(t)} \mid G_{(t)}, \boldsymbol{\lambda})$.

Wprowadzenie algorytmu genetycznego miało na celu rozwiązanie niektórych skomplikowanych problemów optymalizacyjnych, szczególnie na okoliczność, gdy nie będzie można łatwo obliczyć współczynnika różniczkowego funkcji celu. W prezentowanym modelu stwierdzono jednak, że gdy rozmiar sieci wzrośnie, model ten w dużym stopniu stanie się mniej skuteczny.

Wydaje się, że w przypadku tego badania istotne było przyjęcie założenia krótkiego odcinka czasowego, co przekładało się na niezmienność struktury grupy w czasie oraz ocenę jej działania na stosunkowo niewielkiej liczbie kont. Autorzy zauważyli, że im operowanie relacjami odbywa się na „większej liczbie rachunków", tym samym wzrasta problem ujęcia całości relacji, stąd potrzeba doskonalenia modelu.

Jednym ze sposobów interpretacji zachowań użytkowników-sprawców może być ocena zachowań klientów oparta na użyciu kart płatniczych. Instytucje obowiązane (dalej jako: IO) umożliwiają korzystanie ze zdeponowanych środków na kontach bankowych przez przydzielanie usługi korzystania z kart płatniczych/bankomatowych. Obserwowanie zachowań klientów, jeżeli chodzi o karty kredytowe, może prowadzić zarówno do wykrycia procederu ML/FT, jak i do ujawnienia przestępstw „źródłowych" prania pieniędzy (czynów zabronionych) czy finansowania terroryzmu (czynów pierwotnych). Dochodzi do tego wówczas, gdy źródłem aktywów pozyskiwanych w celu ich legalizacji lub dostarczenia dla beneficjentów terrorystycznych są czyny zabronione.

Posługiwanie się kartą płatniczą to kolejny obszar, który jest poddawany badaniu w celu opracowania charakterystycznego wzorca użytkowania kart oraz opisu korzystania z konta przez użytkownika. W tym zakresie jest również możliwe zastosowanie metody HMM. Zagadnieniem tym zajmowali się Vidhya Bhusari i Suhani Patil (2011, s. 204). Skorzystanie z metody HMM miało na celu analizę profilu wydatków z każdej karty posiadacza środków oraz wykrycie wszelkich rozbieżności w schematach wydatków. Można więc odkryć oszustwo na podstawie analizy danych dotyczących poprzednich transakcji (jako wyjściowego wzorca porównawczego), co pomaga w ustaleniu profilu wydatków z karty. Każda karta posiada unikalny wzór zawierający informacje o liczbie i datach transakcji, szczegółach dotyczących zakupionych przedmiotów oraz inne informacje handlowe (Bhusari, Patil, 2011, s. 204). HMM nie wymaga podpisów sprawców-oszustów, a mimo to jest w stanie wykryć oszustwa samą „pamięcią" o nawyku wydawania pieniędzy przez posiadacza karty. Ważną zaletą podejścia opartego na HMM jest ekstremalny spadek liczby transakcji fałszywie pozytywnych, uznawanych za złośliwe jako wykrywane oszustwo, mimo że są one rzeczywiście autentyczne.

W celu wykrycia oszustw autorzy brali pod uwagę trzy różne profile wydatków posiadacza karty, tj. w zależności od przedziału kwotowego, nazywane wysokim (h, ≥ 500 USD), średnim (m, 100-500 USD) i niskim (l, 0-100 USD). Po sfinalizowaniu stanu i reprezentacji symboli następnym krokiem było określenie różnych

komponentów HMM, tj. macierzy prawdopodobieństwa A, B i π, tak aby znane były wszystkie parametry wymagane dla HMM. Początkowy wybór parametrów wpływa na wydajność stosowanego algorytmu i dlatego też konieczne stało się staranne dobranie wszystkich tych parametrów. HMM początkowo sprawdza, czy nadchodząca transakcja jest fałszywa, czy nie. Podejmuje także decyzję o dodaniu nowej nadchodzącej transakcji do istniejącej sekwencji lub nie, co będzie zależeć od procentowej zmiany prawdopodobieństw starego i nowego ciągu. Następnie decyduje, czy ta transakcja jest prawdziwa, czy oszukańcza, w zależności od wartości progowych. Istotne jest również przyjęcie losowego zbioru danych wszystkich transakcji, które się wydarzyły i które zostały podzielone na kategorie według rodzajów zakupów. Za pomocą tego modelu można obliczyć prawdopodobieństwo każdego profilu wydatków.

W przyjętym modelu skategoryzowano także różne rodzaje przedmiotów i usług, takich jak restauracja, płatności rachunków, płatności za bilety, media, płatności za usługi elektroniczne itp. Te różne kategorie zostały uznane za trzy różne stany HMM (trzy różne profile wydatków posiadacza karty). W każdej kategorii płatności podzielone zostały na trzy dalsze grupy oparte na różnych zakresach kwot transakcji: wysoką, średnią i niską. Grupy te uznano za obserwacyjne i nadano im określoną symbolikę. Technika ta pomaga poznać zwyczaje posiadaczy kart związane z wydawaniem pieniędzy w ramach zakupu różnych przedmiotów (płacenie rachunków, wydatki w restauracji czy nabycie artykułów elektronicznych). Najważniejszym zastosowaniem tej techniki stało się podejmowanie decyzji, ustalenie wartości początkowej symboli obserwacji, prawdopodobieństwo stanów przejściowych i wstępne oszacowanie parametrów modelu (Bhusari, Patil, 2011, s. 210). Po określeniu parametrów HMM ustalane jest utworzenie początkowej sekwencji istniejącego zachowania posiadacza karty w zakresie prowadzonych wydatków. Sekwencja umieszczona w modelu HMM oblicza prawdopodobieństwo akceptacji (sekwencja w czasie $t+1$, gdy transakcja ma zostać przetworzona). HMM bierze pod uwagę nową sekwencję $OR+1$ z niskim prawdopodobieństwem, a zatem ta transakcja zostanie uznana za transakcję oszustwa wtedy i tylko wtedy, gdy procentowa zmiana prawdopodobieństwa jest większa niż wstępnie zdefiniowana wartość progowa, którą można obliczyć empirycznie. System wykrywania ustalił (odkrył) rozkład średniego prawdopodobieństwa fałszywych i prawdziwych transakcji. W przypadku gdy transakcja zostanie określona jako fałszywa, zostanie odrzucona, a gdy jako „prawdziwa", zostanie włączona do zbioru uczącego i będzie brana pod uwagę w przyszłości w celu wykrywania oszustw. Czy decyzja o dodaniu nowej nadchodzącej transakcji do istniejącej sekwencji nie będzie zależała od procentowej zmiany prawdopodobieństwa starej i nowej sekwencji? Tym samym czy gdy maleje prawdopodobieństwo prawdziwej transakcji, odpowiednio wzrasta prawdopodobieństwo fałszywej transakcji i odwrotnie? Jeżeli procent zmiany prawdopodobieństwa fałszywej transakcji będzie większy niż wartość progowa, wówczas nastąpi alarm w związku z nieuczciwą transakcją.

Przedstawione podejście umożliwia uzyskanie wiedzy o „podejrzanej transakcji" z użyciem karty. Tym samym jako podejście predykcyjne umożliwi jego identyfikację jeszcze przed procederem zalegalizowania środków w schematach kartowych usług i produktów oferowanych przez instytucję obowiązaną (dalej jako: IO). Ponadto pozwoli ono na w miarę szybkie zidentyfikowanie „zdarzenia", które będzie można ocenić w ramach analizy rozpoznania, czy nie stanowi ono źródła aktywów z czynu zabronionego mającego posłużyć innej celowościowej działalności beneficjenta terrorystycznego. W przypadku zastosowania modelu HMM efektem może być zidentyfikowanie podejrzanego zdarzenia (np. oszustwa) oraz zapobiegnięcie jego konsekwencjom nie tylko jako działaniu na szkodę innego klienta czy IO, lecz także przekształceniu wygenerowanych wobec jego zaistnienia środków w przedmiot procederu prania pieniędzy/finansowania terroryzmu. Przyjęte rozwiązanie może służyć nie tylko identyfikowaniu oszustw. Ze względu na prowadzoną analizę z użyciem HMM niskich kwot może posłużyć także rozpoznawaniu zachowań osób wspierających finansowo działania terrorystyczne, m.in. w zakresie finansowania społecznościowego, drobnych datków na eksponowane konta internetowe, organizacji internetowych zbiórek pieniężnych czy zarządzania własnym kontem w czasie przygotowania się indywidualnego sprawcy do aktu terrorystycznego. Tego typu zachowania pozostają rozpoznawalne wobec wspierania finansowego terroryzmu przez tzw. akolitów/kibiców terrorystycznych oraz osoby pozostające w nieświadomej nieumyślności dokonywania przestępstwa finansowania terroryzmu. Cechą wspólną pozostają niskie kwoty zasileń oraz zarządzania niskimi aktywami na rzecz beneficjentów terrorystycznych. Dlatego też w przyszłości ten rodzaj badania mógłby posłużyć także do zidentyfikowania nie tylko źródeł przestępczych finansowania terroryzmu, lecz również na potrzeby identyfikacji zachowań sprawców w tzw. obszarach legalnego wspierania tego typu niezgodnej z prawem działalności.

2. Model Markowa jako narzędzie do identyfikacji ryzyka/zagrożenia

Jednym z charakterystycznych elementów zdarzenia o charakterze terrorystycznym jest dokonanie go – na potrzeby realizacji celu, tj. poważnego zastraszenia wielu osób – w miejscu publicznym. W konsekwencji organy odpowiedzialne za przeciwdziałanie zagrożeniu stosują różne metody, zwłaszcza fizycznego monitorowania skupisk ludzkich wytypowanych jako najbardziej narażone na zamach terrorystyczny. Tym samym powstaje problem przewidywalności tego typu zdarzeń w przestrzeni publicznej. Dlatego też innym rodzajem wykorzystania omawianej metody jest przyjęcie HMM, które będzie opierać się na założeniu, że poziom zagrożenia można uznać za stan ukryty (nieobserwowalny).

Innymi słowy, ukryty proces w proponowanym HMM reprezentuje poziom zagrożenia sytuacją, która nas interesuje na potrzeby oszacowania jej skali zagrożenia bezpieczeństwa. Przy czym uważa się, że proces obserwacji składa się z czynników, które wpływają na poziom zagrożenia sytuacji, takiej jak zaobserwowane podejrzane zachowania i działania (Theodosiadou, Chatzakou, Tsikrika, Vrochidis et al., 2023, s. 3-4). Probabilistyczne podejście stosuje się w tym przypadku do szacowania fizycznego zagrożenia mogącego nastąpić w przestrzeni publicznej. Aby wydobyć jak najwięcej wartościowych informacji, należy rozważyć wiele procesów automatycznej analizy wizualnej, a mianowicie wykrywanie obiektów, rozpoznawanie twarzy, rozpoznawanie aktywności i wykrywanie przemocy w tłumie, co pozwala na skuteczne zobrazowanie (z punktu widzenia bezpieczeństwa) ogólnej sytuacji podczas wydarzenia. W tym przypadku HMM zostało wykorzystane do oceny poziomu zagrożenia związanego z terroryzmem w sytuacjach takich jak wydarzenia publiczne. Podejście uwzględnia ryzyko jako zmienną ukrytą i zapewnia okresowe szacowanie go za pomocą HMM. Celem pracy O. Theodosiadou, D. Chatzakou, T. Tsikrika, S. Vrochidis i innych było pokazanie możliwości zastosowania modelu przedstawiającego ocenę poziomu zagrożenia związanego z terroryzmem w wydarzeniach publicznych na podstawie wyników kilku komponentów analizy wizualnej, które automatycznie przetwarzają treść wizualną uzyskaną z kamer monitoringu. W prezentowanym stanowisku poziom zagrożenia sytuacji uważany jest za stan ukryty, a proces ukryty reprezentuje poziom zagrożenia sytuacji, który można oszacować („ujawniony") przez sekwencję obserwacji. Przy czym przestrzeń stanów proponowanego HMM do oceny zagrożenia w sytuacji jest oznaczona jako $S = \{S_1, S_2, \ldots, S_n\}$. Jako gradację przyjęto liczbę poziomów zagrożenia, która wynosi $n = 3$. Są to:

- niski (L – *low*): atak jest mało prawdopodobny;
- umiarkowany (M – *moderate*): atak jest prawdopodobny;
- wysoki (H – *high*): atak jest wysoce prawdopodobny.

Wobec powyższego przestrzeń stanów proponowanego HMM jest zdefiniowana jako $S = \{S_1, S_2, S_3\} = \{L, M, H\}$ *i* Xt, $t = 1, \ldots$, T oznacza stan ukryty w chwili t, odpowiadający poziomowi zagrożenia. Ponadto stany komunikują się ze sobą, co oznacza, że istnieją niezerowe prawdopodobieństwa przejścia między zdefiniowanymi poziomami zagrożenia. Model HMM stosowany w celu oszacowania poziomu zagrożenia może obejmować czynniki ryzyka, które, jak się zakłada, wpływają na stan bezpieczeństwa sytuacji, takich jak wykrycia podejrzanych incydentów/ruchów na podstawie kamer/czujników [stany obserwacji w danym czasie: $O_t = (O_{t,1}, O_{t,2}, \ldots, O_{t,k})$]. Przyjęto szesnaście różnych wektorów obserwacji opartych na czterech analizach wizualnych procesów (np. sygnał z kamer monitorujących, dobór wektorów obserwacji musi być adekwatny do możliwości pozyskania danych, dane z nadzoru nie są zazwyczaj publicznie dostępne).

Obserwacje są rejestrowane w dyskretnych krokach czasowych przez jedną kamerę monitorującą lub więcej kamer monitorujących (czujników) i wyodrębniane na podstawie następujących procesów:

- wykrywania obiektów, które koncentrują się na identyfikowaniu i lokalizowaniu wstępnie zdefiniowanego zestawu obiektów interesujących;
- rozpoznawania twarzy;
- rozpoznawania aktywności, które obejmują rozpoznawanie działań będących przedmiotem zainteresowania, wykonywanych na przykład przez ludzi i pojazdy;
- wykrywania przemocy tłumu, która koncentruje się na wykrywaniu wybuchów przemocy tłumu.

W odniesieniu do procesu wykrywania obiektów w tym konkretnym badaniu wskazano obiekty, które mogą być interesujące (w zależności od kontekstu): noże, broń palna, plecaki, butelki itp. (mające wpływ na status bezpieczeństwa obiekty, którym będzie można przypisać określoną wagę). Jeśli chodzi o proces rozpoznawania „aktywności", które mogą wskazywać na podejrzane czyny, gdy są wykonywane w określonym kontekście, może on obejmować na przykład „osobę szybko idącą", „osobę wychodzącą z budynku z nielegalnego wejścia", „osobę prowadzącą niebezpiecznie". Podejścia pozwalają na dynamiczną estymację poziomu zagrożenia w czasie, ponieważ w obliczeniach uwzględnia się także wcześniejsze oceny obserwacji zagrożenia na każdym etapie. W dyskretnym czasie t zakłada się, że ukryty proces Markowa Xt poziomu zagrożenia znajduje się w pewnym stanie, a obserwacja Ot jest generowana zgodnie z macierzą prawdopodobieństwa emisji B. Następnie ukryty proces zmienia swój stan na podstawie macierzy prawdopodobieństwa przejścia A. Parametry A, B i π można oszacować za pomocą algorytmu Bauma–Welcha na podstawie danych historycznych, które składają się z sekwencji poziomów zagrożenia dotyczących sytuacji spowodowanej przez sekwencję obserwacji. Oczekuje się, że wynik proponowanego HMM będzie najbardziej prawdopodobnym ukrytym poziomem zagrożenia w czasie t, warunkowym od sekwencji obserwacji do czasu (prawdopodobieństwo liczone jest w każdym kroku czasowym). Dynamiczna ewolucja poziomu zagrożenia w czasie jest „ujawniana", ponieważ oszacowanie ukrytego stanu w czasie t zależy od wcześniejszych obserwacji. Skutkuje to dostarczeniem skali oceny zagrożenia w każdym czasie na podstawie przyjętych procesów obserwacji. Model HMM przyjmuje podejście probabilistyczne w ocenie zagrożenia i skutkuje „ujawnieniem" dynamicznej ewolucji zagrożenia w czasie, a także zapewnia skalę oceny stanu bezpieczeństwa w każdym momencie. Tym samym model ten może zostać wykorzystany do oceny zagrożenia w przypadkach, gdy proces obserwacji jest zakłócony i istnieją niezerowe prawdopodobieństwa fałszywie pozytywnych/negatywnych wyników. Oceny zagrożeń mogą okazać się znacznie bardziej przydatne we wspomaganiu procesu podejmowania decyzji przez personel ochrony w zakresie podjęcia środków zapobiegawczych w przypadku, gdy poziom zagrożenia wydaje

się rosnąć, nawet zanim osiągnie najwyższy poziom (Theodosiadou, Chatzakou, Tsikrika, Vrochidis et al., 2023, s. 9; Theodosiadou, Pantelidou, Bastas et al., 2021). Przedmiotowe rozwiązanie pozwala na przyjęcie go na potrzeby typowania zagrożenia aktem terrorystycznym w miejscach zagrożenia, ale także tych, które mogą być poddane bieżącej obserwacji ze strony równego rodzaju czynników.

Analiza siatek przestępczych wiąże się z poważnymi wyzwaniami, przed którymi stoją organy ścigania, szczególnie w zakresie prognozowania przestępczości. Informacje dotyczące spraw karnych prowadzonych odnośnie do poszczególnych elementów sieci (sklasyfikowanych jako sprawcy, potencjalni sprawcy) nie są łatwo dostępne publicznie ze względu na ich tajny charakter. Bezpośrednią konsekwencją może być to, iż brak jest pożądanych informacji i zbiorów danych potrzebnych do przeprowadzenia analizy kryminalnej. Podstawowym założeniem HMM zastosowanym w tym kontekście jest to, że przyszły atak jakiegokolwiek elementu przestępczego jest niezależny od przeszłych ataków, biorąc pod uwagę obecne działania. Mathew E. Nwanga, Kennedy Ch. Okafor, Ifeyinwa E. Achumba i Gloria A. Chukwudebe przeprowadzili prace badawcze w tym zakresie (Nwanga, Okafor, Achumba, Chukwudebe, 2022, s. 231-254). Studium przypadku użycia scenariusza dotyczy ataków terrorystycznych sieci ekstremistów Boko Haram i Fulani w Nigerii w latach 2010-2016. Optymalizacja Bauma–Welcha została zastosowana w tych badaniach w celu poprawy jakości analizy informacji i dokładności predykcyjnej działalności elementów przestępczych. Optymalizacja polegała na tym, że w HMM istnieje problem uczenia się parametrów (tj. prawdopodobieństw przejścia i emisji). Dlatego HMM musi zostać przeszkolony. Algorytm Bauma–Welcha to algorytm optymalizacyjny, który umożliwia szkolenie obu parametrów. Działa w formie maksymalizacji oczekiwań i jako algorytm iteracyjny oblicza wstępne oszacowanie prawdopodobieństw, a następnie wykorzystuje te szacunki do obliczenia lepszego oszacowania, w ten sposób iteracyjnie zwiększając prawdopodobieństwo, a tym samym się ucząc (Nwanga, Okafor, Achumba, Chukwudebe, 2022, s. 248).

Autorzy skupili się na nieliniowej analizie szeregów czasowych i teorii sieci złożonych na sieciach rekurencyjnych w przestrzeni fazowej, wykresach (grafach) widoczności (ang. *visibility graph*) i przejściu opartym na łańcuchach Markowa. Przy czym graf jest grafem niewidocznych lokalizacji, zwykle dla zbioru punktów i przeszkód na płaszczyźnie euklidesowej. Każdy węzeł na wykresie reprezentuje położenie punktu, a każda krawędź reprezentuje widoczne połączenie między nimi. Wzięto pod uwagę zwłaszcza „ukryte linki" pomiędzy elementami sieci, tak aby można było przewidywać relacje w ramach wewnętrznej komunikacji (przywódca – wykonawcy). Wobec dokonywanych ataków przyjęto siłę ukrytych elementów i uznano to za spójny ślad i działanie zależności. Założenie HMM jest takie, że stany (S) są ukryte, ale w każdym punkcie czasu stany emitują pewne obserwowalne symbole v z pewnymi prawdopodobieństwami. Zatem v jest widoczne. Prawdopodobieństwo tych emisji zależy wyłącznie od stwierdzonego instrumentu bazowego.

Samo badanie związane było z ustaleniem „aktywności" od dowódcy, przez ogniwo pośrednie, po wykonawcę w jednostce czasowej oraz z uwzględnieniem częstotliwości przewidywanej komunikacji. Stwierdzono, że zarówno dowódca, jak i wykonawca wobec projektowanego ataku mają podobną aktywną komunikację wewnętrzną (ang. *active internal communication*, AIC). Bardzo istotne było, aby mieć na uwadze to, że ataki w ramach sieci przestępczej poprzedzają AIC. Atak i AIC nie odbywają się w tym samym czasie (różnica trzech nocy była najbardziej prawdopodobna) (Nwanga, Okafor, Achumba, Chukwudebe, 2022, s. 251).

3. HMM jako metoda identyfikacji terrorystów

Podstawowym założeniem zastosowania HMM na potrzeby identyfikacji zagrożeń (w tym tych o charakterze terrorystycznym) jest to, że wobec wielości danych dotyczących różnych rodzajów informacji odnoszących się do zdarzeń terrorystycznych możliwe jest wyekstrahowanie takich, które będą mogły cechować odpowiednio stany na potrzeby ich analizowania. Z drugiej strony wiedza pozyskiwana w sposób wewnętrzny i zewnętrzny (wobec agenta analitycznego) nigdy nie będzie do końca pełna, ale jest niezbędna na potrzeby realizowania kontrdziałań, aby neutralizować podmioty terrorystyczne oraz zapobiegać eskalacji i zamachom terrorystycznym. Dlatego też przy występowaniu luk co do źródeł informacji, a tym samym wiedzy niezbędne staje się tworzenie modeli probabilistycznych, które mogłyby wspierać decydentów co do zarządzania bezpieczeństwem w omawianym obszarze. Ponadto należałoby zauważyć, że obszar aktywności finansowania działalności terrorystycznej staje się bardziej wrażliwy i nieprzewidywalny liniowo wobec np. przestępstw prania pieniędzy. W zakresie zagrożenia terrorystycznego decydenci starają się przede wszystkim działać prewencyjnie, nie dopuszczać do zdarzeń terrorystycznych. Z kolei w zakresie prania pieniędzy mamy do czynienia z sytuacją, w której sprawcy już dokonali czynu zabronionego, a ich celem jest *post factum* „zalegalizowanie" tym sposobem pozyskanych aktywów. A więc konsekwentnie w tym zakresie prewencja staje się mniej widoczna.

Do zagadnienia związanego z przeciwdziałaniem terroryzmowi można podejść przynajmniej na dwa sposoby. Pierwsze podejście związane jest z postdziałaniami wobec zaistniałego zdarzenia terrorystycznego (np. w postaci śledztwa powybuchowego) lub z przeddziałaniami (prewencyjnymi/zapobiegawczymi) wobec możliwych zdarzeń o charakterze terrorystycznym (np. w zakresie rozpoznawania źródeł finansowania zamachów).

Drugie podejście wymaga znalezienia sposobów na śledzenie aktywności terrorystycznej i wnioskowanie o następnych posunięciach taktycznych sprawców. Jeżeli tak, to muszą powstać mechanizmy, które pozwolą na ocenę predykcyjną zachowań terrorystów na podstawie aktualnej wiedzy oraz danych historycznych

i pozainstytucjonalnych umieszczonych w *open source*. Śledzenie aktywności grup terrorystycznych pozwala na ocenę ich dynamiki wykonawczej lub interwykonawczej nie tylko wobec potrzeby oceny przewidywalności zamachów, lecz również przygotowywania się do nich łącznie z kwestiami logistycznymi i finansowymi. Wobec takich wyzwań najbardziej umiędzynarodowione, ale także lokalnie identyfikowalne (ze względu na miejsce zagrożenia) i zawierające jak najwięcej szczegółów dane pozwalają na otrzymywanie modeli predykcyjnych postępowania sprawców. Mając na uwadze to, że bieżące śledzenie symptomów związanych z podejrzeniem finansowania terroryzmu jest znacznie utrudnione, podejście oparte na modelowaniu predykcyjnym daje szanse na celowe i ujęte we właściwym czasie zintensyfikowanie działań ocennych i analitycznych, do których zobowiązane są między innymi IO.

Ważnym elementem ustaleniowym byłoby wykazanie, czy zróżnicowane pod względem celów grupy terrorystyczne mają określone cechy wspólne co do przyjmowania taktyki, sposobów przygotowania zamachów czy budowania zaplecza dla swojego funkcjonowania. Oprócz gromadzenia danych opartych na monitoringu finansowym i operacyjnym czy ustaleń z prowadzonych postępowań należy mieć na uwadze to, iż pozostaje obszar niewiedzy (utajony) dotyczący funkcjonalności grup terrorystycznych (np. w sensie organizacyjnym, taktycznym i planowania aktów terroru). A ponadto pozostaje istotne to, jak podejść do kwestii przyznania się podmiotu X do autorstwa danego zamachu, gdy nie ma pewności, że informacja ta nie została świadomie wprowadzona jako fałszywa pod tą egidą (fałszywą flagą) do przestrzeni publicznej. W celu rozwiązywania tego typu problemów podjęto próby budowy modeli analitycznych, np. TAR (ang. Threshold Auto-Regressive, model progowej autoregresji) stanowi przykład nieliniowego modelu regresji, w którym parametry zmieniają swoje wartości w zależności od stanu, w jakim znajduje się model, czy SEHM (ang. Self-Exciting Hurdle Model, samopobudzający model płotków). Zagadnienie dotyczy tzw. procesów Hawkesa (uogólnione, słowniczek, pkt 7), które są znakowanymi procesami punktowymi mającymi własność: samopobudzania (ang. *self-excitation*) (samowzbudzający się proces punktowy). Proces Hawkesa to proces obliczeniowy, który modeluje sekwencję „przybyć" pewnego typu w czasie, np. trzęsień ziemi, przemocy gangów, zleceń handlowych lub niewypłacalności banków. Każde przybycie pobudza proces w tym sensie, że szansa na kolejne przybycie wzrasta przez pewien okres po pierwotnym przybyciu. Własność ta przejawia się tym, że intensywność procesu ma dodatni skok w momentach pojawienia się zdarzeń, czyli można to interpretować tak: pojawianie się zdarzeń zwiększa szanse wystąpienia kolejnych w przyszłości. Komponent samowzbudzający określa, że prawdopodobieństwo zdarzenia jest funkcją czasu (i ewentualnie innych aspektów) wszystkich poprzednich zdarzeń, tak więc wpływ na prawdopodobieństwo maleje z czasem (Hawkes, 1971). Może to pomóc wyjaśnić klasteryzującą i dynamiczną naturę terroryzmu. Należy jednak, przy interpretacji wyników, mieć na uwadze to, że w przypadku małych (prostych) próbek estymator generuje znaczące odchylenie,

napotyka wiele lokalnych optimów i jest bardzo wrażliwy na wybór funkcji wzbudzenia, natomiast w przypadku wysokiej złożoności metoda okaże się bezużyteczna, gdy próbki staną się tak duże, że każda iteracyjna w procedurze optymalizacji obliczyłaby funkcję wiarygodności być może tysiące razy (Laub, Taimre, Pollett, 2015).

Modele badawcze aktywności terrorystycznej mogą być modelami liniowymi lub nieliniowymi. Modele, które zakładają, że podstawowy proces generowania danych jest liniowy, wskazują na to, iż wartość w danym momencie jest liniową kombinacją wartości z przeszłości. Jednakże szeregi czasowe w świecie rzeczywistym wykazują zmienność i nieliniowość – załamanie dotychczasowego trendu czy zmianę taktyki. Stąd też niezwykle ważne jest zbudowanie dynamicznego modelu działalności terrorystycznej. Niestety przeciwnością badań pozostaje rzadkość występowania określonego typu zdarzeń. Badane były modele stanowe (HMM) i autoregresyjne (ARIMA, ang. The Autoregressive Integrated Moving Average, model autoregresyjnej zintegrowanej średniej ruchomej i RARE) do generowania prognoz zdarzeń ze wskaźnikami zewnętrznymi (Hossain, Gao, Kennedy et al., 2020, s. 269-283). Wynikiem tych działań było stwierdzenie, że model HMM i model RARE realizują się całkiem dobrze przy rozsądnej ilości danych (zdarzenia na poziomie sprawcy i kraju), podczas gdy ich wydajność pogarsza się w przypadku zdarzeń rzadkich. Gdy gęstość zdarzeń jest niska, a typ zdarzenia jest rzadki, stanowi to wyzwanie dla proponowanych modeli przewidywania zdarzeń w takich warunkach. Tym samym w razie występowania niskiej gęstości zdarzeń, dla których realizowane są modele HMM i autoregresyjne, te modele wydają się być nieodpowiednie. Aby rozwiązać te problemy, należałoby przyjąć modele predykcyjne, które uwzględniłyby skomplikowany kontekst zdarzenia, biorąc pod uwagę źródła zewnętrzne (Hossain, Gao, Kennedy et al., 2020, s. 282).

Metoda HMM ma też inne zastosowanie, jest wykorzystywana w odkrywaniu obecności grup zbrojnych kojarzonych z aktywnością terrorystyczną. Takie rozwiązanie zaproponował Mauricio V. Baron (2021). W przypadku konfliktu nieobserwowaną zmienną ukrytą jest obecność grupy zbrojnej i możemy założyć, że spełnia ona własność Markowa. Chociaż ta zmienna nie jest obserwowana, można ją wywnioskować z obserwowanych gwałtownych działań grup zbrojnych, np. starcia między grupami zbrojnymi lub między grupą zbrojną a oddziałami reprezentującymi władzę państwową. Modele te mogą wykrywać podstawowe struktury utajone i wykrywać nieobserwowalne stany (również autokorelacje zdarzeń). Korzystanie z modeli HMM ma tę zaletę, że stosuje nie tylko zmienne geolokalizacyjne, lecz także inne zmienne kontekstowe. Jako dane przedmiotowe użyto informacje dotyczące Rewolucyjnych Sił Zbrojnych Kolumbii (FARC) oraz grup paramilitarnych (za lata 1998-2018). Obecność grupy uzbrojonej, *Pt*, można modelować jako stan dyskretny z kilkoma *m* kategoriami, od zerowej obecności grupy uzbrojonej do obecności grupy silnie uzbrojonej, i spełniający własności Markowa (w badaniu nie uwzględniono czynnika „kontroli" terytorium przez uzbrojone grupy, uznano go

za jednostronny i błędny). Modelowanie obecności grupy uzbrojonej jako procesu Markowa jest realistyczne, ponieważ poziom obecności grupy uzbrojonej w czasie *t* w dużym stopniu zależy od poziomu w *t − 1*, ale niekoniecznie w *t − k*. Zmienna losowa nielegalnej obecności grupy może zachowywać się w sposób, w jaki przeszłość i przyszłość zależą tylko od teraźniejszości. HMM obejmuje również proces zależny od stanu {*Xt* : *t* = 1, 2, . . .}, w którym rozkład *Xt* zależy tylko od bieżącego *Pt*, a nie od poprzednich stanów lub obserwacji. W tym badaniu *Xt* reprezentuje gwałtowne działania popełniane przez grupy zbrojne, które można również kategoryzować rodzajem zbrojnego działania.

Metodologia HMM pozwala na oszacowanie ukrytych cech procesu, takich jak prawdopodobieństwo przejścia z jednego stanu do drugiego, na podstawie bezpośrednio obserwowalnych danych. HMM został użyty do przewidywania obecności grup zbrojnych w każdej gminie w każdym kwartale. Wskazano parametry do oszacowania: sześć prawdopodobieństw przejścia określających łańcuch Markowa i sześć prawdopodobieństw dla każdego z trzech stanów (każdy stan będzie reprezentował poziom obecności grupy zbrojnej: poziom 1 – niska obecność grupy zbrojnej, poziom 2 – średnia obecność grupy zbrojnej i poziom 3 – wysoka obecność grupy zbrojnej). Prawdopodobieństwo przejścia daje prawdopodobieństwo przejścia z różnych *m* stanów obecności grupy zbrojnej do innego (tj. zarówno rodzajów militarnych wystąpień, jak i przemieszczania terytorialnego pomiędzy gminami). Na przykład prawdopodobieństwo przejścia z terytorium z wysoką obecnością grupy zbrojnej *H* do niskiej obecności grupy zbrojnej *L*.

Wynikiem przeprowadzonego badania było stwierdzenie, że większość skutków wstrząsów gospodarczych występuje w gminach o niskiej obecności grup zbrojnych. Ponadto niektóre skutki wstrząsów gospodarczych różnią się, gdy przemoc popełniają kolumbijskie FARC lub grupy paramilitarne (grupy służące ochronie prywatnych interesów elit regionalnych i handlarzy narkotyków z użyciem siły dopuściły się wielu naruszeń praw człowieka i były powiązane z nielegalną działalnością, taką jak eksport kokainy, przemyt, nielegalne górnictwo). Zyski z kokainy utrzymują FARC, co umożliwia rekrutację bojowników. Inaczej jest w przypadku cen kawy – jako miejscowego regulatora wystąpień militarnych. Ich wzrost powoduje zamożność miejscowej ludności i generowanie sympatii wobec grup paramilitarnych, w których upatrują ochronę dla swoich gospodarczych interesów. Z kolei wstrząsy naftowe wydają się zwiększać ataki partyzanckie w gminach o dużej obecności FARC, ale nie w gminach o małej obecności FARC. Jak sugerują badania, wstrząsy naftowe mogą zwiększać nieregularne taktyki, takie jak ataki na rurociągi naftowe, które FARC może łatwo przeprowadzić na terytoriach o większej obecności grup paramilitarnych.

Vasanthan Raghavan, Aram Galstyan i Alexander G. Tartakovsky (2013, s. 2403) zaproponowali inne rozwiązanie oparte na HMM jako konfrontacje wobec innych modeli, takich jak TAR (ang. Threshold Autoregressive Model, model autoregresji progowej) i SEHM. Wskazano HMM dla stanu *d* dla profilu działalności, w którym

każdy z *d* możliwych wartości odpowiada pewnemu odrębnemu poziomowi atrybutu instrumentu bazowego. Najprostszym nietrywialnym ustawieniem jest *d = 2* ze stanami: „aktywnym" i „nieaktywnym". Ustawienie to okazało się dobrym modelem oddającym większość aspektów rzeczywistości danych dotyczących terroryzmu. Kluczem do oceny jest hipoteza, że obecną działalność grupy można ująć w całości, opierając się na pewnych stanach/cechach grupy, zamiast na całej przeszłej historii grupy. W obu stanach *d* dni aktywności są modelowane jako dyskretny czas Poissona, proces punktowy z modelem geometrycznym opartym na przeszkodach, który dobrze pasuje do liczby ataków w danym dniu. Podejście HMM zapewnia kompetentne alternatywne ramy modelowania dla podejścia TAR i SEHM, zarówno w aspekcie wyjaśniającym, jak i predykcyjnym. W modelu TAR bieżąca obserwacja jest wyraźnie zależna od obserwacji z przeszłości, ewentualnie wpływu innych niezależnych zmiennych odpowiadających określonym wydarzeniom/interwencjom geopolitycznym. Z drugiej strony w SEHM prawdopodobieństwo ataku zwiększa się zgodnie z historią grupy. HMM łączy oba te aspekty, wprowadzając sekwencję stanów ukrytych. Kolejność stanów zależy wyraźnie od jego najbliższej przeszłości (Pattipati, Willett, Allanach et al., 2006, s. 26). Autorzy zaproponowali hipotezę, że wzrost (lub spadek) intensywności ataku terrorystycznego można naturalnie przypisać pewnym zmianom w wewnętrznych stanach grupy, które odzwierciedlają dynamikę jej ewolucji, a nie faktowi, że grupa przeprowadziła już ataki w poprzednim dniu/tygodniu/miesiącu (Raghavan, Galstyan, Tartakovsky, 2013, s. 2403). Jest to alternatywne podejście do prezentowanego w modelach TAR i SEHM. Zwrócono także uwagę na to, że na modelowanie wpływ ma niejednoznaczność czasowa oznaczająca, że dokładny przypadek (czas) wystąpienia incydentu terrorystycznego jest trudny do ustalenia. Wynika to z faktu, że relacje z większości zdarzeń terrorystycznych pochodzą ze źródeł zewnętrznych. W związku z tym najbardziej istotna jest szczegółowość zgłaszania incydentów (czyli skala czasowa, w której incydenty są zgłaszane) wynosząca zwykle kilka dni.

Kolejny czynnik to niejednoznaczność atrybucyjna wynikająca z tego, że w wielu bazach danych istnieje niejasność w przypisywaniu pewnego incydentu terrorystycznego do określonej grupy.

I ostatni czynnik to rzadkość danych. Uznając właściwość Markowa, zwrócono uwagę na to, że grupa terrorystyczna (teoretycznie) posiadająca nieskończone zasoby do działania i stale organizująca zamachy może działać w określony sposób. W takim przypadku każdy dodatkowy atak przyczynia się w równym stopniu do sukcesu – osiągnięcia zadanego celu ostatecznego i dopóki cel grupy nie zostanie osiągnięty, dopóty jego osiągnięcie w przyszłości nie zależy od poprzednich ataków. Możliwe jest także spowodowanie niewielkiej modyfikacji dynamiki grupy, zakładającej, że zaistniały opór/przeszkoda dla grupy musi zostać pokonana, zanim ten *modus operandi* zacznie działać. Prowadzi to do oceny funkcjonowania go jako modelu geometrycznego opartego na przeszkodach (ang. *hurdle-based geometric model*) (Raghavan, 2014).

Jakościowe porównanie między ramami TAR, SEHM i HMM wskazuje, że wszystkie trzy modele zakładają, że bieżąca obserwacja/aktywność zależy od historii, modele jednak różnią się sposobem realizacji tej zależności. Kolejność stanu zależy wyraźnie od jego najbliższej przeszłości (jednoetapowy proces struktury Markowa, posiadanie stacjonarnych prawdopodobieństw przejścia oznacza, że one się nie zmieniają), natomiast prawdopodobieństwo ataku zwiększa się na podstawie realizacji stanu. W podsumowaniu wskazano na to, że modele TAR i HMM są podobne do siebie pod względem przełączania reżimów, ponieważ cechy te są modelowane jawnie. Jednak mechanizm przełączania reżimów jest różny w obu przypadkach: pierwszy zakłada zmianę w procesie autoregresyjnym, podczas gdy drugi zakłada przejście stanu w modelu HMM. W szczególności w modelu TAR bieżąca obserwacja jest wyraźnie zależna od wcześniejszych obserwacji wraz z (możliwym) wpływem innych niezależnych zmiennych odpowiadających pewnym wydarzeniom/interwencjom geopolitycznym (Raghavan, Galstyan, Tartakovsky, 2013, s. 2426). Model SEHM obejmuje również przejścia między stanami (wywołane przez składnik samowzbudzający), ale to przejście jest raczej niejawną cechą modelu niż jawnym jego składnikiem. Model TAR uwzględnia raczej globalne trendy terroryzmu, a nie trendy ograniczone do konkretnego regionu lub konkretnej grupy. HMM prowadzi do lepszego dopasowania modelu dla zestawu danych lokalnych w porównaniu do SEHM. Ta logika również sugeruje, że HMM może być gorszym modelem dla trendów regionalnych/globalnych (działanie to może być lepsze jakościowo, pod warunkiem że okres szkolenia jest długi, tak aby zapewnić dokładne uczenie się modelu dla HMM). Jako uzupełnienie można także wskazać badania przeprowadzone przez Charfeddine'a Lanouara i Mohameda Goaieda w zakresie wpływu ataków terrorystycznych i niestabilności politycznej na działalność turystyczną w Tunezji w latach 2000-2016.

Dzięki oszacowaniu trzystanowego modelu przełączania Markowa, składającego się ze średniej, trendu i wariancji, ustalono, że tunezyjska rewolucja jaśminowa i dwa ataki terrorystyczne, jeden w Muzeum Narodowym Bardo, 18 marca 2015 r., a drugi w kurorcie turystycznym w Port El Kantaoui, Sousse, 26 czerwca 2015 r., odegrały ważną rolę w wywieraniu wpływu na działalność turystyczną kraju. Ponieważ hipoteza prawdziwej długiej pamięci została odrzucona z użyciem Testu Shimotsu (Shimotsu, 2008), kolejny krok polegał na zastosowaniu modeli uwzględniających krótką pamięć i zmiany reżimów. W tym przypadku wybrano pod uwagę model autoregresyjnego przełączania Markowa MS (zob. słowniczek, pkt 4). We wnioskach wskazano, że: wpływ wstrząsów powstałych w wyniku ataków terrorystycznych na działalność turystyczną jest poważniejszy niż wpływ rewolucji jaśminowej. Pod względem czasu trwania wstrząsy powstałe w wyniku ataków terrorystycznych mają bardziej długotrwały wpływ (1 rok i 2 miesiące) w porównaniu do wstrząsu rewolucji jaśminowej (8 miesięcy), w przypadku Tunezji wstrząsy wewnętrzne mają największy wpływ na działalność turystyczną, podczas gdy wstrząsy zewnętrzne,

w tym ataki terrorystyczne z 11 września 2001 r. (WTC) i światowy kryzys finansowy z 2008 r., które należą do drugiego reżimu, mają jedynie umiarkowany wpływ. Ten ostatni wynik można wyjaśnić rodzajem i charakterem sektora turystycznego w Tunezji, która jest znana jako miejsce o niskich kosztach, jako destynacja niskobudżetowa (Lanouar, Goaied, 2019, s. 414).

Krishna Pattipati, Peter Willett, James C. Allanach, Haiying Tu i Satnam Singh (2006, s. 28) również podjęli próbę zastosowania HMM wobec typowania zdarzeń terrorystycznych. W tym przypadku „ukryty" proces odnosi się do serii prawdziwych transakcji opisujących zachowanie określonej grupy terrorystycznej, a proces obserwacji to wywiadowcza baza danych zawierająca wszelkie informacje, które można przedstawić jako zaobserwowane transakcje (w tym przypadku transakcje to dane świadczące o aktywności terrorystycznej osób w nią zaangażowanych). Autorzy zaproponowali połączenie możliwości wykrywania HMM z siecią węzłów – siecią Bayesa (BN), którą można zwizualizować jako bezpośredni wykres acykliczny składający się ze zbioru zmiennych i zbioru skierowanych krawędzi pomiędzy zmiennymi. Te zmienne to mogą być podmioty lub wydarzenia będące przedmiotem zainteresowania, takie jak „organizacja terrorystyczna X rekrutuje nowych członków" lub że „planowany jest nowy atak". Połączenie między węzłami oznacza, że istnieje związek przyczynowy, związek pomiędzy odpowiednimi zmiennymi. Całość realizowana jest w ramach SNA (ang. Social Network Analysis), czyli analizy sieci społecznych schematów, do których prowadzone były powiązania terrorystyczne.

Wprowadzony przez autorów podstawowy badawczy model procesu ASAM (ang. Adaptive Safety Analysis and Monitoring) ma na celu wsparcie podejmowania strategicznych decyzji. A więc aby ułatwić wdrożenie ASAM, wybrano strukturę hierarchiczną powiązań, a na najniższym poziomie ASAM wykorzystano ukryte modele Markowa (HMM). ASAM odnosi się do zadania, ucząc się – jeśli to możliwe – z danych historycznych, stosuje się schemat oceniający najbardziej prawdopodobną sekwencję zdarzeń i przewidujący przyszłe wydarzenia. Ponadto uznano, że HMM jest główną metodą modelowania procesów stochastycznych i dlatego też stanowi idealny sposób na wyciąganie wniosków na temat ewolucji siatek terrorystycznych. Przy czym należy pamiętać, że HMM działała w środowisku o niskim współczynniku SNR, tj. danych obserwowalnych jest wiele, stanowią one po prostu szum informacyjny i dlatego powiązanie danych (które transakcje są istotne) stanowi szczególny problem. Dane wejściowe do procesu ASAM stanowią serię transakcji pomiędzy osobami, miejscami i rzeczami podejrzanego pochodzenia. Osoby, miejsca i rzeczy reprezentują węzły, a transakcje, czyli relacje, reprezentują połączenia pomiędzy węzłami.

Oparcie badań nad terroryzmem na analizie SNR z wykorzystaniem HMM prezentują także Clifford Weinstein, William Campbell, Brian Delaney i Gerald O'Leary (2009). Autorzy badali modelowania, wykrywania i śledzenia grup terrorystycznych i ich zamiarów na podstawie danych multimedialnych.

W badaniu wykorzystano także język opisu ataku terrorystycznego (TADL), który jest używany jako podstawa do modelowania i symulacji ataków terrorystycznych. Przedmiotem badań był zamach bombowy na ambasadę Australii w Dżakarcie we wrześniu 2004 r. (w tym zakresie wykorzystano źródła otwarte i akta sądowe) oraz fikcyjny scenariusz, który został opracowany w innym projekcie do badań nad SNA. Uznano, że zaletą wykorzystania struktury HMM jest to, że można ją łatwo kontrolować jako ogólną sekwencję zdarzeń scenariusza. Ponadto HMM zapewnia rygorystyczną strukturę teoretyczną do analizy i modelowania. Wadą modelowania HMM było to, że trudno jest przedstawić za jej pomocą wiele zjawisk, które występują w scenariuszach (możliwe jest ich pojedyncze przedstawienie, ale łączne powoduje utrudnienia). HMM został wykorzystany na potrzeby procesu tworzenia formalnych reprezentacji scenariuszy, który stanowi opis kolejności i prawdopodobieństw transakcji ujawnionych w rozpatrywanej przestrzeni informacyjnej. Za transakcje uznano działania i komunikację między terrorystami, a dla uproszczenia materiałem wyjściowym była wiedza o określonej osobie – ustalonym sprawcy zamachu terrorystycznego. Używając dyskretnej struktury HMM, należało określić potencjalne wyjścia dla każdego stanu i powiązane prawdopodobieństwa emisji. Dane wejściowe do systemu to duża ilość surowych danych multimedialnych, które obejmują głos, tekst, sesje sieciowe, dane czujników, raporty i inne źródła. Istotą przeprowadzonych symulacji było to, aby wygenerować niewidziane scenariusze. W konsekwencji użyto język, który stochastycznie generuje transakcje obliczenia, opierając symulację scenariuszy na dyskretnym modelowaniu ukrytego modelu Markowa (HMM). Dla każdego stanu dopuszczono występowanie wielu różnych typów transakcji, a każdy z nich miał prawdopodobieństwo emisji przy założeniu, że znajdował się w określonym stanie wyjściowym.

Opierając swoje badania na danych symulacyjnych, przyjęto, że: sieć społecznościowa jest zmienna w czasie, wprowadzono transakcje bramkowane (transakcja bramkowa wymaga, aby pewna transakcja wystąpiła przed przejściem do następnego stanu), prawdopodobieństwo miało określać także, czy transakcja wygenerowana przez HMM jest faktycznie obserwowana.

Kolejnym aspektem wykorzystania HMM w badaniu było to, aby w zakresie procesu tworzenia formalnych reprezentacji scenariuszy nastąpiło ustalenie opisu kolejności i prawdopodobieństw transakcji. HMM wykorzystał język oprogramowania TADL połączony z interfejsem graficznym. W konsekwencji użycia HMM dążono do rozpoznawania intencji celem wskazania analitykowi zagrożeń, które mogą być obecne w strumieniu transakcji. Istotą pozostaje wykrywanie znanych lub hipotetycznych scenariuszy docelowych, priorytetyzacja scenariuszy docelowych i interpretacja wyników uzyskanych na podstawie tego wykrycia. Zadanie to jest o tyle trudne, iż „wiedza" opiera się na danych pozyskiwanych z niepewnych źródeł, w tym bez możliwości określenia „prawda" czy „fałsz". Przy dużych nieustrukturyzowanych masach danych multimedialnych dostępnych w sieci WWW

konwersja surowych danych do innej formy tworzy niestety nowy zalew ustrukturyzowanych danych (Campbell, Barrett, Acevedo-Aviles et al., 2010). W tej kwestii HMM określa kolejność, w jakiej można obserwować transakcje, oraz prawdopodobieństwo każdego możliwego uporządkowania. Zapewnia również sposób zwięzłego przedstawienia wielu kierunków działań, które można podjąć w różnych punktach podczas opracowywania scenariusza. Struktura modelu HMM określa ogólny przepływ zdarzeń, które stanowią scenariusz. Ów scenariusz jest dzielony na stany i odrębne fazy, przez które scenariusz może przejść podczas swojego rozwoju. Przebieg symulacji może się różnić w zależności od przebiegu i jest stochastycznie opisywany przez rozkład prawdopodobieństwa przejścia stanu. Każdy stan modelu HMM zawiera zestaw transakcji, które są reprezentatywne dla tego stanu (stosowana jest także dyrektywa mająca na celu losowe wybieranie predykatów z bazy wiedzy i włączania ich do transakcji). Wyniki i prawdopodobieństwa przejścia modeli HMM rozpoznających scenariusze zostały wytrenowane na pozytywnych i negatywnych przykładach treningowych. Badanie obcięcia wpływu na zdolność rozpoznawania scenariuszy jest ważne, ponieważ pożądane jest wykrywanie ataków na etapach planowania, zanim nastąpi sam atak terrorystyczny. We wnioskach wskazano, że całkowite odwrócenie scenariusza jest najgorszym scenariuszem (jest to sytuacja, w której zdarzenie terrorystyczne następuje przed planowaniem lub rekrutacją). Ponadto wskazano, że wykrywanie scenariuszy za pośrednictwem HMM konsekwentnie przewyższa wykrywanie za pomocą innych metod (np. SVM, ang. Support Vector Machines – metoda wektorów nośnych). Adekwatnie model można odnieść do oceny scenariuszy procederu prania pieniędzy z zastosowaniem innych parametrów oceny stanów.

Podsumowanie

Modele HMM znajdują obecnie powszechne zastosowanie tam, gdzie problemy decyzyjne ujawniają się w kontekście systemu dynamicznego, którego stany nie są bezpośrednio obserwowalne dla decydenta. Takimi stanami są wszelkie stany wiązane z aktywnością terrorystyczną czy praniem pieniędzy. Ukryte modele Markowa HMM różnią się od klasycznych łańcuchów Markowa brakiem możliwości bezpośredniej obserwacji stanu, w jakim znajduje się proces. Zamiast tego obserwować można realizację probabilistycznej funkcji określonej na zbiorze stanów procesu, której wartościami są symbole pewnego przyjętego zbioru zachowań. We wskazanych przykładach tymi stanami ukrytymi były: transakcje opisane kwotowo, poziom zagrożenia sytuacyjnego, relacje pomiędzy członkami przestępczej społeczności czy militarna obecność obserwowalnej grupy zbrojnej na danym terenie. Wydaje się, że przy takiej właściwości możliwe byłoby jedynie „wyławianie" anomalnych zachowań ze zbioru zachowań, jakimi dysponuje IO w ramach systemu AML/CFT,

oraz z tzw. źródeł zewnętrznych, a także z uprawnionych do gromadzenia danych ośrodków analitycznych (Centro de Investigación y Educación Popular, CINEP) (Baron, 2021). Ponadto użycie metody HMM pozwoliłoby na „dyskretne obserwowanie" jedynie w celu ustalenia wielokrotności takich stanów w jednostce czasowej (jako stanów bliskich sobie, czyli występujących w krótkich jednostkach czasowych i wykazywaniu ich pierwotnego zachowania jako anomalii w dłuższym okresie), które decydują o zwiększaniu się ryzyka i zagrożenia. IO musi sobie jednak zdawać sprawę z tego, iż powinna wstępnie określić parametry mierzalne stanów i poszukać źródeł informacyjnych umożliwiających ich ocenę i kwalifikację. Wszak ujawnienie powinno być możliwe do obserwowania na podstawie procesu stochastycznego, który generuje sekwencje obserwacji. Tym samym początkowo badacz identyfikuje stany ukryte, wyznacza ich mierzalność i poszukuje źródeł informacji, które potrafią je zidentyfikować i nadać mierzalne kwalifikacje. Wstępny wybór parametrów wpływa na wydajność zastosowanego algorytmu obliczeniowego. Pierwszy wynik byłby oceną „intensyfikacji" działania sprawcy S_1, drugi zaś sprawcy S_2 jako działającego jak S_1 (anomalnie). Wcześniej taka „obserwacja" wymagałaby od IO ustalenia stanu „wzorca" oraz zdefiniowanego stanu/stanów „anomalii" oraz atrybutów dla stanów. Przy czym pewnie należałoby określić jako stany anomalne te, które będą najbardziej „wartościowe", czyli z którymi IO wiąże największe zagrożenie. Tym samym HMM może być także użyte jako stały model obserwacyjny w stosunku do tych klientów, wobec których nie stwierdzono potrzeby stosowania wzmożonych środków bezpieczeństwa finansowego lub nie do końca zakwalifikowanych jako nowych, gdyż nie ma pewności w zakresie wyniku ich identyfikacji i weryfikacji, a jednocześnie nie wynika to z posiadanych danych, aby ocena ryzyka powodowała potrzebę wzmożenia ich obserwacji. Wobec takich podmiotów można używać dłuższych sekwencji czasowych i powtarzanej sekwencji oceny stanów. Modele HMM stanowią nie tylko element „wykrywania" zachowań „ukrytych", lecz także stają się elementem procesów decyzyjnych, a w konsekwencji zarządczych wobec ustalonych predykcyjnych zagrożeń (głównie prawdopodobieństwa ich wystąpienia). Tym samym stanowią one także element wsparcia dla decyzji wykrywczych w procesach decyzyjnych z dziedziny bezpieczeństwa.

Bazowanie na metodzie HMM jest pewnym niezbędnym rozwiązaniem, zwłaszcza jeżeli chodzi o typowanie stanów zagrożeń związanych z możliwymi zdarzeniami terrorystycznymi, które można jedynie przewidzieć, posługując się prawdopodobieństwem. Należy pamiętać, że liczba przypadków zdarzeń terrorystycznych jest bardzo niska, zawiera luki informacyjne, dlatego zaprojektowanie modeli opartych na podejściu „uczenie się na danych" kompletowanych w dłuższym przedziale historycznym jest możliwe, ale traktowane jest jako problematyczne. Ponadto istnieje potrzeba pozyskiwania pewnych wymaganych zewnętrznych informacji (wobec agenta analitycznego IO czy wobec samej grupy, sięgając do danych z jej otoczenia) na temat prawdopodobnej struktury komórki terrorystycznej.

Informacje te będą wymagane do odfiltrowania mało prawdopodobnych danych, które wydają się potencjalnie groźne (Pattipati, Willett, Allanach et al., s. 28). Stąd także wyniknęła potrzeba budowania wiedzy o terrorystach na podstawie danych niezwiązanych bezpośrednio z tym rodzajem przestępczości (jako pośrednie wyniki obserwacyjne). Ma to też swoje przełożenie na tworzenie zbiorów uczących dla matematycznych/nieprobabilistycznych modeli przeciwdziałania. W konsekwencji prowadzenie badań na podstawie niskiej liczby danych i dostępnych w większych przedziałach czasowych może dawać nieadekwatne wyniki. Dlatego też badacze skłaniają się w takich sytuacjach do stosowania modelu probabilistycznego HMM.

Można także zauważyć, że HMM może być „lepiej" wykorzystane na potrzeby identyfikacji prania pieniędzy niż finansowania terroryzmu ze względu na to, że pierwszy z procederów pozostawia znacznie więcej śladów aktywności sprawcy, a ponadto proces integracji identyfikuje poszczególne stany „nieuczciwe" ze stanami „uczciwymi". W konsekwencji stanów ukrytych jest mniej niż w przypadku finansowania terroryzmu, ale są one trudniej rozpoznawalne, gdyż niosą one ze sobą pierwiastek „legalności". HMM stosowane na rzecz przeciwdziałania finansowaniu terroryzmu staje się czasami jedynym modelem probabilistycznym na rzecz przewidywalności stanów zagrożenia, gdy wiedza o stanach poprzednich jest niewielka lub jej brak. Kwestia odmienności patrzenia na wykorzystanie HMM związana jest także z tym, że w przypadku prania pieniędzy sprawca dąży do zakończenia procesu stanem zalegalizowania środków (pewności nadania im nowych cech), a w przypadku zdarzeń terrorystycznych cykle ciągłości czasowej są bardzo krótkie i rozproszone (np. geograficznie) lub też występują jedynie pojedynczo (mogą być więc niestabilne czasowo). Tym samym w przypadku finansowania terroryzmu trudne jest usystematyzowanie szeregów czasowych na potrzeby typowania kolejnych stanów zagrożenia. Istotnym elementem otrzymania precyzyjniejszego wyniku jest zastosowanie algorytmów Bauma–Welcha i Viterbiego.

Należy także zauważyć, że możliwości zastosowania metod opartych na ukrytym modelu Markowa HMM podlegają pewnym istotnym ograniczeniom. To podstawowe ograniczenie związane jest z założeniem, iż poszczególne elementy ciągu obserwacji są od siebie niezależne. Kolejne ograniczenie wynika z założeń Markowa, że prawdopodobieństwo przejścia do danego stanu w chwili t zależy jedynie od stanu układu w chwili $t-1$. Innym istotnym faktem, na który należy zwrócić uwagę, jest ograniczona dokładność opisu cech statystycznych sygnału w przypadku obserwacji o ciągłym charakterze (rozkład obserwacji w postaci funkcji Gaussa, autoregresja) (Fabian, Szedel, 2002, s. 326-327). Co istotne, ważne jest także ustanowienie w HMM parametrów startowych w procesie estymacji (segmentacja szeregu) oraz doboru liczby ukrytych stanów.

W przypadku, w którym IO nie jest zdolna lub nie jest możliwe stałe monitorowanie (obserwowanie) zachowań klienta i przeprowadzanych transakcji w warunkach „tradycyjnej obserwacji", metoda HMM daje – w ogóle – próbę możliwości, przy zastosowaniu jej właściwości podjęcia tej obserwacji na podstawie prawdopodobieństwa wytypowanych kolejnych stanów. Wynik, który powinien znacznie ograniczyć szczegółowe zajęcie się danym przypadkiem, umożliwi w konsekwencji, nawet tradycyjne, monitorowanie klienta/transakcji na potrzeby zweryfikowania ostatecznego jego zachowania jako „podejrzalności" udziału w procederze prania pieniędzy/finansowania terroryzmu. W wyniku takiego postępowania HMM niesie pomoc w zakresie typowania zachowań anomalnych (lub prawdopodobieństwa wystąpienia kolejnego określonego rodzaju stanu), identyfikowalnych w IO, jako mogących świadczyć o praniu pieniędzy/finansowaniu terroryzmu, jako stanów *S* w danym czasie *t*. Stan początkowy dla HMM może być ustalony na podstawie metody estymacji z wykorzystaniem analizy skupień (Staniak, 2016). Należy jednak mieć na uwadze to, że podejście statyczne oceny stanu początkowego nie może zdominować oceny dynamicznej stanów. Ale to rozwiązanie może być pomocne w ocenie zachowań klientów typowanych jako „uśpionych" w łańcuchu dostaw w procederze prania pieniędzy czy finansowania terroryzmu (istotna jest zmiana parametrów w pewnym momencie w trakcie próby, oszacowania toczącego się stanu). Analiza tocząca (ang. *polling analysis*) jest powszechnie stosowana do testowania wstecznego modelu statystycznego na danych historycznych w celu oceny stabilności i dokładności predykcyjnej.

Mając na uwadze akcje sabotażowe (jako quasi-terrorystyczne) organizowane przez zewnętrze czynniki rosyjskie, metoda HMM możliwa będzie także do zastosowania wobec tego typu aktywności, w szczególności w zakresie typowania możliwego czasu i miejsca ich wystąpienia. Przy czym wydaje się, że ataki terrorystyczne organizowane przez ugrupowania terrorystyczne postępują w myśl takich „zasad", iż gdy wynikające z dokonanych zamachów środki zaradcze zastosowane w jednym kraju doprowadziły do neutralizacji ataków, to działania należy kontynuować w innych, słabiej przygotowanych krajach. W tym jednak przypadku taktyka może być podobna do tej, jaką wobec tzw. „państw zachodnich" realizowało ZSRR (Związek Socjalistycznych Republik Radzieckich), mając na celu wprowadzanie wewnętrznej destrukcji na poziomie zapewniania bezpieczeństwa i utrzymywania ograniczonego zaufania do państwa kapitalistycznego przez obywateli (np. przez zarządzanie refleksyjne). Rozkład i prawdopodobieństwo dzisiejszych zagrożeń może dotyczyć relacji Rosja/Białoruś – Unia Europejska. W szczególności, że w tym przypadku można typować, iż występuje wspólny czynnik lub czynnik napędzający do działań sabotażowych (np. może nim być wektor efektywności działań wojennych w konflikcie Rosja – Ukraina).

SŁOWNICZEK

[1] ALGORYTM BAUMA–WELCHA – znany również jako algorytm do przodu i do tyłu, jest podejściem do programowania dynamicznego i szczególnym przypadkiem algorytmu maksymalizacji oczekiwań (algorytm EM). Jego celem jest dostrojenie parametrów HMM, czyli macierzy przejść stanów A, macierzy emisji B i rozkładu stanu początkowego π_0, tak aby model maksymalnie przypominał obserwowane dane. Algorytm Bauma–Welcha polega na znalezieniu w kolejnych iteracjach lokalnego maksimum funkcji wiarygodności.

[2] ALGORYTM VITERBIEGO – algorytm dekodujący, o strategii programowania dynamicznego, opracowany przez Andrew Viterbiego i opublikowany przez niego w 1967 roku w „IEEE Transactions on Information Theory", IT-13 w artykule *Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm* (Wikipedia, 2024).

[3] ANALIZA SIECI SPOŁECZNOŚCIOWYCH – czyli SNA, metoda badawcza służąca do wizualizacji i analizy relacji i połączeń między podmiotami lub osobami w sieci. W metodzie tej wykorzystywana jest analiza sieci i teoria grafów.

[4] ARIMA (ang. Auto Regressive Integrated Moving Average) – model statystyczny wykorzystywany do analizy i prognozowania szeregów czasowych. Szeregi czasowe to dane, które są rejestrowane, obserwowane lub mierzone w równych odstępach czasu, np. dzienna cena akcji lub miesięczna sprzedaż produktu (Bigglo.pl, 2024).

[5] MODEL AUTOREGRESYJNEGO PRZEŁĄCZANIA MARKOWA MS – modele, w których zarówno zmienna, jak i parametry opisują dynamikę procesu między stanami. Po raz pierwszy dynamiczny model ekonometryczny z przełączeniem typu Markowa wprowadził J. Hamilton (1989, 1994) jako narzędzie opisujące wewnętrzną strukturę przejścia między stanami procesu cyklu gospodarczego. Cechą przełącznikowego modelu Markowa jest możliwość przełączania się wybranych parametrów procesu między reżimami (stanami) zgodnie z procesem Markowa (Kośko, 2005).

[6] SYSTEM ADAPTIVE SAFETY ANALYSIS AND MONITORING (ASAM) – hybrydowe narzędzie programowe oparte na modelu, które pomaga analitykom wywiadu identyfikować zagrożenia terrorystyczne, przewidywać możliwą ewolucję działań terrorystycznych i sugerować strategie przeciwdziałania terroryzmowi. System ASAM zapewnia rozproszoną strukturę przetwarzania do gromadzenia, udostępniania, rozumienia i wykorzystywania informacji w celu oceny i przewidywania stanów sieci terrorystycznych (Tu, Allanach, Satnam et al., 2004).

[7] PROCESY HAWKESA – procesy punktowe, które znajdują bardzo szerokie zastosowanie od sejsmologii, po finanse, ubezpieczenia, modelowanie sieci społecznościowych, aż do rozwoju epidemii. Charakteryzują się one własnością samopobudzania (ang. *selfexcitation*), polegającą na tym, że warunkowe rozkłady czasów oczekiwania na kolejne zdarzenia zależą od historii procesu do momentu, na który dokonujemy warunkowania. Procesy Hawkesa nie są procesami Markowa, ale w pewnych szczególnych przypadkach można dokonać jego tzw „markowianizacji". Oznacza to, że można znaleźć taki proces X, iż proces Hawkesa N rozszerzony o X, tzn. (N,X), będzie procesem Markowa (Niewęgłowski, 2022).

BIBLIOGRAFIA

[1] Baron, M.V., 2021. Identifying armed group presence using Hidden Markov Models, *Arts & Sciences Electronic Theses and Dissertations*, https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=3325&context=art_sci_etds (dostęp: 24.08.2024).

[2] Bhusari, V., Patil, S., 2011. Application of Hidden Markov Model in Credit Card Fraud Detection, *International Journal of Distributed and Parallel Systems*, nr 2 (6), s. 203-211.

[3] Bigglo.Pl, 2004. *Co to jest ARIMA? Definicja*, https://bigglo.pl/slownik/co-to-jest-arima/ (dostęp: 25.08.2024).

[4] Campbell, W.M., Barrett, S., Acevedo-Aviles, J., Delaney, B., Weinstein, C., 2010. Detection and simulation of scenarios with hidden Markov models and event dependency graphs, *Acoustics, Speech, and Signal Processing*, ICASSP-88, 1988 International Conference on 2010.

[5] Coffman, T.R., Marcus, S.E., 2004. Dynamic classification of groups through social network analysis and HMMs, [w:] *Aerospace Conference, Proceedings, 2004 IEEE*, vol. 5, s. 3197-3205.

[6] Fabian, P., Szedel, J., 2002. Teoretyczne podstawy zastosowań ukrytego modelu Markowa do rozpoznawania wzorców, *Studia Informatica*, vol. 23, nr 4 (51), s. 301-328.

[7] Hawkes, A.G., 1971. Spectra of some self-exciting and mutually exciting point processes, *Biometrika*, nr 58, s. 83-90.

[8] Hossain, T., Gao, S., Kennedy, B., Galstyan, A., Natarajan, P., 2020. Forecasting violent events in the Middle East and North Africa using the Hidden Markov Model and regularized autoregressive models, *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 17, nr 3, s. 269-283.

[9] Kośko, M., 2005. Zastosowanie przełącznikowych modeli Markowa w analizie stóp zwrotu cen akcji, IX Ogólnopolskie Seminarium Naukowe, Katedra Ekonometrii i Statystyki, Uniwersytet Mikołaja Kopernika w Toruniu, 6-8 września 2005, https://www.dem.umk.pl/DME/2005/28_kosko.pdf (dostęp: 24.08.2024).

[10] Lanouar, Ch., Goaied, M., 2019. Tourism, terrorism and political violence in Tunisia: Evidence from Markov switching models, *Tourism Management*, nr 70, s. 404-414.

[11] Laub, P.J., Taimre, T., Pollett, P.K., *Hawkes Processes*, https://www.researchgate.net/publication/280034116_Hawkes_Processes (dostęp: 24.08.2024).

[12] Li, Y., Duan, D., Hu, G., Lu, Z., 2009. *Discovering Hidden Group in Financial Transaction Network Using Hidden Markov Model and Genetic Algorithm*, Sixth International Conference on Fuzzy Systems and Knowledge Discovery, Tianjin, https://ieeexplore.ieee.org/document/5360621 (dostęp: 20.08.2024).

[13] Niewęgłowski M., 2022. *Markowskie wielowymiarowe procesy Hawkesa*, https://www.impan.pl/~zakopane/50/Nieweglowski.pdf (dostęp: 24.08.2024).

[14] Nwanga, M.E., Okafor, K.C., Achumba, I.E., Chukwudebe, G.A., 2022. *Predictive Forensic Based – Characterization of Hidden Elements in Criminal Networks Using Baum-Welch Optimization Technique*, [w:] *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, Cham: Springer International Publishing, s. 231-254.

[15] Pattipati, K., Willett, P., Allanach, J., Tu, H., Singh, S., 2006. *Hidden Markov Models and Bayesian Networks for Counter-Terrorism*, [w:] Popp, R.L., Yen, J. (Eds.), *Emergent Information Technologies and Enabling Policies for Counter-Terrorism*, Hoboken, NJ: Wiley, s. 27-50.

[16] Raghavan, V., 2014. *Modeling and inferencing for activity profile of terrorist groups*, Bridgewater, NJ: Qualcomm Flarion Technologies, Inc.

[17] Raghavan, V., Galstyan, A., Tartakovsky, A.G., 2013. Hidden Markov models for the activity profile of terrorist groups, *The Annals of Applied Statistics*, vol. 7, nr 4, s. 2402-2430.

[18] Shimotsu, K., 2008. *Simple (but effective) tests of long memory versus structural breaks*, Department of Economics Queen's University, https://www.bayes.city.ac.uk/__data/assets/pdf_file/0007/64177/27-Shimotsu.pdf (dostęp: 24.08.2024).

[19] Staniak, J., 2016. Inicjalizacja ukrytych modeli Markowa z wykorzystaniem analizy skupień, *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, nr 446, s. 224-236.

[20] Theodosiadou, O., Chatzakou, D., Tsikrika, T., Vrochidis, S., Kompatsiaris, J., 2023. Real-time Threat Assessment based on Hidden Markov Models, *Risk Analysis*, vol. 43, nr 10.

[21] Theodosiadou, O., Pantelidou, K., Bastas, N., Chatzakou, D., Tsikrika, T., Vrochidis, S., Kompatsiaris, I., 2021. Change Point Detection in Terrorism-Related Online Content Using Deep Learning Derived Indicators, *Information*, nr 12, s. 1-15.

[22] Tu, H., Allanach, J., Satnam, S., Pattipati Krishna, R., Willett, P., 2004. *The Adaptive Safety Analysis and Monitoring system*, https://www.researchgate.net/publication/228580863_The_Adaptive_Safety_Analysis_and_Monitoring_system (dostęp: 22.08.2024).

[23] Weinstein, C., Campbell, W., Delaney, B., O'leary, G., 2009. *Modeling and Detection Techniques for Counter-Terror Social Network Analysis and Intent Recognition*, https://www.researchgate.net/publication/224407872_Modeling_and_detection_techniques_for_Counter-Terror_Social_Network_Analysis_and_Intent_Recognition (dostęp: 25.08.2024).

[24] Wikipedia, 2024. *Algorytm Viterbiego*, https://pl.wikipedia.org/wiki/Algorytm_Viterbiego (dostęp: 20.08.2024).