


Prognozowanie zagrożeń terrorystycznych jako element systemu antyterrorystycznego¹

Forecasting terrorist threats as an element of the anti-terrorist system

TOMASZ ALEKSANDROWICZ

Akademia Policji w Szczytnie

 <https://orcid.org/0000-0002-3419-5577>

Abstrakt

Artykuł jest poświęcony problematyce prognozowania zagrożeń terrorystycznych i jego roli w systemie antyterrorystycznym państwa. Celem artykułu jest zaprezentowanie metodyki prognozowania zagrożeń terrorystycznych na trzech poziomach: strategicznym, operacyjnym i taktycznym. Przedstawiono podstawowe metody, techniki i narzędzia stosowane w prognozowaniu zagrożeń. Główną tezę artykułu jest stwierdzenie, że prawidłowo przygotowana prognoza pozwala na określenie z wysokim stopniem prawdopodobieństwa możliwości wystąpienia zagrożenia terrorystycznego, jednak zawsze jest to jedynie oszacowanie takiej możliwości, a nie pewność poznawcza. Jako podstawową metodę badawczą zastosowano analizę systemową.

Słowa kluczowe

prognozowanie, zagrożenia terrorystyczne, system antyterrorystyczny

¹ Artykuł powstał na podstawie fragmentów książki: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne*, Warszawa 2022, wydanej przez wydawnictwo Difin. Dokonano zmian redakcyjnych względem oryginału.

Abstract

The article is devoted to the problem of forecasting terrorist threats and its role in the state's anti-terrorist system. The aim of the article is to present the methodology of forecasting terrorist threats at three levels: strategic, operational and tactical. The text presents basic methods, techniques and tools used in threats forecasting. The main thesis of the article is the statement that a properly prepared forecast allows to determine with a high degree of probability the possibility of a terrorist threat, however, in such a case we are always dealing with the assessment of such a possibility, and not with cognitive certainty. System analysis was used as the basic research method.

Keywords

forecasting, terrorist threats, anti-terrorist system

Wprowadzenie

Trudno wyobrazić sobie funkcjonowanie współczesnego państwa i społeczeństwa bez prognozowania, tj. kształtowania choćby przybliżonego obrazu przyszłości i to w każdej niemal dziedzinie życia. Wynika to z prostego faktu: powzięte decyzje będą miały konsekwencje w przyszłości, muszą być zatem podejmowane na podstawie wyobrażeń na jej temat, obserwowanych tendencji, prognozowanych kierunków rozwoju sytuacji, czynników wpływających na ten rozwój. Jest to szczególnie istotne w sferze bezpieczeństwa podmiotu. Prognozowanie to jej niezbędny element, strategie bezpieczeństwa nie mogą bowiem polegać wyłącznie na działaniach reaktywnych, lecz muszą się skupiać na antycypacji zagrożeń. Dotyczy to także strategii zwalczania terroryzmu.

Celem artykułu jest zaprezentowanie metodyki prognozowania zagrożeń terrorystycznych na trzech poziomach: strategicznym, taktycznym i operacyjnym. Jego główna teza to stwierdzenie, że prawidłowo przygotowana prognoza pozwala na określenie z wysokim stopniem prawdopodobieństwa możliwości wystąpienia zagrożenia terrorystycznego, jednak w takim przypadku zawsze wiąże się to jedynie z oszacowaniem takiej możliwości, a nie z pewnością poznawczą. Metoda badawcza wykorzystana do potwierdzenia tezy to analiza systemowa.

Prognozowanie w naukach społecznych

Prognozowanie naukowe jest szczególnym przypadkiem przewidywania przyszłości. Jak twierdził Max Weber, istnieje nieprzekraczalna granica między nauką a wiarą. Wszelkie przypuszczenia są wyprowadzane z rzeczywistości i oparte na prawdach, które potwierdzona empirycznie wiedza jest w stanie zaoferować².

Badacze prezentują stosunkowo jednolite stanowisko co do istoty prognozowania³. Uogólniając, można stwierdzić, że prognoza to sąd, który jest sformułowany z wykorzystaniem dorobku nauki, odnosi się do określonej przyszłości, jest weryfikowalny empirycznie, co oznacza, że musi go cechować precyzja sformułowania i możliwość sprawdzenia jego trafności, oraz jest niepewny, ale poziom tej niepewności jest akceptowalny⁴.

W literaturze przedmiotu pojawia się podział na cztery rodzaje przewidywań przyszłości: prognozę, projekcję, predykcję i *foresight*. Nie zawsze są to podziały o jasno wytyczonych granicach, szczególnie w zastosowaniach praktycznych. Halina Świeboda podkreśla, że te rozróżnienia terminologiczne nie są uzgodnione, ustalone w sposób jednoznaczny, lecz zależą od konwencji przyjmowanych przez różnych autorów i badaczy. Warto jednak było je przywołać dla przejrzystości wyводу⁵.

Robert U. Ayres wyróżnił trzy rodzaje przewidywań⁶:

- prognozę (ang. *forecast*), definiowaną jako wypowiedź na temat przyszłości o rozsądnie wysokim poziomie wiarygodności, przyjmującą na ogół pewne założenia ograniczające w sensie warunku niezmiennego się lub wolno zmieniającego się (np. brak wojen, kryzysów gospodarczych, przewrotów politycznych, innymi słowy brak punktów siodłowych, czyli czynników mogących zmienić trend),
- projekcję (ang. *projection*), rozumianą jako niepewną wypowiedź o przyszłości na ogół dotyczącą jednej z całej grupy możliwości

² Zob. M. Weber, *On the Methodology of the Social Sciences*, Glencoe 1949, s. 110.

³ Przegląd literatury na ten temat w: H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2017, s. 31–45.

⁴ *Prognozowanie gospodarcze. Metody i zastosowania*, M. Cieślak (red.), Warszawa 2005, s. 18, 20.

⁵ Zob. M. Sułek, *Prognozowanie i symulacje międzynarodowe*, Warszawa 2010; H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa...*, s. 22–31.

⁶ R.U. Ayres, *Prognozowanie rozwoju techniki i planowanie długookresowe*, Warszawa 1973, s. 45–46.

- (jednego ze scenariuszy, uznanego przez twórcę projekcją za najbardziej prawdopodobny),
- predykcję (ang. *prediction*), czyli apodyktyczną, podawaną bez zastrzeżeń wypowiedź o przyszłości lub o zdarzeniu jeszcze nieobserwowanym.

W literaturze przedmiotu⁷ wskazuje się na podstawowe metody prognozowania:

- ekstrapolację,
- metody oparte na analogii,
- metody heurystyczne, w tym analizę morfologiczną,
- analizę scenariuszową.

W ostatnich dziesięcioleciach pojawiła się również analiza sieciowa (znana jako SNA, z ang. *social network analysis* – analiza sieci społecznych, niekiedy określana jako analiza struktur sieciowych) oparta na teorii grafów.

Ekstrapolacja trendu, czyli przedłużanie w przyszłość zauważalnych tendencji, jest stosowana do prognozowania rozwoju zdarzeń we względnie stabilnym otoczeniu. Trend to tendencja rozwojowa szeregu czasowego przedstawiająca długookresową skłonność do monotonicznych (jednokierunkowych) zmian prognozowanej zmiennej. Trend jest wynikiem trwałego oddziaływania na konkretne zjawisko danego i rozpoznanego zestawu czynników determinujących kierunek trendu (rosnący, malejący)⁸. Skuteczna prognoza wymaga jednak określenia czynników determinujących badany trend oraz punktów krytycznych (punktów siodłowych).

Metody oparte na analogii (prognozowanie analogowe) sprowadzają się do przenoszenia twierdzeń o jednym przedmiocie badań na inny na podstawie zachodzącego pomiędzy nimi podobieństwa. Za przykład może posłużyć prognozowanie dotyczące konfliktu palestyńsko-izraelskiego przez analogię do konfliktu w Kraju Basków.

Odrębną grupę tworzą metody heurystyczne, zwane niekiedy metodami twórczego myślenia lub metodami eksperckimi. Heurystyka to umiejętność odkrywania nowych prawd przez odpowiednie stawianie pytań, tworzenie hipotez, wyszukiwanie danych i materiałów służących za punkt wyjścia do procesu intelektualnego. Metody te są stosowane do analizy i prognozy zmiennych trudno wymiernych lub niepoddających się kwantyfikacji. Do najpopularniejszych metod heurystycznych zalicza się: burzę

⁷ Zob. T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, s. 32–41.

⁸ Zob. B. Wiśniewski, *Praktyczne aspekty badań bezpieczeństwa*, Warszawa 2020, s. 179.

mózgów, metodę delficką i analizę morfologiczną. Burza mózgów polega, w dużym uproszczeniu⁹, na postawieniu problemu analitycznego przed grupą wybranych ekspertów. Metoda delficka stanowi de facto wariant burzy mózgów. Jej istotą jest opracowanie szczegółowych ankiet dotyczących badanego problemu i kierowanie ich do specjalistów z różnych dziedzin wiedzy. Proces ten ma wiele etapów, respondenci są informowani o wynikach ankiety i w ten sposób dąży się do uzgodnienia bądź ujednolicenia opinii¹⁰.

Analiza morfologiczna jest przeznaczona do strukturyzacji i ustalania relacji w ramach problemów niekwantyfikowalnych (ang. *wicked problems/ social messes*). Metoda polega na uporządkowaniu wybranych parametrów i określeniu ich stanów, co oznacza stworzenie pola morfologicznego oraz ustalenie zgodności (logiczności) pomiędzy różnymi stanami różnych parametrów. Andrzej Dawidczyk zauważa, że zaletą analizy morfologicznej jest różnorodność spełnianych przez nią funkcji. Jego zdaniem to de facto „metoda kombinatoryczna, swoisty stymulator skojarzeń”, który pozwala analitykowi na „kojarzenie obiektów pochodzących z niebranych zazwyczaj pod uwagę zbiorów”¹¹. Analiza morfologiczna jest rozumiana jako (...) *totalna metodologia myślenia i postępowania polegająca na dostrzeganiu takiego obrazu rzeczywistości, w którym uwzględnione byłyby przejrzyste wszystkie ważniejsze powiązania strukturalne między obiektami, zjawiskami, ideami i działaniami*¹².

W prognozowaniu jakościowym najczęściej stosuje się analizę scenariuszową. Scenariusze są definiowane jako „zbiory racjonalnie prawdopodobnych, ale różnych sytuacji w przyszłości”¹³. Przy konstruowaniu scenariusza wychodzi się od analizy bieżącej rzeczywistości w danym jej wycinku,

⁹ Zob. szerzej: K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 182 oraz przywołana tam literatura.

¹⁰ Zob. szerzej: *The Delphi Method. Techniques and Applications*, H.A. Linstone, M. Turoff (red.), Thousand Oaks 2002, https://foresight.pl/assets/downloads/publications/Turoff_Linstone.pdf [dostęp: 7 VI 2024].

¹¹ A. Dawidczyk, J. Jurczak, P. Łuka, *Metody, techniki, narzędzia nauk o bezpieczeństwie*, Warszawa 2019, s. 93.

¹² M. Trocki, M. Wyrozębski, *Zastosowanie analizy morfologicznej w naukach o zarządzaniu, „Organizacja i Kierowanie”* 2014, nr 2 (162), s. 27–28.

¹³ G. Gierszewska, M. Romanowska, *Analiza strategiczna przedsiębiorstwa*, Warszawa 2009, s. 37. Por. *Metody badań nad bezpieczeństwem i obronnością*, P. Sienkiewicz (red.), Warszawa 2010, s. 200, 204–207; A. Dawidczyk, J. Jurczak, P. Łuka, *Metody, techniki, narzędzia...*, s. 89–100.

określa czynniki determinujące i tworzy alternatywne scenariusze na zasadzie „co, jeżeli” (ang. *what if*). Można i należy wykorzystać ustalenia poczynione dzięki ekstrapolacji trendu i określeniu punktów siodłowych.

Analiza sieci społecznych powstała w rezultacie badań nad teorią sieci wywodzącą się z teorii grafów i należy do kategorii metod matematycznych. Jest to narzędzie pozwalające na opracowywanie modeli struktur sieciowych¹⁴.

Stosowanie w praktyce naukowych metod prognozowania

Przystępując do rozważań na temat prognozowania w naukach o bezpieczeństwie, w tym w zakresie prognozowania zagrożeń terrorystycznych, należy podkreślić szczególny związek tej sfery z praktyką. Można w tym kontekście wskazać – ograniczając się do drugiej połowy XX w. – dwa aspekty.

Po pierwsze, analiza środowiska bezpieczeństwa, a więc i prognozowanie jego rozwoju, szczególnie w obszarze zagrożeń, stała się najważniejszą częścią działań na rzecz zapewniania bezpieczeństwa państwa. Przy realizacji zadań związanych z tą analizą sięgano po rozwiązania wykorzystywane w różnych naukach – ekonomii, socjologii, naukach o polityce – i adaptowano je na potrzeby specyfiki bezpieczeństwa państwa. Ważne miejsce zajmuje w tym kontekście analiza systemowa, która ma swoje źródło w biologii¹⁵. Do sfery bezpieczeństwa wprowadził ją sekretarz obrony Stanów Zjednoczonych Robert McNamara, korzystając ze swoich doświadczeń w biznesie. Podobną drogę adaptacji przeszła teoria grafów i jej kontynuacja – teoria sieci, które znalazły swoje zastosowanie nie tylko przy tworzeniu Internetu, lecz także w analizie zagrożeń terrorystycznych¹⁶.

¹⁴ Zob. A.L. Barabási, *Linked. How Everything is Connected to Everything Else and What It Means for Business, Science and Everyday Life*, New York 2009; M. Morzy, A. Ławrynowicz, *Wprowadzenie do analizy sieci społecznych*, <https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf> [dostęp: 7 VII 2018].

¹⁵ Jako datę powstania ogólnej teorii systemów przyjmuje się 1954 r. Zob. L. von Bertalanffy, *Ogólna teoria systemów*, Warszawa 1984.

¹⁶ Zob. J. Wojciechowski, K. Pieńkosz, *Grafy i sieci*, Warszawa 2013; Ch. Leuprecht, O. Walther, *Applying Social Network Analysis to Terrorist Financing*, w: *The Palgrave Handbook of Criminal and Terrorism Financing Law*, C. King, C. Walker, J. Gurulé (red.), Cham 2018, s. 945–966; Ch.C. Yang, N. Liu, M. Sageman, *Analyzing the Terrorist Social Networks with Visualization Tools*, w: *Intelligence and Security Informatics. IEEE International Conference on Intelligence and*

Po drugie, praktyczne zastosowanie metod stworzonych dzięki badaniom naukowym stało się przedmiotem zainteresowania nauki, co doprowadziło do jej swoistego połączenia z praktyką. Zaczęło to być szczególnie widoczne w Stanach Zjednoczonych po drugiej wojnie światowej. Państwo to stało się wtedy globalnym mocarstwem i potrzebowało strategii na taką skalę, a zatem analizy światowego środowiska bezpieczeństwa i prognoz dotyczących szans, wyzwań, zagrożeń i ryzyka. W związku z tym powstała m.in. amerykańska szkoła analizy wywiadowczej¹⁷, w której ramach kształtowały się praktyczne metody analizy wywiadowczej łączące teorię i praktykę, inspirujące badania naukowe, a następnie korzystające z ich efektów. W ten sposób pojawiło się sprzężenie zwrotne pomiędzy nauką a praktyką w obszarze bezpieczeństwa państwa. Jak zauważa Rob Johnston, (...) *analiza wywiadowcza to sztuka, rzemiosło i wiedza. Istnieją specyficzne narzędzia i techniki wykorzystywane przez analityków, jednak ostatecznie to sam analityk musi dokonać osądu i zdecydować o kształcie analizy*¹⁸.

Krótki przegląd metod prognostycznych¹⁹ warto zacząć od modelu SEES proponowanego przez Davida Omanda. Nazwa modelu to akronim utworzony od wyrażen: *situational awareness* (świadomość sytuacji), *explanation* (wyjaśnienie), *estimations* (oszacowania) i *strategic notice* (uwaga, ostrzeżenie strategiczne). Poszczególne etapy tego modelu autor definiuje następująco, wskazując równocześnie problemy i trudności, jakie podczas jego stosowania napotyka analityk:

- świadomość sytuacji – jest to wiedza o tym, co się dzieje i jakie to może powodować zagrożenia. Na tym etapie są obecne wszystkie problemy występujące w fazie oceny sytuacji, czyli luki w informacji czy niechęć do zmiany ocen w miarę pojawiania się nowych dowodów, które są sprzeczne z przyjętymi pierwotnie wyjaśnieniami;
- wyjaśnienie – ten element jest konieczny, fakty bowiem, wbrew potocznemu przekonaniu, nie mówią same za siebie, lecz wymagają

Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006, S. Mehrotra i in. (red.), New York 2006, s. 331–342. Por. T.R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2018, s. 80–84; tenże, *Terroryzm międzynarodowy*, Warszawa 2015, s. 49–51.

¹⁷ Na temat amerykańskiej szkoły analizy wywiadowczej zob. szerzej: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, s. 54–57.

¹⁸ R. Johnston, *Analytic culture in the U.S. Intelligence Community. An Ethnographic Study*, Washington 2005, s. 62.

¹⁹ Zob. szerzej: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, s. 61–72.

wyjaśnień. Należy zatem znaleźć odpowiedzi na pytanie o przyczyny zdarzeń, które zostały wzięte pod uwagę podczas pierwszego etapu budowania prognozy, motywacje zaangażowanych w nie aktorów. W tym przypadku podstawową trudność stanowią problemy ze zrozumieniem działań tych aktorów: ich motywów, roli edukacji i wychowania, jakie były ich udziałem, kultury, w jakiej funkcjonują. Problemy te nabierają szczególnego znaczenia, gdy aktorzy wywodzą się z odmiennych kultur niż osoba tworząca prognozę. Tych trudności doświadczają np. Europejczycy próbujący zrozumieć motywacje islamskich fundamentalistów;

- oszacowanie i prognozy – to odpowiedź na pytanie, jak rozwinie się sytuacja w zależności od przyjęcia różnych założeń. Omand przestrzega, że prognozy mogą się okazać błędne, ponieważ przewidywania analityków mogą zostać zweryfikowane przez niespodziewane zdarzenia, które przy konstrukcji prognozy nie były brane pod uwagę;
- ostrzeżenie strategiczne – dotyczy przyszłych zdarzeń, które w dającej się przewidzieć przyszłości mogą stworzyć zagrożenie. Na tym etapie podstawowymi błędami są zbyt wąskie spojrzenie na rzeczywistość i brak wyobraźni w przewidywaniu rozwoju wydarzeń²⁰.

Znacznie bardziej szczegółową procedurę zawiera model LAMP (Lockwood Analytic Method for Prediction) stworzony przez Jonathana Samuela Lockwooda²¹. Składa się na nią 12 kolejnych kroków. Niektóre wydają się oczywiste, jednak pominięcie któregośkolwiek z nich prowadzi do zafałszowania prognozy.

1. Zdefiniowanie przedmiotu prognozy, czyli tego, na jakie pytanie prognoza ma odpowiedzieć, jaką kwestię rozstrzygnąć.
2. Zdefiniowanie głównych aktorów, których działania mogą się okazać istotne dla rozwoju badanej sytuacji.
3. Ustalenie, jak każdy z aktorów postrzega kwestię będącą przedmiotem prognozy.
4. Określenie wszystkich możliwości działania każdego z rozpatrywanych aktorów.
5. Zbudowanie głównego scenariusza mogącego określić alternatywne przeszłości.

²⁰ D. Omand, *How Spies Think. Ten Lessons in Intelligence*, London 2020, s. 8–13.

²¹ Zob. J. Singh, *The Lockwood Analytical Method for Prediction within a Probabilistic Framework*, „Journal of Strategic Security” 2013, t. 6, nr 3, s. 83–99. Tłumaczenia w tekście pochodzą od autora (dop. red.).

6. Określenie liczby alternatywnych przyszłości dla każdego scenariusza.
7. Porównanie alternatywnych przyszłości w ramach każdego scenariusza, by określić ich relatywne prawdopodobieństwo.
8. Stworzenie rankingu alternatywnych przyszłości, przeanalizowanie scenariuszy od najbardziej do najmniej prawdopodobnego.
9. Przeanalizowanie każdej z alternatywnych przyszłości pod kątem ich konsekwencji dla przedmiotu prognozy określonego w punkcie pierwszym.
10. Ustalenie kluczowych zdarzeń, które stanowią *conditio sine qua non* nastąpienia każdej z alternatywnych przyszłości.
11. Ustalenie dla każdego z takich kluczowych zdarzeń wskaźników, których wystąpienie będzie determinowało ziszczenie się danej alternatywnej przyszłości.
12. Określenie potencjału każdej alternatywnej przyszłości do przekształcenia się w inną alternatywną przyszłość.

Przegląd metod prognostycznych zaliczanych do ustrukturalizowanych technik analitycznych został zawarty w opracowaniu Randolpha H. Phersona i Richardsa J. Heueura Jr.²² Punktem wyjścia do zaprezentowanych technik jest założenie, że niektóre zdarzenia są z natury przewidywalne. Najważniejszy element opracowania prognozy to zatem zidentyfikowanie kluczowych czynników (ang. *key drivers*), które mogą determinować przyszłość, i monitorowanie ich wpływu na rozwój sytuacji, ponieważ mogą one stać się w przyszłości najważniejszym elementem prognozy²³. Warto zwrócić uwagę na to, że nazwy niektórych z tych metod zostały oznaczone znakiem towarowym TM (ang. *trademark*):

- zdefiniowanie kluczowych czynników (*Key Drivers GenerationTM*) jest uznawane przez autorów za punkt wyjścia do dalszej pracy nad prognozą. Chodzi o ustalenie, jakie czynniki będą wpływać na zmianę rozpatrywanej sytuacji, zachowanie aktora itp.;
- ustalenie kluczowych niepewności (*Key Uncertainties FinderTM*), które nie zostały wzięte pod uwagę podczas poprzedniego etapu, a które mogą zyskać status najważniejszych czynników. Innymi słowy to przekształcenie rezultatów analizy dokonanej za pomocą

²² R.H. Pherson, R.J. Heuer Jr., *Structured Analytic Techniques for Intelligence Analysis*, Thousand Oaks 2021.

²³ Tamże, s. 250.

- sprawdzenia kluczowych założeń (*Key Assumptions Check*) w zbiór czynników, które mogą się okazać kluczowe;
- odwrócenie założeń (*Reversing Assumptions*), czyli zakwestionowanie przyjętych założeń i dokonanie analizy sytuacji wobec założeń przeciwnych do tych przyjętych na wstępie. Dotyczy to także założeń ukrytych;
 - proste scenariusze (*Simple Scenarios*) polegające na stworzeniu różnych scenariuszy za pomocą zmieniania siły wpływu poszczególnych kluczowych czynników;
 - stożek wiarygodności (*Cone of Plausibility*) polega na wykorzystaniu kluczowych czynników i założeń w celu stworzenia zakresu prawdopodobnych scenariuszy alternatywnych;
 - analiza przyszłości alternatywnych (*Alternative Futures Analysis*) to metoda systematycznego identyfikowania alternatywnych ścieżek rozwoju sytuacji przez opracowywanie wiarygodnych historii opartych na kluczowych niepewnościach. Ta metoda jest wykorzystywana w ramach prac dużych grup ekspertów;
 - generowanie wielu scenariuszy (*Multiple Scenarios Generation*) wymaga zastosowania metody burzy mózgów. Jej celem jest opracowanie kilku scenariuszy rozwoju sytuacji przy wykorzystaniu różnych niepewności i kluczowych czynników. W zasadzie jest to adaptacja metody *what if*, z zastosowaniem wielu zmiennych, co pozwala na wygenerowanie różnych scenariuszy przy zachowaniu tej samej sytuacji wyjściowej;
 - analiza morfologiczna (*Morphological Analysis*) w uproszczeniu polega na określeniu wielu zmiennych i analizie wszystkich możliwych kombinacji tych zmiennych;
 - rozumowanie kontrfaktyczne (*Counterfactual Reasoning*) to opracowanie prognozy rozwoju sytuacji na podstawie czynników, których istnienia nie stwierdzono, ale które mogą się pojawić, i/lub kluczowych czynników mogących ulec zmianie. Innymi słowy otrzymuje się obraz rozwoju sytuacji determinowanej przez czynniki, których wystąpienie nie jest przewidywane, ale które teoretycznie mogą się pojawić;
 - analiza kontrastujących narracji (*Analysis by Contrasting Narratives*) polega na przeprowadzeniu analizy złożonych problemów przez identyfikowanie narracji związanych z podmiotami zaangażowanymi w rozpatrywane problemy;

- tworzenie wskaźników, walidacja i ewaluacja (*Indicators Generation, Validation, Evaluation*) to metoda polegająca na określeniu, co będzie wskazywało na rozwój sytuacji zgodnych z jednym z prognozowanych scenariuszy rozwoju wydarzeń. Ten zestaw wskaźników jest następnie monitorowany, co pozwala na formułowanie ostrzeżeń na poziomie strategicznym, operacyjnym lub taktycznym przed zdarzeniami stwarzającymi zagrożenie. Prawidłowo wytypowane wskaźniki mają następujące właściwości: poddają się obserwacji, można prześledzić ich występowanie i zmiany, mają istotne znaczenie dla rozwoju sytuacji, są stabilne i jednoznaczne²⁴.

Prognozowanie to najtrudniejsza część analizy informacji. Na temat przeszłości i teraźniejszości można wydawać sądy na podstawie znanych faktów, o przyszłości można wnioskować, opierając się na faktach, które są znane i które dotyczą przeszłości lub teraźniejszości. Na rozwój sytuacji w przyszłości mogą jednak wpływać fakty, które jeszcze nie zaistniały lub – podobnie jak w przypadku przeszłości i teraźniejszości – po prostu nie są znane. Należy zatem podkreślić, że prognoza nigdy nie oznacza pewności, jej wyniki są bardziej lub mniej prawdopodobne. Warto też zwrócić uwagę, że w sferze bezpieczeństwa do określeń „niskie” czy „niewielkie prawdopodobieństwo” podchodzi się inaczej niż w życiu codziennym. W praktyce bezpieczeństwa niskie prawdopodobieństwo wystąpienia zagrożenia nie oznacza, że można je zignorować.

Dawidczyk zauważa, że klasyczne prognozowanie opiera się na analizie tego obszaru rzeczywistości, który udało się poznać. Otrzymuje się w ten sposób fragment obrazu przyszłości ograniczony przyzwyczajeniami, przyjętymi paradygmatami, ukrytymi założeniami, determinowany kanonami myślowymi. Istnieje jednak obszar znajdujący się poza sferą obserwacji, niedostępny ludzkiemu poznaniu. W tym obszarze zachodzą procesy mające bezpośredni i niekiedy decydujący wpływ na rozwój sytuacji w przyszłości²⁵. W opracowaniach poświęconych teorii analizy informacji taką sytuację zwykle nazywano problemem „analizy w sytuacji braku wystarczającej ilości danych” i nakazywano analitykom, by szukali „tego, czego nie ma”²⁶. Uświadomienie sobie, że istnieje konieczność takich

²⁴ Tamże, s. 249–304.

²⁵ Zob. A. Dawidczyk, *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody*, Warszawa 2020, s. 29–30.

²⁶ Zob. T.R. Aleksandrowicz, *Analiza informacji w administracji i w biznesie*, Warszawa 1999, s. 59, 105–107.

poszukiwań intelektualnych, określono „świadomością informacyjną”²⁷. Omand zauważa, że wiedza człowieka o otaczającym świecie jest zawsze fragmentaryczna, niekompletna i nieraz popełnia on błędy w rozpoznaniu sytuacji, gdyż brakuje mu wszystkich potrzebnych informacji, a co więcej – odczuwa niechęć do uznania, że nowe informacje mogłyby zmienić wypracowany już przez niego obraz rzeczywistości. Źródłem problemów są również trudności z rozumieniem motywacji przeciwnika, co wynika m.in. z braku znajomości kultury, w jakiej on funkcjonuje, i wypracowanych przez niego przekonań²⁸.

Jak zauważa Bobby W., (...) *nie istnieje taka technika prognozowania, która byłaby w stanie określić czas wystąpienia faktu zmieniającego trend (timing of nonlinearity)*²⁹. Analityk wywiadu może sformułować prognozę dotyczącą zwiększającego się poziomu skomplikowania planów Al-Kaidy i wzrostu napięcia na Bliskim Wschodzie, ale nie jest w stanie przewidzieć, kiedy samoloty uprowadzone przez terrorystów uderzą w wieże World Trade Center, ani kiedy samopodpalenie sprzedawcy ulicznego w Tunezji doprowadzi do wybuchu niepokoju społecznych. Procesy prowadzące do zmian w aktywności są stopniowe, lecz gdy jakieś zjawisko zaczyna wykraczać poza obserwowany dotychczas schemat, dzieje się to w „jednym dramatycznym momencie” i stanowi nieprzewidywalny punkt krytyczny³⁰. Należy dodać do tego powszechną walkę informacyjną, której elementem jest dezinformacja i wprowadzanie w błąd tych, którzy starają się prognozować przyszłość³¹.

Podsumowując ten wątek, należy podkreślić trzy istotne kwestie. Po pierwsze, rozpoznanie (prognoza) zagrożenia może spowodować zmiany planów, jeśli podmiot, którego działalności dotyczy prognoza, dowie się o tym. Po drugie, wykorzystywanie metod matematycznych w postaci teorii prawdopodobieństwa zawodzi w przypadku prognozowania pojedynczych wydarzeń, jeśli podstawą do zastosowania tych obliczeń jest zbyt mała liczba

²⁷ Zob. np. A.P. Garvin, R. Berkman, *The Art of Being Well Informed. What You Need to Know to Gain the Winning Edge in Business*, New York 1996, s. 25.

²⁸ D. Omand, *How Spies Think...*, s. 11, 19.

²⁹ Bobby W., *An Analyst's Reflections on Forecasting. The Limits of Prediction – or How I Learned to Stop Worrying About Black Swans and Love Analysis*, „Studies in Intelligence” 2019, t. 63, nr 4, s. 9.

³⁰ Tamże.

³¹ Zob. szerzej: J.B. Bruce, *The Rise and Fall of an Intelligence Discipline and its Uncertain Future*, „Studies in Intelligence” 2020, t. 64, nr 1, s. 13–30; *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*, G.K. Haines, R.E. Leggett (red.), Washington 2004.

przypadków. Po trzecie, ekstrapolacja trendu okazuje się niezbyt pomocna w prognozowaniu dramatycznych zmian – wystąpienia punktów siodłowych³². Richard Betts stwierdza wprost, że prognozy ostrzegawcze tworzą pewne kontinuum, niespodziewane ataki zaś stanowią z reguły zakończenie narastających napięć, a nie są czymś w rodzaju *Deus ex machina*. Decydenci muszą zatem bazować głównie na ostrzeżeniach przed zagrożeniami³³.

Prognozowanie zagrożeń terrorystycznych

Prognozowanie zagrożeń terrorystycznych to jedna z trudniejszych i bardziej skomplikowanych kategorii analitycznych. Punktem wyjścia do rozważań jest teza, że terroryści zawsze mają przewagę nad państwem, mogą zaatakować bowiem w wybranym przez siebie momencie, w wybrany przez siebie sposób i przeciwko wybranemu celowi, państwo natomiast nie jest w stanie bronić przez cały czas przed każdym rodzajem zamachu każdego potencjalnego celu. Dotyczy to przede wszystkim państw demokratycznych, ponieważ terroryści wykorzystują podstawowe atrybuty tego ustroju, czyli wolność słowa, dostęp do informacji, swobodę poruszania się, prawo do prywatności. Można zatem stwierdzić, że w ten sposób demokracja sprzyja terroryzmowi – dokonanie zamachu terrorystycznego np. w Korei Północnej jest mało prawdopodobne z uwagi na zaawansowaną inwigilację wszystkich przebywających tam osób. Wolność i demokracja mają swoją cenę – w tym przypadku jest nią zagrożenie zamachami terrorystycznymi³⁴.

Jak zauważa Waldemar Zubrzycki, system przeciwdziałania zagrożeniom o charakterze terrorystycznym powinien się opierać na kilku obszarach oddziaływania państwa. Są to:

- zapobieganie – obejmujące inicjatywy, które mają na celu powstrzymanie poszczególnych osób lub grup osób przed podjęciem działań terrorystycznych;
- zwalczanie – czyli działania wymierzone bezpośrednio w strukturę terrorystyczne w celu ustalenia ich lokalizacji, liczebności, powiązań itp. oraz unieszkodliwienia, ukarania sprawców, a także

³² Zob. R.K. Betts, *Surprise despite warning. Why sudden attacks succeed*, w: *Secret Intelligence: A Reader*, Ch. Andrew, R.J. Aldrich, W.K. Wark (red.), London–New York 2020, s. 111.

³³ Tamże, s. 114.

³⁴ Zob. T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, s. 96–107.

- uniemożliwienia ponownego odtworzenia struktur, systemów komunikowania się czy też źródeł finansowania;
- ochrona – jej zakres dotyczy możliwie najpełniejszego i najskuteczniejszego zabezpieczenia osób oraz całej zagrożonej infrastruktury przed atakami terrorystycznymi;
 - reagowanie – działania związane z minimalizacją skutków ewentualnego zamachu terrorystycznego;
 - prognozowanie – obejmujące analizę rzeczywistych oraz potencjalnych celów, dobór możliwych form, środków i metod działania w odniesieniu do rozmiaru zagrożenia, wykaz potencjalnych ofiar, a także możliwych sprawców zamachów. Obszar ten stanowi swoisty łącznik, spajający cztery wymienione wcześniej elementy, z uwzględnieniem interakcji między nimi³⁵.

W ramach systemu antyterrorystycznego Rzeczypospolitej Polskiej prognozowanie zagrożeń terrorystycznych odbywa się na poziomie operacyjnym, w którego obszarze są realizowane zadania służące koordynacji wymiany informacji między poszczególnymi służbami i instytucjami wchodzącymi w skład systemu antyterrorystycznego, jak również prowadzi się bieżący monitoring i analizę zagrożeń o charakterze terrorystycznym³⁶.

Budowanie prognoz zagrożeń terrorystycznych wymaga zastosowania podejścia systemowego, mówiąc ogólnie – analizy systemowej. W praktyce pociąga to za sobą konieczność tworzenia prognozy zagrożeń terrorystycznych na poziomach: strategicznym, operacyjnym i taktycznym.

Prognozowanie zagrożeń terrorystycznych na poziomie strategicznym

Podstawowym celem prognozy zagrożeń terrorystycznych na poziomie strategicznym jest odpowiedź na zasadnicze pytania: czy takie zagrożenie istnieje? Czy w dającej się przewidzieć przyszłości może zaistnieć konieczność zmierzenia się z nim? Z jakich kierunków może się pojawić? Jaki może mieć charakter? Czy i jakich reakcji państwa to zagrożenie wymaga na poziomie strategicznym? Tym samym jest to klasyczna analiza i prognoza wieloczynnikowa, której rezultaty stanowią podstawę do podejmowania

³⁵ W. Zubrzycki, T. Aleksandrowicz, J. Cymerski, *Terroryzm 2019. Działania antyterrorystyczne*, Warszawa 2019, s. 22–48.

³⁶ Tamże; *Narodowy Program Antyterrorystyczny na lata 2015–2019* (M.P. z 2014 r. poz. 1218, zał.), <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20140001218/O/M20141218.pdf> [dostęp: 7 VI 2024].

decyzji politycznych. Decyzje te wynikają nie tylko z prognozowanych zagrożeń wobec państwa, lecz także z jego zobowiązań prawnomiędzynarodowych, sojuszniczych, takich jak udział w konwencjach wielostronnych, umowach dwustronnych, porozumieniach, sojuszach, czy też z czynników wskazujących na potrzebę przystąpienia do takowych lub intensyfikacji współpracy międzynarodowej w tym zakresie. W sferze polityki wewnętrznej ustalenia prognozy strategicznej powinny być podstawą decyzji o budowie systemu antyterrorystycznego, jego kształcie, elementach składowych i kierunkach rozwoju. Jeżeli taki system już istnieje, określa się kierunki jego udoskonalania w odniesieniu do zmian wskazanych w prognozie.

Punktem wyjścia budowy prognozy zagrożeń terrorystycznych na poziomie strategicznym jest stworzenie relacyjnej bazy danych na temat globalnej skali zamachów w konkretnym przedziale czasowym, co pozwala na określenie trendu w zagrożeniach. Można w tym celu korzystać z baz publicznych, np. START³⁷, Global Terrorism Index³⁸ czy TE-SAT³⁹. Trzeba jednak uwzględnić stosowane w nich kryteria, czyli to, jakie przypadki użycia przemocy są przez twórców poszczególnych baz kwalifikowane jako zamach terrorystyczny. Taka baza musi zawierać nie tylko informacje o dokonanych zamachach, lecz także wiele innych rekordów. Musi też mieć charakter relacyjny, czyli pozwalać na przeszukiwanie na podstawie danych kryteriów.

Taka globalna „mapa” zagrożeń daje tylko ogólny obraz. Aby go uszczegółowić, należy stworzyć na jej podstawie bazy odnoszące się do poziomu zagrożeń terrorystycznych w rozbiciu na regiony i poszczególne państwa (rozkład geograficzny). Budowa prognozy zagrożeń terrorystycznych na poziomie strategicznym jest zatem działaniem złożonym, i co za tym idzie – wymagającym stosowania różnych metod analitycznych i prognostycznych. Do jej opracowania jest konieczna perspektywa striangulowana⁴⁰.

³⁷ *Country Reports on Terrorism – Statistical Annex*, <https://www.start.umd.edu/research-projects/country-reports-terrorism-statistical-annex>.

³⁸ *Overall Terrorism Index Score*, Vision of Humanity, <https://www.visionofhumanity.org/maps/global-terrorism-index/#/>.

³⁹ *European Union Terrorism Situation and Trend report 2023 (TE-SAT)*, <https://www.europol.europa.eu/publications-events/main-reports/tesat-report>.

⁴⁰ Określenie Haliny Świebody oznaczające „połączenie dwóch lub więcej metod badawczych w trakcie analizy tego samego zagadnienia”. Zob. H. Świeboda, *Prognozowanie scenariuszowe w stosunkach międzynarodowych*, w: *Prognozowanie w naukach społecznych. Wymiar narodowy i międzynarodowy*, H. Świeboda (red. nauk.), Warszawa 2018, s. 45.

W związku z tym należy wykorzystać badanie trendu. Niezbędne jest przy tym wskazanie czynników determinujących badany trend oraz określenie punktów siodłowych. Ustalenie korelacji pomiędzy różnymi poziomami zagrożeń terrorystycznych oraz punktów krytycznych pozwala na zastosowanie metod heurystycznych i metod opartych na analogii. Wynik takiej analizy daje z kolei możliwość skorzystania z analizy morfologicznej, zagrożenia terrorystyczne należą bowiem do kategorii problemów niekwantyfikowalnych. Jako parametry występują w tym przypadku tendencje zdefiniowane na poprzednim etapie analizy (czynniki determinujące trend zagrożeń terrorystycznych), a jako stany – np. poziom zagrożeń terrorystycznych, ich charakter i trend w przyszłości. W praktyce rezultaty osiągnięte z zastosowaniem analizy morfologicznej mogą i powinny dotyczyć wszystkich zmiennych branych pod uwagę przy budowaniu bazy danych, a więc nie tylko liczby zamachów, lecz także modus operandi sprawców. Za przykład może posłużyć spadek liczby zamachów samobójczych czy rezygnacja z dużych zamachów (typu zamach na World Trade Center) na rzecz działań podejmowanych przez samotne wilki (ang. *lone wolves*).

Prognoza zagrożeń terrorystycznych na poziomie strategicznym spełnia de facto dwie zasadnicze funkcje. Po pierwsze, stanowi punkt wyjścia do kształtowania polityki antyterrorystycznej państwa. Po drugie, jest podstawą do opracowania prognozy zagrożeń terrorystycznych na poziomie operacyjnym. Jej podstawowy cel to ocena możliwości wystąpienia potencjalnych i realnych zagrożeń bezpieczeństwa i interesów podmiotu bezpieczeństwa, dla którego jest wykonywana.

W polskim *Narodowym Programie Antyterrorystycznym na lata 2015–2019* stwierdzono, że na poziomie operacyjnym systemu antyterrorystycznego są realizowane zadania służące koordynacji wymiany informacji między poszczególnymi służbami i instytucjami wchodzącymi w skład systemu antyterrorystycznego RP, a także są prowadzone: bieżący monitoring oraz analiza zagrożeń o charakterze terrorystycznym.

Prognozowanie zagrożeń terrorystycznych na poziomie operacyjnym

Podobnie jak w przypadku analizy zagrożeń na poziomie strategicznym podstawą do tworzenia prognozy na poziomie operacyjnym jest zbudowanie relacyjnej bazy danych, w której są zawarte incydenty (zdarzenia) dające podstawy do stwierdzenia istniejącego zagrożenia. Ma ona jednak inny charakter niż analogiczna baza danych na poziomie strategicznym,

dotyczy bowiem nie zamachów, do których już doszło, lecz potencjalnych zamachów. Taka baza zawiera informacje zdobywane podczas bieżącego monitoringu zagrożeń terrorystycznych.

W Polsce wśród danych tworzących taką bazę znajdują się m.in. te, które wymienia się w rozporządzeniach ministra spraw wewnętrznych i administracji⁴¹, czy też opracowany przez Agencję Bezpieczeństwa Wewnętrznego *Wykaz incydentów mających wpływ na ocenę ryzyka zagrożenia o charakterze terrorystycznym dla obszarów, obiektów i urzędzeń podlegających obowiązkowej ochronie*⁴². Są to sytuacje wymagające potwierdzenia, że sygnalizowane w ich ramach fakty mają związek z szeroko rozumianą działalnością terrorystyczną, a więc mogą stwarzać zagrożenia terrorystyczne. W języku profesjonalnym takie informacje nazywa się naprowadzeniami operacyjnymi, czyli sytuacjami, które muszą zostać poddane sprawdzeniu i weryfikacji nie tyle pod kątem ich rzeczywistego zaistnienia, ile w kontekście zaistnienia zagrożeń o charakterze terrorystycznym.

Reasumując, pomiędzy prognozami zagrożeń terrorystycznych na poziomach strategicznym i operacyjnym zachodzi sprzężenie zwrotne. Ustalenia zawarte w prognozie strategicznej stanowią niejednokrotnie uzupełnienie prognoz operacyjnych, choćby w przypadku, gdy są wykazywane powiązania między różnymi podmiotami (np. osobami czy firmami zaangażowanymi w działalność terrorystyczną), a z prognozy operacyjnej wynika, że są one zaangażowane w rozpoznawane sytuacje.

O podobnych relacjach można mówić w kontekście stosowania różnego rodzaju zabezpieczeń technicznych obiektów, które zgodnie z prognozą strategiczną mogą zostać uznane za potencjalne cele zamachu terrorystycznego, np. obiekty rządowe czy infrastruktury krytycznej. Z zagrożeń określanych na poziomie strategicznym wynika bowiem konieczność ochrony tych obiektów, w postaci np. kontroli ruchu osobowego. Prognoza na poziomie operacyjnym sygnalizuje możliwość pojawienia się potencjalnego zagrożenia, choćby na podstawie stwierdzenia konkretnych

⁴¹ Zob. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lutego 2017 r. zmieniające rozporządzenie w sprawie katalogu incydentów o charakterze terrorystycznym.*

⁴² *Procedura uzgadniania planu ochrony obszarów, obiektów i urzędzeń podlegających obowiązkowej ochronie w zakresie zagrożeń o charakterze terrorystycznym*, <https://bip.abw.gov.pl/bip/procedury/495,Procedura-uzgadniania-planu-ochrony-obszarow-obiektow-i-urzedzen-podlegajacych-o.html?sid=47275ed2396b07ffaf12903f115c296b> [dostęp: 29 III 2022].

obserwacji. Skutkuje to koniecznością wdrożenia określonych procedur. Wprowadzenie zabezpieczeń technicznych i wcześniejsze przygotowanie wspomnianych procedur było jednak wynikiem ustaleń dokonanych w ramach prognozy na poziomie strategicznym, ich uruchomienie spowodowały natomiast ustalenia zawarte w prognozie na poziomie operacyjnym.

Podobne zależności (sprzężenia zwrotne) zachodzą także w przypadku prognoz na poziomie taktycznym, dotyczą one relacji tej prognozy z jej odpowiednikami na poziomie strategicznym i operacyjnym.

Prognozowanie zagrożeń terrorystycznych na poziomie taktycznym

Na poziomie taktycznym, w przeciwieństwie do prognozy strategicznej, operuje się konkretnymi danymi dotyczącymi zagrożeń, a w przeciwieństwie do prognozy operacyjnej – realnymi, a nie potencjalnymi zagrożeniami. Prognoza zagrożeń terrorystycznych na poziomie taktycznym jest zatem najtrudniejszą kategorią spośród omawianych w niniejszym artykule. Wynika to z trzech czynników:

- krótkiego horyzontu czasowego takiej prognozy (presja czasu),
- konieczności precyzyjności i szczegółowości,
- konieczności „odczytania” intencji terrorystów odnośnie do miejsca (celu) zamachu, czasu, w jakim zostanie on przeprowadzony, i sposobu działania wybranego przez sprawców.

Punktem wyjścia (podstawą) do tworzenia prognoz zagrożeń terrorystycznych na poziomie taktycznym jest kilka kategorii danych. Po pierwsze, są to ustalenia wynikające z prognozy na poziomie strategicznym, czyli główne kierunki zagrożeń, preferowane cele zamachów i sposoby działania sprawców, czas polityczny (np. wybory, strajki i niepokoje społeczne). Na podstawie tych danych można opracować kryteria wyboru celu, czasu i modus operandi sprawców i zastosować je do lokalnych warunków, czyli wytypować obiekty, które mogą się stać celem zamachu, określić prawdopodobny czas zamachu i sposób działania. Po drugie, budując prognozę na poziomie taktycznym, należy wykorzystać dane zawarte w prognozie operacyjnej. Umożliwiają one wytypowanie potencjalnych celów (obiektów) ataków, a więc równocześnie działań polegających na rozpoznaniu ich przez służby kontrterrorystyczne pod kątem charakterystyki terenu, rozkładu pomieszczeń, sposobu ochrony, zabezpieczeń technicznych czy procedur. Po trzecie, należy wykorzystać dane pochodzące z bieżącego rozpoznania operacyjnego, dotyczące stwierdzonych przygotowań do zamachu

lub dokonanego zamachu (precyzyjnie: takiego, który jest w toku), np. w sytuacji wzięcia zakładników.

Tomasz Bajerowski i Anna Kowalczyk są twórcami koncepcji ryzyka urealnionego. Stwierdzają, że (...) *istnieje potrzeba uzupełnienia metod oceny ryzyka o analizę wykonalności (możliwości realizacji) zdarzeń kryzysowych, w których wykonalność (możliwość) to deterministyczna waga zjawiska losowego*⁴³. Ich propozycją jest formuła szacowania ryzyka (za pomocą metody matematycznej) określonych zjawisk lub zdarzeń, która obejmuje wykonalność (możliwość) ich realizacji, ze szczególnym uwzględnieniem zjawisk niemalże nieprawdopodobnych, ale możliwych i mogących wywołać katastrofalne skutki. Autorzy rozgraniczają w tej koncepcji dwa pojęcia: prawdopodobieństwa i możliwości (wykonalności) zajścia zdarzenia⁴⁴.

W literaturze przedmiotu podkreśla się także znaczenie wykorzystania systemów informacji geograficznej (Geographic Information System, GIS)⁴⁵. Jak zauważają Bajerowski i Kowalczyk, GIS jest:

(...) zbiorem danych i informacji z przyporządkowaną lokalizacją geodezyjną. Każda informacja zarejestrowana i przechowywana w GIS ma ściśle określoną lokalizację przestrzenną, a coraz częściej również ściśle określoną 'lokalizację' czasową. Jest to więc system odwzorowujący realną przestrzeń standardowo w układzie 2D i 3D oraz coraz częściej w 4D, co umożliwi prowadzenie analiz dynamicznych. Dynamiczne analizy geoprzestrzenne natomiast są najbliższą przyszłością i koniecznością, zwłaszcza w obszarze działań antykryzysowych w najszerszym tego słowa znaczeniu. GIS jest współczesną formą mapy. Wszystko, co dzieje się w realnym życiu, dzieje się w czasie i przestrzeni, i to wszystko jesteśmy dzisiaj w stanie skartować – sporządzić mapę każdego zjawiska⁴⁶.

W prognozowaniu zdarzeń terrorystycznych może być również pomocna taksonomia numeryczna (szacowanie prawdopodobnych skutków oraz typowanie miejsc ataku). Jej zastosowanie opiera się na założeniu, że cechy przestrzeni są istotnymi atraktorami zdarzeń terrorystycznych, czyli

⁴³ T. Bajerowski, A. Kowalczyk, *Feasibility (Possibility) And Probability In Risk And Crisis Management* (maszynopis powielony w posiadaniu autora).

⁴⁴ Tamże.

⁴⁵ Zob. szerzej: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, s. 150–152.

⁴⁶ T. Bajerowski, A. Kowalczyk, *Metody geoinformacyjnych analiz jawnoźródłowych w zwalczaniu terroryzmu*, Olsztyn 2013, s. 15.

podobny zestaw cech (geoinformacji) charakteryzujący określone miejsce w przestrzeni sprzyja wyborowi tego miejsca jako celu zamachu i powoduje podobne skutki. Zakłada się przy tym, że terroryści nie wybierają celów ataku przypadkowo, lecz posługują się wybranymi przez siebie kryteriami, a zatem miejsca, w których może dojść do ataku, charakteryzują się pewnymi cechami – atraktorami⁴⁷.

Wnioski

Podejmowanie decyzji na podstawie prognoz wiąże się z ryzykiem, ale jednocześnie jest koniecznością. Prognoza opiera się na kilku kategoriach informacji i danych. Przede wszystkim są to dane pochodzące z obszarów, które mogą być poddane poznaniu – można je analizować, wyciągać z nich wnioski, odpowiedzieć na klasyczne pytania analityczne: „co?” i „co z tego?”. To twarde dane, które można nazwać silnymi sygnałami dotyczącymi rozwoju sytuacji w przyszłości. Do drugiej kategorii należą słabe sygnały, a więc takie, które identyfikuje się z trudnością, a które mogą w przyszłości mieć istotny wpływ na rozwój sytuacji. Są to zdarzenia (procesy) stanowiące pewną nowość i albo znajdujące się poza sferą dostępną ludzkiemu poznaniu, albo bagatelizowane. Niekiedy w odniesieniu do nich używa się określenia *slow burning issues*, są bowiem przez dłuższy czas trudno dostrzegalne, a ich wpływ można zauważyć dopiero po dłuższym czasie od pojawienia się pierwszych symptomów. Trzecią kategorią są sądy i przypuszczenia analityka dotyczące obszarów jego niewiedzy. Konieczne jest zatem uświadomienie sobie istnienia tych obszarów i podjęcie próby oszacowania ich zakresu. Należy dodać do tego także te informacje i dane, o których nie chce się wiedzieć. Przyczyny tej niechęci mogą być rozmaite: od politycznych (konieczność podejmowania niepopularnych społecznie decyzji) po psychologiczne (dysonans poznawczy).

Prognoza nigdy zatem nie jest pewnością – jej słuszność może być zweryfikowana wyłącznie po upływie określonego czasu, *post factum*. Dobrze przygotowana sprawa jednak, że przyszłość może być mniej zaskakująca. Skuteczność prognozy, rozumiana jako trafne określenie tego, co zdarzy się w przyszłości, nie jest jednak – szczególnie w obszarze bezpieczeństwa – jedynym kryterium jej oceny. Na jej podstawie często

⁴⁷ Tamże, s. 124.

podejmuje się decyzje, które uniemożliwiają zaistnienie zagrożeń, przed którymi przestrzega prognoza. To oznacza, że była ona nie tylko słuszna, lecz także skuteczna.

Bibliografia

Aleksandrowicz T.R., *Analiza informacji w administracji i w biznesie*, Warszawa 1999.

Aleksandrowicz T.R., *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne*, Warszawa 2022.

Aleksandrowicz T.R., *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2018.

Aleksandrowicz T.R., *Terroryzm międzynarodowy*, Warszawa 2015.

Ayres R.U., *Prognozowanie rozwoju techniki i planowanie długookresowe*, Warszawa 1973.

Bajerowski T., Kowalczyk A., *Feasibility (Possibility) And Probability In Risk And Crisis Management* (maszynopis powielony w posiadaniu autora).

Bajerowski T., Kowalczyk A., *Metody geoinformacyjnych analiz jawnoźródłowych w zwalczaniu terroryzmu*, Olsztyn 2013.

Barabási A.L., *Linked. How Everything is Connected to Everything Else and What It Means for Business, Science and Everyday Life*, New York 2009.

Bertalanffy L. von, *Ogólna teoria systemów*, Warszawa 1984.

Betts R.K., *Surprise Despite Warning: Why Sudden Attacks Succeed*, w: *Secret Intelligence: A Reader*, Ch. Andrew, R.J. Aldrich, W.K. Wark (red.), London–New York 2020.

Bobby W., *The Limits of Prediction – or How I Learned to Stop Worrying About Black Swans and Love Analysis*, „Studies in Intelligence” 2019, t. 63, nr 4, s. 7–16.

Bruce J.B., *The Rise and Fall of an Intelligence Discipline and its Uncertain Future*, „Studies in Intelligence” 2020, t. 64, nr 1, s. 13–30.

Dawidczyk A., *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody*, Warszawa 2020.

Dawidczyk A., Jurczak J., Łuka P., *Metody, techniki, narzędzia nauk o bezpieczeństwie*, Warszawa 2019.

Garvin A.P., Berkman R., *The Art of Being Well Informed. What You Need to Know to Gain the Winning Edge in Business*, New York 1996.

Gierszewska G., Romanowska M., *Analiza strategiczna przedsiębiorstwa*, Warszawa 2009.

Johnston R., *Analytic culture in the U.S. Intelligence Community. An Ethnographic Study*, Washington 2005.

Leuprecht Ch., Walther O., *Applying Social Network Analysis to Terrorist Financing*, w: *The Palgrave Handbook of Criminal and Terrorism Financing Law*, C. King, C. Walker, J. Gurulé (red.), Cham 2018, s. 945–966.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka*, Warszawa 2012.

Metody badań nad bezpieczeństwem i obronnością, P. Sienkiewicz (red.), Warszawa 2010.

Omand D., *How Spies Think. Ten Lessons in Intelligence*, London 2020.

Pherson R.H., Heuer R.J. Jr., *Structured Analytic Techniques for Intelligence Analysis*, Thousand Oaks 2021.

Singh J., *The Lockwood Analytical Method for Prediction within a Probabilistic Framework*, „Journal of Strategic Security” 2013, t. 6, nr 3, s. 83–99.

Sulek M., *Prognozowanie i symulacje międzynarodowe*, Warszawa 2010.

Świeboda H., *Prognozowanie scenariuszowe w stosunkach międzynarodowych*, w: *Prognozowanie w naukach społecznych. Wymiar narodowy i międzynarodowy*, H. Świeboda (red. nauk.), Warszawa 2018.

Świeboda H., *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2017.

Trocki M., Wyrozębski M., *Zastosowanie analizy morfologicznej w naukach o zarządzaniu*, „Organizacja i Kierowanie” 2014, nr 2 (162), s. 27–44.

Watching the Bear: Essays on CIA's Analysis of the Soviet Union, G.K. Haines, R.E. Leggett (red.), Washington 2004.

Weber M., *On the Methodology of the Social Sciences*, Glencoe 1949.

Wiśniewski B., *Praktyczne aspekty badań bezpieczeństwa*, Warszawa 2020.

Wojciechowski J., Pieńkosz K., *Grafy i sieci*, Warszawa 2013.

Yang Ch.C., Liu N., Sageman M., *Analyzing the Terrorist Social Networks with Visualization Tools*, w: *Intelligence and Security Informatics. IEEE International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006*, S. Mehrotra i in. (red.), New York 2006, s. 331–342.

Zubrzycki W., Aleksandrowicz T., Cymerski J., *Terroryzm 2019. Działania antyterrorystyczne*, Warszawa 2019.

Źródła internetowe

Country Reports on Terrorism – Statistical Annex, <https://www.start.umd.edu/research-projects/country-reports-terrorism-statistical-annex>.

European Union Terrorism Situation and Trend report 2023 (TE-SAT), <https://www.europol.europa.eu/publications-events/main-reports/tesat-report>.

Morzy M., Ławrynowicz A., *Wprowadzenie do analizy sieci społecznych*, <https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf> [dostęp: 7 VII 2018].

Overall Terrorism Index Score, Vision of Humanity, <https://www.visionofhumanity.org/maps/global-terrorism-index/#/>.

Procedura uzgadniania planu ochrony obszarów, obiektów i urzędzeń podlegających obowiązkowej ochronie w zakresie zagrożeń o charakterze terrorystycznym, <https://bip.abw.gov.pl/bip/procedury/495,Procedura-uzgadniania-planu-ochrony-obszarow-obiektow-i-urzedzen-podlegajacych-o.html?sid=47275ed2396b07ffaf12903f115c296b> [dostęp: 29 III 2022].

The Delphi Method. Techniques and Applications, H.A. Linstone, M. Turoff (red.), Thousand Oaks 2002, https://foresight.pl/assets/downloads/publications/Turoff_Linstone.pdf [dostęp: 7 VI 2024].

Akty prawne

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lutego 2017 r. zmieniające rozporządzenie w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2017 r. poz. 395).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2016 r. poz. 1092).

Inne dokumenty

Narodowy Program Antyterrorystyczny na lata 2015–2019 (M.P. z 2014 r. poz. 1218, zał.), <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20140001218/O/M20141218.pdf> [dostęp: 7 VI 2024].

Dr hab. Tomasz Aleksandrowicz, prof. APwSz

Prawnik, ekspert ds. bezpieczeństwa. Kierownik Pracowni Walki Informacyjnej Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi Collegium Civitas. Zajmuje się zagadnieniami związanymi z terroryzmem, przestępczością zorganizowaną, nadzorem nad działalnością służb, legislacją w zakresie bezpieczeństwa, stosowaniem środków ograniczających. Autor ponad stu pozycji książkowych i artykułów naukowych na temat różnych aspektów bezpieczeństwa.

Kontakt: tomek.aleksandrowicz@me.com