Terrorism – Studies, Analyses, Prevention, 2024, no. 6: 405–427

https://doi.org/10.4467/27204383TER.24.028.20248

Article

Forecasting terrorist threats as an element of the anti-terrorist system[1]

TOMASZ ALEKSANDROWICZ
https://orcid.org/0000-0002-3419-5577
Police Academy in Szczytno

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

[1] The article is based on excerpts from the book: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne* (Eng. Forecasting terrorist threats. Methodological aspects), Warszawa 2022, published by Difin. Editorial changes have been made to the original.

Introduction

It is difficult to imagine the functioning of a modern state and society without forecasting, i.e. shaping at least an approximate picture of the future, and in almost every area of life. This is due to a simple fact: decisions taken will have consequences in the future, so they must be taken on the basis of perceptions of the future, observed trends, projected directions of situation development, factors influencing this development. This is particularly important in the area of entity security. Forecasting is an indispensable part of it, as security strategies cannot rely solely on reactive measures, but must focus on anticipation of threats. This also applies to counter-terrorism strategies.

The aim of the article is to present a methodology for forecasting terrorist threats at three levels: strategic, tactical and operational. Its main thesis is the statement that a properly prepared forecast makes it possible to determine with a high degree of probability the possibility of a terrorist threat, but in such a case this always involves only an estimation of such a possibility and not cognitive certainty. The research method used to validate the thesis is system analysis.

Forecasting in social sciences

Scientific forecasting is a special case of predicting the future. As Max Weber claimed, there is an impassable boundary between science and faith. All assumptions are derived from reality and based on the truths that empirically confirmed knowledge is able to offer[2].

There is a relatively unified view among researchers on the nature of forecasting[3]. Generalizing, it can be said that a forecast is a judgment that is formulated using scientific knowledge, refers to a specific future, is empirically verifiable, which means that it must be characterised by precision of formulation and verifiability, and is uncertain, but the level of this uncertainty is acceptable[4].

---

[2] See: M. Weber, *On the Methodology of the Social Sciences,* Glencoe 1949, p. 110.

[3] For a review of the literature on this subject, see: H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej* (Eng. Forecasting threats to the national security of the Republic of Poland), Warszawa 2017, pp. 31–45.

[4] *Prognozowanie gospodarcze. Metody i zastosowania* (Eng. Economic forecasting. Methods and Applications), M. Cieślak (ed.), Warszawa 2005, p. 18, 20.

In the literature, a division into four types of future prediction appears: forecast, projection, prediction and foresight. These are not always divisions with clearly defined boundaries, especially in practical applications. Halina Świeboda emphasises that these terminological distinctions are not agreed, established in an unambiguous way, but depend on the conventions adopted by different authors and researchers. However, it was worth recalling them for the clarity of the argument[5].

Robert U. Ayres distinguished three types of predictions[6]:

- *forecast* defined as a statement about the future with a reasonably high level of credibility, generally making certain limiting assumptions in the sense of an unchanging or slowly changing condition (e.g. no wars, economic crises, political upheavals, in other words, no saddle points, i.e. no factors that could change the trend),
- *projection* understood as an uncertain statement about the future generally concerning one of a whole group of possibilities (one of the scenarios considered most likely by the person making the projection),
- *prediction*, i.e. an apodictic, unqualified statement about the future or about an event not yet observed.

The literature[7] points to basic forecasting methods:

- extrapolation,
- methods based on analogy,
- heuristic methods, including morphological analysis,
- scenario analysis.

In recent decades, network analysis (known as SNA, from *social network analysis*, sometimes referred to as network structure analysis), based on graph theory, has also emerged.

Trend extrapolation, the extension into the future of observable trends, is used to forecast the development of events in a relatively stable environment. A trend is a developmental tendency of a time series presenting the long-term propensity for monotonic (unidirectional)

[5] See: M. Sułek, *Prognozowanie i symulacje międzynarodowe* (Eng. Forecasting and international simulations), Warszawa 2010; H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa...*, pp. 22–31.

[6] R.U. Ayres, *Prognozowanie rozwoju techniki i planowanie długookresowe* (Eng. Technological forecasting and long-range planning), Warszawa 1973, pp. 45–46.

[7] See: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, pp. 32–41.

changes in the forecast variable. A trend is the result of the sustained effect on a particular phenomenon of a given and recognised set of factors determining the direction of the trend (increasing, decreasing)[8]. However, effective forecasting requires the identification of the determinants of the trend under study and the critical points (saddle points).

Methods based on analogy (analogue forecasting) boil down to transferring claims about one object of study to another on the basis of the similarity between them. An example is forecasting the Palestinian-Israeli conflict by analogy with the conflict in the Basque Country.

A separate group is formed by heuristic methods, sometimes referred to as creative thinking methods or expert methods. Heuristics are the ability to discover new truths by appropriately posing questions, forming hypotheses, and searching for data and materials that serve as a starting point for the intellectual process. These methods are used to analyse and predict variables that are difficult to quantify or are unquantifiable. The most popular heuristic methods include brainstorming, the Delphi method and morphological analysis. Brainstorming consists, in a nutshell[9], of putting an analytical problem in front of a group of selected experts. The Delphi method is a de facto variant of brainstorming. Its essence is to develop detailed questionnaires on the problem under investigation and to address them to specialists in various fields of knowledge. The process has a number of stages, the respondents are informed of the results of the survey and in this way an attempt is made to agree or harmonise opinions[10].

Morphological analysis is designed to structure and establish relationships within non-quantifiable problems (*wicked problems/ social messes*). The method involves ordering selected parameters and determining their states, which means creating a morphological field and establishing correspondences (logicality) between different states of different parameters. Andrzej Dawidczyk notes that an advantage

[8] See: B. Wiśniewski, *Praktyczne aspekty badań bezpieczeństwa* (Eng. Practical aspects of security research), Warszawa 2020, p. 179.

[9] See in more detail: K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka* (Eng. Information analysis. Theory and practice), Warszawa 2012, p. 182 and the literature cited therein.

[10] See in more detail: *The Delphi Method. Techniques and Applications*, H.A. Linstone, M. Turoff (eds.), Thousand Oaks 2002, https://foresight.pl/assets/downloads/publications/Turoff_Linstone.pdf [accessed: 7 VI 2024].

of morphological analysis is the variety of functions it performs. In his view, it is a de facto "combinatorial method, a kind of association stimulator" that allows the analyst to "associate objects from sets not usually considered"[11]. Morphological analysis is understood as (…) *a total methodology of thinking and acting by perceiving such a picture of reality in which all major structural connections between objects, phenomena, ideas and actions would be taken into account transparently*[12].

Scenario analysis is most commonly used in qualitative forecasting. Scenarios are defined as "sets of reasonably likely but different future situations"[13]. When constructing a scenario, one starts from an analysis of the current reality in a given slice of it, identifies the determining factors and creates alternative scenarios on a "what if" basis. Findings made by extrapolating the trend and identifying saddle points can and should be used.

Social network analysis emerged from research into network theory derived from graph theory and belongs to the category of mathematical methods. It is a tool for developing models of network structures[14].

Putting scientific forecasting methods into practice

In proceeding to a consideration of forecasting in the security sciences, including terrorist threat foresight, it is important to emphasise the particular relationship of this sphere to practice. It is possible to

[11] A. Dawidczyk, J. Jurczak, P. Łuka, *Metody, techniki, narzędzia nauk o bezpieczeństwie* (Eng. Methods, techniques, tools of security sciences), Warszawa 2019, p. 93.

[12] M. Trocki, M. Wyrozębski, *Zastosowanie analizy morfologicznej w naukach o zarządzaniu* (Eng. The use of morphological analysis in management sciences), "Organizacja i Kierowanie" 2014, no. 2 (162), pp. 27–28.

[13] G. Gierszewska, M. Romanowska, *Analiza strategiczna przedsiębiorstwa* (Eng. Strategic analysis of the company), Warszawa 2009, p. 37. Cf. *Metody badań nad bezpieczeństwem i obronnością* (Eng. Security and defence research methods), P. Sienkiewicz (ed.), Warszawa 2010, p. 200, 204–207; A. Dawidczyk, J. Jurczak, P. Łuka, *Metody, techniki, narzędzia*..., pp. 89–100.

[14] See: 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* (Eng. Introduction to social network analysis), https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf [accessed: 7 VII 2018].

identify in this context - limiting ourselves to the second half of the 20th century - two aspects.

Firstly, the analysis of the security environment, and thus the forecasting of its development, especially in the area of threats, became the most important part of efforts to ensure state security. In carrying out the tasks associated with this analysis, solutions used in various sciences - economics, sociology, political science - were drawn upon and adapted to the specific needs of state security. Systems analysis, which has its origins in biology, has an important place in this context[15]. It was introduced into the security sphere by U.S. Secretary of Defence Robert McNamara, drawing on his experience in business. Graph theory and its continuation, network theory, have undergone a similar path of adaptation and have found their way not only into the creation of the internet, but also into the analysis of terrorist threats[16].

Secondly, the practical application of methods created through scientific research became the focus of science, which led to its peculiar merging with practice. This began to be particularly evident in the United States after the Second World War. The country then became a global superpower and needed a strategy on this scale and therefore an analysis of the global security environment and forecasts of opportunities, challenges, threats and risks. This gave rise, among other things, to the American school of intelligence analysis[17], within which practical methods of intelligence analysis were shaped, combining theory and practice, inspiring scientific research and then benefiting from its results. Thus, a feedback loop has

[15] 1954 is taken as the date of origin of general systems theory. See: L. von Bertalanffy, *Ogólna teoria systemów* (Eng. General systems theory), Warszawa 1984.

[16] See: J. Wojciechowski, K. Pieńkosz, *Grafy i sieci* (Eng. Graphs and networks), Warszawa 2013; Ch. Leuprecht, O. Walther, *Applying Social Network Analysis to Terrorist Finansing*, in: *The Palgrave Handbook of Criminal and Terrorism Financing Law*, C. King, C. Walker, J. Gurulé (eds.), Cham 2018, pp. 945–966; Ch.C. Yang, N. Liu, M. Sageman, *Analyzing the Terrorist Social Networks with Visualization Tools*, in: *Intelligence and Security Informatics. IEEE International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006*, S. Mehrotra et al. (eds.), New York 2006, pp. 331–342. Cf. T.R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego* (Eng. The world in the network: states – societies – people. In search of a new paradigm of national security), Warszawa 2018, pp. 80–84; idem, *Terroryzm międzynarodowy* (Eng. International terrorism), Warszawa 2015, pp. 49–51.

[17] On the U.S. school of intelligence analysis, see in more detail: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych*..., pp. 54–57.

emerged between science and practice in the area of state security. As Rob Johnston notes, (…) *intelligence analysis is art, tradecraft, and science. There are specific tools and techniques to help perform the tasks, but, in the end, it is left to individuals to use their best judgment in making decisions*[18].

It is worth starting a brief overview of forecasting methods[19] with the SEES model proposed by David Omand. The name of the model is an acronym formed from the expressions: situational awareness, explanation, estimations and strategic notice. He defines the various stages of the model as follows, while pointing out the problems and difficulties the analyst encounters when applying it:

- situational awareness - is the knowledge of what is happening and what risks it may cause. All the problems that occur in the situation assessment phase are present at this stage, i.e. gaps in information or reluctance to change assessments as new evidence emerges that contradicts the explanations originally accepted;
- explanation - this element is necessary, because facts, contrary to popular belief, do not speak for themselves, but require explanations. It is therefore necessary to find answers to the causes of the events that were taken into account during the first stage of building the forecast, the motivations of the actors involved. In this case, the main difficulty is in understanding the actions of these actors: their motives, the role of education and upbringing they were involved in, the culture in which they operate. These problems become particularly important when the actors come from different cultures than the person making the forecast. These difficulties are experienced, for example, by Europeans trying to understand the motivations of Islamic fundamentalists;
- estimations and forecasts - is the answer to the question of how the situation will develop depending on the different assumptions made. Omand warns that forecasts can turn out to be wrong, as analysts' predictions can be verified by unexpected events that were not taken into account when constructing the forecast;
- strategic notice - is concerned with future events that may pose a risk in the foreseeable future. At this stage, the fundamental

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

[19] See in more detail: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, pp. 61–72.

errors are a too narrow view of reality and a lack of imagination in anticipating the development of events[20].

A much more detailed procedure is contained in the LAMP (Lockwood Analytic Method for Prediction) model created by Jonathan Samuel Lockwood[21]. It consists of 12 consecutive steps. Some seem obvious, but omitting any of them leads to falsification of the prediction.

1. Define the object of the forecast, i.e. what question the forecast is supposed to answer, what issue it is supposed to resolve.
2. Define the main actors whose actions are likely to be relevant to the development of the situation under review.
3. Determine how each actor perceives the issue being forecast.
4. Identify all possibilities for action by each of the actors under consideration.
5. Build a main scenario that can define alternative futures.
6. Determine the number of alternative futures for each scenario.
7. Compare alternative futures within each scenario to establish their relative probability.
8. Create a ranking of alternative futures, analysing the scenarios from most to least likely.
9. Analyse each alternative futures in terms of their implications for the subject of the forecast identified in step one.
10. Identify the focal events that constitute the *conditio sine qua non* of the occurrence of each alternative future.
11. Identify for each such focal event the indicators whose occurrence will determine the realisation of that alternative future.
12. Determine the potential of each alternative future to transform into another alternative future.

An overview of forecasting methods categorised as structured analytical techniques is provided by Randolph H. Pherson and Richards J. Heueur Jr.[22] The starting point for the techniques presented is the assumption that some events are inherently predictable. The most important part of developing a forecast is therefore to identify the key drivers that may determine the future and to monitor their impact on

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

[21] Singh, *The Lockwood Analytical Method for Prediction within a Probabilistic Framework*, "Journal of Strategic Security" 2013, vol. 6, no. 3, pp. 83–99.

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

developments, as they may become the most important element of the forecast in the future[23]. It is worth noting that the names of some of these methods have been marked with a ™ trademark:

- Defining Key Drivers Generation™ is considered by the authors to be the starting point for further forecasting work. The idea is to determine what factors will change the situation under consideration, the behaviour of the actor, etc;
- the identification of Key Uncertainties Finder™ that have not been taken into account during the previous step, and which may gain the status of the most important factors. In other words, it is the transformation of the results of the analysis made by means of the Key Assumptions Check into a set of factors that may turn out to be key;
- Reversing Assumptions, i.e. questioning the assumptions made and analysing the situation in the face of assumptions opposite to those made initially. This includes implicit assumptions;
- Simple Scenarios, which involves creating different scenarios by varying the strength of influence of individual key factors;
- Cone of Plausibility - involves using key factors and assumptions to create a range of plausible alternative scenarios;
- Alternative Futures Analysis is a method for systematically identifying alternative pathways by developing plausible stories based on key uncertainties. This method is used in the work of large expert groups;
- Multiple Scenarios Generation - involves a brainstorming method. Its aim is to develop several scenarios of how things could develop using different uncertainties and key factors. In essence, it is an adaptation of the *what-if* method, using multiple variables to generate different scenarios while keeping the same initial situation;
- Morphological Analysis in simple terms it involves identifying multiple variables and analysing all possible combinations of these variables;
- Counterfactual Reasoning is the formulation of a forecast of the situation development on the basis of factors that have not been identified but which may emerge, and/or key factors that may

[23] Ibid.

change. In other words, one obtains a picture of the development of a situation determined by factors that are not predicted to occur, but that could theoretically occur;
- Analysis by Contrasting Narratives - involves conducting an analysis of complex problems by identifying narratives related to the actors involved in the problems under consideration;
- Indicators Generation, Validation, Evaluation is a method of identifying what will indicate developments that are consistent with one of the projected event scenarios. This set of indicators is then monitored, allowing warnings to be formulated at a strategic, operational or tactical level against risk events. Correctly selected indicators have the following properties: they are observable, their occurrence and changes can be traced, they are relevant to developments, they are stable and unambiguous[24].

Forecasting is the most difficult part of information analysis. Judgements can be made about the past and present on the basis of known facts, and judgements can be made about the future based on facts that are known and that relate to the past or present. However, future developments may be influenced by facts that have not yet occurred or - as in the case of the past and present - that are simply not known. It should therefore be emphasised that a forecast never implies certainty, its results are more or less likely. It is also worth noting that the terms "low" or "low probability" are approached differently in the security sphere than in everyday life. In security practice, a low probability of a threat does not mean that it can be ignored.

Dawidczyk notes that classical forecasting is based on an analysis of that area of reality which has become known. One thus obtains a fragment of a picture of future limited by habits, accepted paradigms, implicit assumptions, determined by canons of thought. However, there is an area beyond the sphere of observation, inaccessible to human cognition. In this area, processes take place that have a direct and sometimes decisive impact on future developments[25]. In studies devoted to the theory of information analysis, such a situation was usually referred to as the problem of "analysis in the absence of sufficient data" and directed analysts to look for "what is

[24] Ibid., pp. 249–304.

[25] See: A. Dawidczyk, *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody* (Eng. Strategic analysis in state security. Selected methods), Warszawa 2020, pp. 29–30.

not there"[26]. The realisation that there is a need for such an intellectual search has been termed informational awareness[27]. Omand notes that man's knowledge of the world around him is always fragmentary, incomplete and he sometimes makes mistakes in recognising situations because he lacks all the information he needs and, moreover, feels reluctant to recognise that new information could change the picture of reality he has already developed. Difficulties in understanding the motivation of the opponent are also a source of problems, due, among other things, to a lack of knowledge of the culture in which he operates and the beliefs he has developed[28].

As Bobby W. notes, (…) *there is no such forecasting technique that is able to determine the timing of a trend-changing fact (timing of nonlinearity)*[29]. An intelligence analyst can formulate a forecast about the increasing sophistication of al-Qaeda's plans and the rising tension in the Middle East, but he cannot predict when terrorist-hijacked planes will hit the World Trade Center towers or when the self-immolation of a street vendor in Tunisia will lead to civil unrest. The processes leading to changes in activity are gradual, but when a phenomenon starts to go beyond the pattern observed so far, it happens in "one dramatic moment" and represents an unpredictable tipping point[30]. Add to this the widespread information warfare, part of which is disinformation and misleading those who try to forecast the future[31].

To summarise this theme, three important points should be highlighted. Firstly, the identification (forecast) of a threat may result in changes to plans if the subject of the forecast becomes aware of it. Secondly, the use of mathematical methods in the form of probability theory fails when forecasting single events if the basis for applying these calculations

[26] See: T.R. Aleksandrowicz, *Analiza informacji w administracji i w biznesie* (Eng. Information analysis in administration and business), Warszawa 1999, p. 59; 105–107.

[27] See e.g.: 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, p. 25.

[28] D. Omand, *How Spies Think*..., p. 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 Angels*, "Studies in Intelligence" 2019, vol. 63, no. 4, p. 9.

[30] Ibid.

[31] See in more detail: J.B. Bruce, *The Rise and Fall of an Intelligence Discipline and its Uncertain Future*, "Studies in Intelligence" 2020, vol. 64, no. 1, pp. 13–30; *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*, G.K. Haines, R.E. Leggett (eds.), Washington 2004.

is too few cases. Thirdly, trend extrapolation proves not very helpful in forecasting dramatic changes - the occurrence of saddle points[32]. Richard Betts states explicitly that warning forecasts form a continuum, while unexpected attacks are usually the end of escalating tensions, rather than a kind of *Deus ex machina*. Decision-makers therefore need to rely primarily on threat warnings[33].

Terrorist threats forecasting

Forecasting terrorist threats is one of the more difficult and complex analytical categories. The starting point for this discussion is the thesis that terrorists always have an advantage over the state, as they can attack at a time, in a manner and against a target of their choice, while the state is not able to defend every potential target against every type of attack at all times. This is especially true in democratic states, as terrorists exploit the basic attributes of that system, namely freedom of speech, access to information, freedom of movement, and the right to privacy. It could therefore be argued that democracy thus encourages terrorism - the perpetration of a terrorist attack in North Korea, for example, is unlikely due to the advanced surveillance of everyone there. Freedom and democracy come at a price - in this case the threat of terrorist attacks[34].

As Waldemar Zubrzycki notes, the system for countering terrorist threats should be based on several areas of state influence. These are:

- prevention - which includes initiatives aimed at deterring individuals or groups of individuals from engaging in terrorist activities;
- combating - that is, actions that directly target terrorist structures in order to determine their location, numbers, links, etc., and to neutralise, punish the perpetrators, and prevent the re-establishment of structures, communication systems or sources of funding;

[32] See: R.K. Betts, *Surprise despite warning. Why sudden attacks succeed*, in: *Secret Intelligence: A Reader*, Ch. Andrew, R.J. Aldrich, W.K. Wark (eds.), London–New York 2020, p. 111.

[33] Ibid., p. 114.

[34] See: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych*..., pp. 96–107.

– protection - its scope is concerned with securing individuals and the entire infrastructure under threat as fully and effectively as possible against terrorist attacks;
– response - activities related to minimising the consequences of a possible terrorist attack;
– forecasting - involving an analysis of actual and potential targets, the selection of possible forms, means and methods of action in relation to the size of the threat, a list of potential victims, as well as possible perpetrators. This area represents a kind of link, uniting the four elements mentioned earlier, taking into account the interaction between them[35].

Within the anti-terrorist system of the Republic of Poland, forecasting of terrorist threats is carried out at the operational level, in the area of which tasks are performed to coordinate the exchange of information between individual services and institutions that are part of the anti-terrorist system, as well as ongoing monitoring and analysis of threats of a terrorist nature[36].

Building forecasts of terrorist threats requires a systems approach, generally speaking a systems analysis. In practice, this entails building terrorist threat forecasts at strategic, operational and tactical levels.

Forecasting terrorist threats at strategic level

The primary objective of terrorist threat forecasting at a strategic level is to answer the fundamental questions: does such a threat exist? Might it need to be confronted in the foreseeable future? From what directions might it emerge? What might be its nature? Does this threat require, and what state responses does it require at the strategic level? Thus, it is a classic multi-factor analysis and forecast, the results of which form the basis for policy decisions. These decisions not only derive from the projected threats against the state, but also from the state's international legal, alliance obligations, such as participation in multilateral conventions, bilateral agreements, accords, alliances, or from factors indicating the need to join such or to intensify international cooperation in this regard. In the sphere

[35] W. Zubrzycki, T. Aleksandrowicz, J. Cymerski, *Terroryzm 2019. Działania antyterrorystyczne* (Eng. Terrorism 2019. Anti-terrorist activities), Warszawa 2019, pp. 22–48.

[36] Ibid: *Narodowy Program Antyterrorystyczny na lata 2015–2019* (Eng. National Anti-Terrorist Programme for 2015-2019), (M.P. of 2014, item 1218, app.), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20140001218/O/M20141218.pdf [accessed: 7 VI 2024].

of internal policy, the findings of the strategic forecast should be the basis for decisions on the construction of the anti-terrorist system, its shape, components and directions of development. If such a system already exists, directions for its improvement in relation to the changes indicated in the forecast.

The starting point for the construction of a terrorist threat forecast at the strategic level is the creation of a relational database on the global scale of attacks in a specific time period, which allows the identification of a trend in threats. Public databases can be used for this purpose, e.g. START[37], Global Terrorism Index[38] or TE-SAT[39]. However, it is necessary to take into account the criteria they use, i.e. which incidents of violence are classified as terrorist attacks by the creators of each database. Such a database must contain not only information about the attacks committed, but also many other records. It must also be relational in nature, i.e. allow searches based on given criteria.

Such a global "map" of threats only gives a general picture. In order to make it more detailed, it should be used to create databases relating to the level of terrorist threats by region and individual country (geographical distribution). The construction of a terrorist threat forecast at the strategic level is therefore a complex exercise, and thus requires the use of various analytical and forecasting methods. A triangulated perspective[40] is required for its development.

A trend study should therefore be used. In doing so, it is necessary to identify the determinants of the trend under study and to determine the saddle points. The determination of correlations between the different levels of terrorist threats and the critical points allow the use of heuristic and analogy-based methods. The result of such an analysis, in turn,

[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] A term coined by Halina Świeboda to mean "the combination of two or more research methods when analysing the same issue". See: H. Świeboda, *Prognozowanie scenariuszowe w stosunkach międzynarodowych* (Eng. Scenario forecasting in international relations) in: *Prognozowanie w naukach społecznych. Wymiar narodowy i międzynarodowy* (Eng. Forecasting in the social sciences. National and international dimensions), H. Świeboda (sci. ed.), Warszawa 2018, p. 45.

provides an opportunity to use morphological analysis, as terrorist threats belong to the category of non-quantifiable problems. In this case, the trends defined at the previous stage of the analysis (factors determining the trend of terrorist threats) are used as parameters, and the level of terrorist threats, their nature and future trend, for example, are used as states. In practice, the results achieved using morphological analysis can and should apply to all the variables taken into account when building the database, so not only the number of attacks, but also the modus operandi of the perpetrators. The decline in the number of suicide attacks or the abandonment of major attacks (of the World Trade Center type) in favour of lone wolves operations can serve as examples.

The terrorist threat forecast at the strategic level fulfils de facto two essential functions. Firstly, it provides the starting point for shaping the state's counter-terrorism policy. Secondly, it is the basis for developing a terrorist threat forecast at the operational level. Its primary purpose is to assess the possibility of potential and real threats to the security and interests of the security entity for which it is carried out.

The Polish *National Anti-Terrorist Programme for 2015-2019* states that at the operational level of the anti-terrorist system, tasks are carried out to coordinate the exchange of information between individual services and institutions that are part of the anti-terrorist system of the Republic of Poland, as well as: ongoing monitoring and analysis of terrorist threats.

Forecasting terrorist threats at operational level

As in the case of threat analysis at the strategic level, the basis for creating a forecast at the operational level is the construction of a relational database, which includes incidents (events) giving grounds for the determination of an existing threat. However, the nature of this database is different from that of a similar database at strategic level, as it is not concerned with attacks that have already occurred, but with potential attacks. Such a database contains information obtained during the ongoing monitoring of terrorist threats.

In Poland, among the data forming such a database are those listed in the regulations of the Minister of the Interior and Administration[41], or

[41] See: *the Ordinance of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist incidents and Ordinance of the Minister of the Interior and Administration of 24 February 2017 amending the Ordinance on the catalogue of terrorist incidents*.

The list of incidents affecting the assessment of the risk of a terrorist threat for areas, facilities and equipment subject to mandatory protection, developed by the Internal Security Agency[42]. These are situations that require confirmation that the facts signalled within them are related to terrorist activities in the broadest sense, and therefore may pose terrorist threats. In professional language, such information is referred to as operational leads, i.e. situations that must be checked and verified not so much in terms of their actual occurrence, but in terms of the existence of terrorist threats.

In conclusion, there is a feedback loop between terrorist threat forecasts at the strategic and operational levels. The findings of the strategic forecast are sometimes complementary to the operational forecasts, if only when links between different actors (e.g. individuals or companies involved in terrorist activities) are demonstrated and the operational forecast shows that they are involved in the identified situations.

A similar relationship can be referred to in the context of the application of various types of technical security to facilities which, according to the strategic forecast, may be considered potential targets of a terrorist attack, e.g. government facilities or critical infrastructure. This is because the threats identified at the strategic level imply the need to protect these facilities, in the form of, for example, control of personal traffic. A forecast at the operational level signals the possibility of a potential threat, if only on the basis of a finding of specific observations. This results in the need to implement certain procedures. However, the introduction of technical safeguards and the prior preparation of these procedures was the result of the findings of the strategic-level forecast, their activation was triggered by the findings of the operational-level forecast.

Similar relationships (feedbacks loops) also exist for the forecasts at the tactical level, concerning the relationship of this forecast with its counterparts at the strategic and operational levels.

Forecasting terrorist threats at tactical level

At the tactical level, unlike strategic forecasting, one operates with concrete threat data and, unlike operational forecasting, with real, rather than potential, threats. Terrorist threat forecasting at the tactical level is

[42] *Procedure for agreeing a security plan for areas, facilities and equipment subject to mandatory protection with regard to terrorist threats*, https://bip.abw.gov.pl/bip/procedury/495,Procedura-uzgadniania-planu-ochrony-obszarow-obiektow-i-urzadzen-podlegajacych-o.html?sid=47275ed2396b07ffaf12903f115c296b [accessed: 29 III 2022].

therefore the most difficult category of those discussed in this article. This is due to three factors:

- the short time horizon of such a forecast (time pressure),
- the need for precision and detail,
- the need to "read" the terrorists' intentions regarding the place (target) of the attack, the time at which it will be carried out, and the modus operandi chosen by the perpetrators.

The starting point (basis) for creating terrorist threat forecasts at the tactical level is several categories of data. Firstly, there are the findings from the forecast at the strategic level, i.e. the main threat directions, the preferred targets of attacks and modus operandi of perpetrators, the political time (e.g. elections, strikes and civil unrest). On the basis of these data, the criteria for the selection of the target, time and modus operandi of the perpetrators can be developed and applied to local conditions, i.e. the selection of objects that can become the target of an attack, the determination of the likely time of the attack and the modus operandi. Secondly, when building a forecast at the tactical level, the data contained in the operational forecast should be used. They make it possible to select the potential targets (objects) of attacks, and thus, at the same time, actions consisting in their recognition by counter-terrorist services in terms of the characteristics of the terrain, the layout of the premises, the method of protection, technical security or procedures. Thirdly, data from ongoing operational reconnaissance should be used on identified preparations for an attack or an executed attack (precisely: in progress), e.g. in a hostage-taking situation.

Tomasz Bajerowski and Anna Kowalczyk are the originators of the concept of realised risk. They state that (...) *there is a need to complement risk assessment methods with an analysis of the feasibility (possibility of realisation) of crisis events, where feasibility (possibility) is the deterministic weight of a random phenomenon*[43]. Their proposal is a formula for estimating the risk (by means of a mathematical method) of specific phenomena or events, which includes the feasibility (possibility) of their realisation, with a particular focus on phenomena that are almost improbable, but possible and capable of causing catastrophic consequences. The authors distinguish

[43] T. Bajerowski, A. Kowalczyk, *Feasibility (Possibility) And Probability In Risk And Crisis Management*, (reproduced typescript in the author's possession).

between two terms in this concept: the probability and the possibility (feasibility) of an event occurring[44].

The literature also highlights the importance of using Geographic Information Systems (GIS)[45]. As Bajerowski and Kowalczyk notes, GIS is:

> (...) a collection of data and information with an assigned geodetic location. Every piece of information recorded and stored in a GIS has a strictly defined spatial location and, increasingly, an equally strictly defined temporal "location". It is therefore a system that maps real space in 2D and 3D as a standard, and increasingly in 4D, which enables dynamic analyses. Dynamic geospatial analyses, on the other hand, are the immediate future and a necessity, especially in the area of anti-crisis operations in the broadest sense of the word. GIS is the modern form of the map. Everything that happens in real life happens in time and space, and we are able to map it all today - to make a map of any phenomenon[46].

Numerical taxonomy (estimation of likely effects and typing of attack sites) can also be helpful in predicting terrorist events. Its application is based on the assumption that features of space are important attractors of terrorist events, i.e. a similar set of features (geo-information) characterising a certain place in space favours the selection of that place as an attack target and causes similar effects. This assumes that terrorists do not choose their attack targets at random, but use criteria of their own choosing, and therefore the places where an attack may take place are characterised by certain features - attractors[47].

Conclusions

Making decisions on the basis of forecasts involves risks, but at the same time is a necessity. Forecasting is based on several categories of information

[44] Ibid.

[45] See in more detail: T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych...*, pp. 150–152.

[46] T. Bajerowski, A. Kowalczyk, *Metody geoinformacyjnych analiz jawnoźródłowych w zwalczaniu terroryzmu* (Eng. Geoinformation methods for open-source analysis in combating terrorism), Olsztyn 2013, p. 15.

[47] Ibid., p. 124.

and data. First of all, it is data from areas that can be subjected to cognition - it can be analysed, conclusions can be drawn from it, the classic analytical questions can be answered: "what?" and "so what?". These are hard data that can be called strong signals about future developments. The second category includes weak signals, i.e. those that are identified with difficulty, but which may have a significant impact on future developments. These are events (processes) that represent some novelty and are either outside the realm accessible to human cognition or downplayed. Sometimes the term *slow burning issues* is used to refer to them, as they are difficult to perceive for a long time and their impact can only be noticed after a long time after the first symptoms appear. The third category is the analyst's judgements and assumptions about his or her areas of ignorance. It is therefore necessary to be aware of these areas and to try to estimate their extent. It is also necessary to add to this the information and data that one does not want to know about. The reasons for this reluctance can range from political (having to make socially unpopular decisions) to psychological (cognitive dissonance).

A forecast is therefore never a certainty - its validity can only be verified after a certain period of time, post factum. If well prepared, however, the future may be less surprising. However, especially in the security field, the effectiveness of a forecast is not the only criterion for its evaluation. On the basis of the forecast, decisions are often taken that prevent the occurrence of the risks that the forecast warns against. This means that it was not only correct, but also effective.

Bibliography

Aleksandrowicz T.R, *Analiza informacji w administracji i w biznesie* (Eng. Information analysis in administration and business), Warszawa 1999.

Aleksandrowicz T.R, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne* (Eng. Forecasting terrorist threats. Methodological aspects), Warszawa 2022.

Aleksandrowicz T.R., *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego* (Eng. The world in the network: states – societies – people. In search of a new paradigm of national security), Warszawa 2018.

Aleksandrowicz T.R., *Terroryzm międzynarodowy* (Eng. International terrorism), Warszawa 2015.

Ayres R.U., *Prognozowanie rozwoju techniki i planowanie długookresowe* (Eng. Technological forecasting and long-range planning), Warszawa 1973.

Bajerowski T., Kowalczyk A., *Feasibility (Possibility) And Probability In Risk And Crisis Management* (reproduced typescript in the author's possession).

Bajerowski T., Kowalczyk A., *Metody geoinformacyjnych analiz jawnoźródłowych w zwalczaniu terroryzmu* (Eng. Geoinformation methods for open-source analysis in combating terrorism), 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* (Eng. General systems theory), Warszawa 1984.

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

Bobby W., *The Limits of Prediction – or How I Learned to Stop Worrying About Black Swans and Love Angels*, "Studies in Intelligence" 2019, vol. 63, no. 4, pp. 7–16.

Bruce J.B., *The Rise and Fall of an Intelligence Discipline and its Uncertain Future*, "Studies in Intelligence" 2020, vol. 64, no. 1, pp. 13–30.

Dawidczyk A., *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody* (Eng. Strategic analysis in state security. Selected methods), Warszawa 2020.

Dawidczyk A., Jurczak J., Łuka P., *Metody, techniki, narzędzia nauk o bezpieczeństwie* (Eng. Methods, techniques, tools of security sciences), 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* (Eng. Strategic analysis of the company), 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 Finansing*, in: *The Palgrave Handbook of Criminal and Terrorism Financing Law*, C. King, C. Walker, J. Gurulé (eds.), Cham 2018, pp. 945–966.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka* (Eng. Information analysis. Theory and practice), Warszawa 2012.

Metody badań nad bezpieczeństwem i obronnością (Eng. Security and defence research methods), P. Sienkiewicz (ed.), Warszawa 2010.

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

Pherson R.H., Heuer Jr. R.J., *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, vol. 6, no. 3, pp. 83–99.

Sułek M., *Prognozowanie i symulacje międzynarodowe* (Eng. Forecasting and international simulations), Warszawa 2010.

Świeboda H., *Prognozowanie scenariuszowe w stosunkach międzynarodowych* (Eng. Scenario forecasting in international relations), in: *Prognozowanie w naukach społecznych. Wymiar narodowy i międzynarodowy* (Eng. Forecasting in the social sciences. National and international dimensions), H. Świeboda (sci. ed.), Warszawa 2018.

Świeboda H., *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej* (Eng. Forecasting threats to the national security of the Republic of Poland), Warszawa 2017.

Trocki M., Wyrozębski M., *Zastosowanie analizy morfologicznej w naukach o zarządzaniu* (Eng. The use of morphological analysis in management sciences), "Organizacja i Kierowanie" 2014, no. 2 (162), pp. 27–44.

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

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

Wiśniewski B., *Praktyczne aspekty badań bezpieczeństwa* (Eng. Practical aspects of security research), Warszawa 2020.

Wojciechowski J., Pieńkosz K., *Grafy i sieci* (Eng. Graphs and networks), Warszawa 2013.

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

Zubrzycki W., Aleksandrowicz T., Cymerski J., *Terroryzm 2019. Działania antyterrorystyczne* (Eng. Terrorism 2019. Anti-terrorist activities), Warszawa 2019.

Internet sources

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

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

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* (Eng. Introduction to social network analysis), https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf [accessed: 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 urządzeń podlegających obowiązkowej ochronie w zakresie zagrożeń o charakterze terrorystycznym (Eng. Procedure for agreeing a security plan for areas, facilities and equipment subject to mandatory protection with regard to terrorist threats), https://bip.abw.gov.pl/bip/procedury/495,Procedura-uzgadniania-planu-ochrony-obszarow-obiektow-i-urzadzen-podlegajacych-o.html?sid=47275ed2396b07ffaf12903f115c296b [accessed: 29 III 2022].

Legal acts

Ordinance of the Minister of the Interior and Administration of 24 February 2017 amending ordinance on the catalogue of terrorist incidents (Journal of Laws of 2017, item 395).

Ordinance of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist incidents (Journal of Laws of 2016, item 1092).

Other documents

Narodowy Programu Antyterrorystyczny na lata 2015–2019 (Eng. National Anti-Terrorist Programme for 2015-2019), (M.P. of 2014, item 1218, app.), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20140001218/O/M20141218.pdf [accessed: 7 VI 2024].

Assoc. Prof. Tomasz Aleksandrowicz,
Professor at the Police Academy in Szczytno

Lawyer, security specialist. Head of the Information Warfare Research Laboratory of the Research Centre on Social and Economic Risk at Collegium Civitas. He works on issues related to terrorism, organised crime, oversight of service activities, security legislation, application of restrictive measures. He is the author of more than one hundred books and scientific articles on various aspects of security.

Contact: tomek.aleksandrowicz@me.com