SECURITY DIMENSIONS
NO. 33; 2020 (217–240)
DOI 10.5604/01.3001.0014.2678

How to Estimate Security – Problem Analysis

Grzegorz Pilarski[1]

ABSTRACT

Background: The article presents a method of estimating the security level which indicates how probable it is for a phenomenon to occur. **Objectives:** The author attempts to answer the question: How do we estimate security? Decision makers usually need percentage showing the probability of an incident taking place in the future. This information is needed in the first place, later decision makers can use more descriptive information. **Methods:** The research problem concerns the assessment of security using the estimation method. Depicting security in numbers is difficult, thus the descriptive method is also usually applied. The estimation method facilitates the assessment. It is helpful since it is partly done by calculation and partly by guessing or approximation. Based on a case study analysing whether a terrorist attack may occur, the author also used tools such as averaging expert predictions, scenario analysis and risk analysis. **Results:** This article provides

[1] Lt. Col. Assoc. Prof. Grzegorz Pilarski, Ph.D., ORCID 0000-0001-9728-2611, War Studies University, Warszawa, Poland; correspondence address: Cybersecurity Branch, Faculty of Military Studies, War Studies University, al. gen. A. Chruściela „Montera" 103, 00-910 Warszawa-Rembertów, Warszawa, Poland; e-mail: g.pilarski@akademia.mil.pl

a view on forecasting security, which results in a method of estimating the level of security. **Conclusions:** The author presents an approach which allows to initially estimate the security level of the analyzed phenomenon in a relatively short period of time.

ARTICLE INFO

Article history
Received: 31.03.2020 Accepted: 30.05.2020

Keywords
security, estimation, risk analysis, political risk, forecasting

Introduction

Ascher and Overholt claim that forecasting is a "complex process which cannot be studied in isolation, but in the context of a policy-making process".[2] In order to enhance security, it is required to initially determine or estimate the security level in the scope of a given phenomenon or an event that might occur in a given place in the world. According to Ascher and Overholt, the demand that "decision makers make upon their analysts can be divided into two categories: a need for making decisions through reasoned judgment and an additional need that reflects the policy makers' politics, insecurities, habits, biases, and other motivations extraneous to the specific task of making a rational decision".[3] According to Świeboda[4], it is common that complex mathematic analyses, applied in different methods of forecasting, do not bring sufficient answers in terms of the level of security or risk. Decision makers frequently need a relatively fast and precise estimation of the level of security in order to make decisions or to get involved themselves or engage their resources into a given undertaking or to perform operations in a specific region in the world.

[2] W. Ascher, W.H. Overholt, *Strategic planning forecasting. Political risk and economic opportunity*, New York 1983, p. xi.

[3] *Ibidem*, p. 43.

[4] *Prognozowanie w naukach społecznych: wymiar narodowy i międzynarodowy*, H. Świeboda (ed.), Warszawa 2018.

Decision makers often need concise information, expressed in numbers or in percent at rough estimate, which indicates how probable it is for an event to take place in the future, i.e. if it is likely to happen or not. This kind of information is needed in the first place. Later, decision makers apply a descriptive method if time allows to do it, or if a need for an in-depth analysis arises.

Security, as an abstract concept, cannot be easily described in numbers. It is usually expressed descriptively, e.g. by a statement: "the visit of President Trump in Poland is burdened with an increased risk of a terrorist attack".

Thus, in order to assess security and try to express it in numbers it is useful to apply an *estimation method*. According to Longman Dictionary of Contemporary English[5] and Cambridge Dictionary[6], the verb 'to estimate' means "to try to judge the value, size, speed, cost etc. of something, partly by calculating and partly by guessing or approximating". In consequence, it is well grounded to apply estimation in order to express the analyzed security-related situation in approximate numbers. Numbers are basically more meaningful for decision makers than a text analysis.

The research problem presented in the article is to assess security with the use of estimation method. However, this procedure is more complicated than it appears. This is the underlying reason for the author to present the problem analysis and show the procedure step-by-step. Based on a probability percentage, it is possible to estimate the level of confidence in a forecast.

Having in mind the complex character of forecasting as an auxiliary tool supporting a decision making process, the author of this article tries to answer the following question: How do we estimate security? The author adopts a hypothesis that estimation is a good method to describe security by providing decision makers with concise information on the probability of the occurrence of a given phenomenon.

The aim of the article is to present a method enabling the estimation of a security level which indicates how probable it is for the analyzed phenomenon to occur. This information constitutes one of the factors taken into consideration by the decision makers in the decision making process. The more precise the gathered data are (taking into consideration the reliability

[5] *Longman dictionary of contemporary English*, Barcelona 2001, p. 465.

[6] *Cambridge international dictionary of English*, New York 1995, p. 46.

of the source of information, expert analysis, etc.), the more reliable factor they become for decision makers.

Based on a case study on whether a terrorist attack may occur, the author used some of the available tools such as averaging expert predictions, scenario analysis, and risk analysis to estimate the security level by specifying the probability of the occurrence of an event.

The article is an attempt to propagate forecasting in the field of security and to evoke further discussion in this field.

Conceptual basis for forecasting

Russo and Schoemaker[7] enumerate four basic stages to go through in order to carry out an analysis prior to making a decision:

1. Framing: simplifying and directing a complex reality to look at a given problem from certain perspective, setting at the same time vital parameters which should be taken into consideration during the analysis (time intended: 22%);
2. Gathering Intelligence: gathering reliable facts and their assessment in the face of uncertainty; it is advised to avoid exaggerated trust in one's own judgments and to seek for facts to prove the subjective assessment (time intended: 33%);
3. Coming to Conclusions: the analysis of facts and the value of the gathered materials in order to choose the crucial ones and to elaborate a decision; one can apply the "pyramid of choice" approach: value analysis, importance weighting – bootstrapping, heuristic procedures – tailored and generic shortcuts, intuitive choice – judgments based on one's own experience[8] (time intended: 22%);
4. Learning from Experience: it is vital to sum up the process of analysis for the sake of continual learning, which might exert influence on the strengthening of abilities and making decisions in the future (time intended: 23%).

Decision-making is a complex process involving cognitive thinking as well as social and emotional components. In this process it is necessary to

[7] J.E. Russo, P.J.H. Schoemaker, *Winning decisions: Getting it right the first time*, New York 2002, pp. 1–17.

[8] *Ibidem*, pp. 133–159.

reject the obvious answers and recognize uncertainty. Thus, how is the term *uncertainty* understood?

According to Courtney, Kirkland and Viguerie[9], this is a situation where the current state of knowledge and the order or nature of things are unknown. One is not able to determine the probability of possible outcomes, everything can happen.[10] The subject literature provides information concerning four levels of uncertainty.[11]

- Level one: a clear enough future – single forecast; the residual uncertainty is irrelevant to making strategic decision;
- Level two: alternative futures – the future can be described as one of a few discrete scenarios and one can establish the probability of each scenario's occurrence;
- Level three: a range of futures – a range of possible future outcomes;
- Level four: true ambiguity – not even a range of possible future outcomes.

It is important to decrease uncertainty as much as possible, and then manage it. In level one uncertainty, it is irrelevant to making strategic decisions; a single forecast constitutes a sufficiently precise basis for decision makers. In levels two and three, one must describe scenarios and assign the probability of occurrence for all scenarios. In level four, it is impossible to identify a range of potential outcomes or a range of scenarios since the level of uncertainty is high. Thus, according to Tetlock and Gardner[12], it is advisable to use the following range of probability:

- <99%–100% – certain;
- <85%–99% – almost certain;
- <60%–85% – probable;
- <40%–60% – chances about even;
- <20%–40% – probably not;
- <1%–20% – certainly not;
- <1–0% – impossible.

[9] H.G. Courtney, J. Kirkland, S.P. Viguerie, *Strategy under uncertainty*, "McKinsey Quarterly", 1 June 2000, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/strategy-under-uncertainty (accessed: 15.12.2019).

[10] I. Bremmer, P. Keat, *Fat tail. The power of political knowledge in an uncertain world*, New York 2009, pp. 15–37.

[11] H.G. Courtney et al., *Strategy under uncertainty*, *op. cit.*

[12] P.E. Tetlock, D. Gardner, *Superforecasting: the art and science of prediction*, Crown Publisher, New York 2015, pp. 47–81.

In the process of forecasting, at the stage of framing, only the key factors describing reality are chosen out of a whole set of factors, depending on the analyst's decision and the specificity of the analysis.[13] These are the factors that must be taken into consideration and analyzed to estimate security. Political risk is one of these elements which must be kept in mind.

In analyzing political risk, it is required to take into consideration numerous factors which can exert influence on the risk, e.g. electoral uncertainties, collapse of goverments, labor unrest, civil protests, terrorist attacks, and religious and ethnic disputes.[14] This leads to a conclusion that an indepth analysis is necessary to properly assess the level of security. This in turn exerts influence on the methods used to manage and mitigate the risk. Moving on to the case study presented in the article, the author sugests that the analysis should be conducted in steps proposed by Glancy[15]:

1. Identification of the analyzed case – clear definition of the goal of the forecast and determination of basic assessment indicators;
2. Background information on the case – gathering information on the analyzed problem and a short description of the issue or country being assessed;
3. An initial indication of uncertainty level for the examined case – preliminary assessment of the level of uncertainty of the issue made on the basis of the gathered information;
4. Rough economic analysis of the examined case – gathering information on the economic aspects of the area affected by the analyzed problem. The following questions might be included: what is the country's economic position? Is it going in the right or in the wrong direction? Would a change in the economic situation affect the analyzed issues? The analysis can be extended with political and social issues. These are only examples; the analyst determines what aspects will be taken into consideration in a given analysis, depending on the problem.

[13] J.E. Russo, P.J.H. Schoemaker, *Winning decisions…*, *op. cit.*, pp. 1–17.

[14] M. Toksöz, *Guide to country risk. How to identify, manage and mitigate the risks of doing business across borders*, London 2014, pp. 138–143.

[15] D. Glancy, materials from Professor David Glancy presented during course IWP 667 *Forecasting and Political Risk Analysis*, The Institute of World Politics, Washington 2017.

5. Chosen analytical techniques – the analysis of the gathered information with the use of tools such as foreign policy analysis[16], averaging expert predictions[17], game theory[18], scenario analysis[19];
6. Assessment of security level for the analyzed case – assessment of the likelihood of a given event, based on a synthesis of the base rate and inside information (which should include the outcomes of analysis noted above plus any information that may be appropriate);
7. Level of confidence of forecast – determining the level at which the analyzed outcome might be, based on the range of probability, indicating at the same time the level of confidence in the forecast;
8. Possible alternative outcomes – search for possible alternative future outcomes, even those most unlikely.

In terms of analysis, visualization based on casual loop diagrams is a solution which "allows to reveal connections or relationships between parts of an organization or a system".[20] The diagrams help illustrating the dynamic and interconnected nature of the world.[21] The already described security estimation analysis is another tool useful in forecasting; it can also be helpful in the process of scenario planning in action, so as to envision multiple futures.[22]

[16] J.S. Lantis, R. Beasley, *Comparative Foreign Policy Analysis*, "Oxford Research Encyclopedia – Politics", May 2017, DOI 10.1093/acrefore/9780190228637.013.398 (accessed: 15.1.2020).

[17] P.L. Bernstein, *Against the Gods: the remarkable story of risk*, New York 1998, pp. 50–53.

[18] G. Bonanno, *Game theory*, second edition, "Department of Economics – University of California", 2018, http://faculty.econ.ucdavis.edu/faculty/bonanno/PDF/GT_book.pdf (accessed: 17.1.2020).

[19] R. MacKay, P. McKiernan, *Scenario Thinking: A Historical Evolution of Strategic Foresight (Elements in Business Strategy)*, Cambridge 2018, DOI 10.1017/9781108571494 (accessed: 20.1.2020).

[20] M. Goodman, *Systems thinking: what, why, when, where, and how?*, "Systems Thinker", n.d., https://thesystemsthinker.com/systems-thinking-what-why-when-where-and-how (accessed: 20.11.2019).

[21] D.H. Kim, *Systems thinking tools. A user's reference guide*, Waltham 1994, pp. 18–21.

[22] P.J.H. Schoemaker, *Scenario planning: a tool for strategic thinking*, " MIT Sloan Management Review", Winter 1995, vol. 36, no. 2, pp. 24–40.

Sample security estimation – case study

Taking into consideration the theoretical background shown above, the author presents an example of security estimation process. It is based on a past event to prove the correctness of the forecasting method. What is more, the presentation of a case study shows how the issue can be addressed in a practical way.

1. Identification of the analyzed case

The author focuses on the situation which was observed during a sport event: Mundial[23] in Russia in 2018. In reality the process is performed prior to any key event. Here, a past event was used to present the process of security assessment and, more importantly, prove its correctness. The following question was posed: "Will there be a terrorist attack on sport facilities where matches will be played during World Cup in Russia in 2018?". It was presumed that an attack would be considered a terrorist one and successful if there was a bomb explosion or a shooting incident in which at least ten people would die.

2. Background information on the case

a) Mundial, or World Cup, is an international football tournament in which male national representations of FIFA federation take part.
b) On 29 September 2012, FIFA made the final decision in Zurich concerning the location of arenas at the 2018 World Cup (Fig. 1). Representations of 32 countries qualified to take part in the tournament (Fig. 2). In total, 64 matches were to be played during the championship at 12 stadiums (in 11 cities) (Fig. 3). The teams of Iceland and Panama were to debut at the tournament.[24]
c) The winner of the championship qualifies for the FIFA Club World Cup 2021, which will take place before the tournament in Qatar in 2022.
d) World Cup 2018 was planned to start in Sochi and Kazan on 14 June, and the final match was to be played in Moscow at the Luzhniki Stadium on 15 July 2018.

[23] "FIFA World Cup 2018", http://www.fifa.com/worldcup/archive/russia2018/index.html (accessed: 25.11.2019).
[24] *Ibidem*.

Fig. 1. Cities selected as hosts of World Cup in Russia in 2018

Source: "FIFA World Cup 2018", http://www.fifa.com/worldcup/archive/russia2018/index.html (accessed: 25.11.2019).

Fig. 2. Countries which qualified to participate in World Cup 2018

AFC (5)
- Australia
- Iran
- Japan
- Saudi Arabia
- South Korea

CAF (5)
- Egypt
- Morocco
- Nigeria
- Senegal
- Tunisia

CONCACAF (3)
- Costa Rica
- Mexico
- Panama

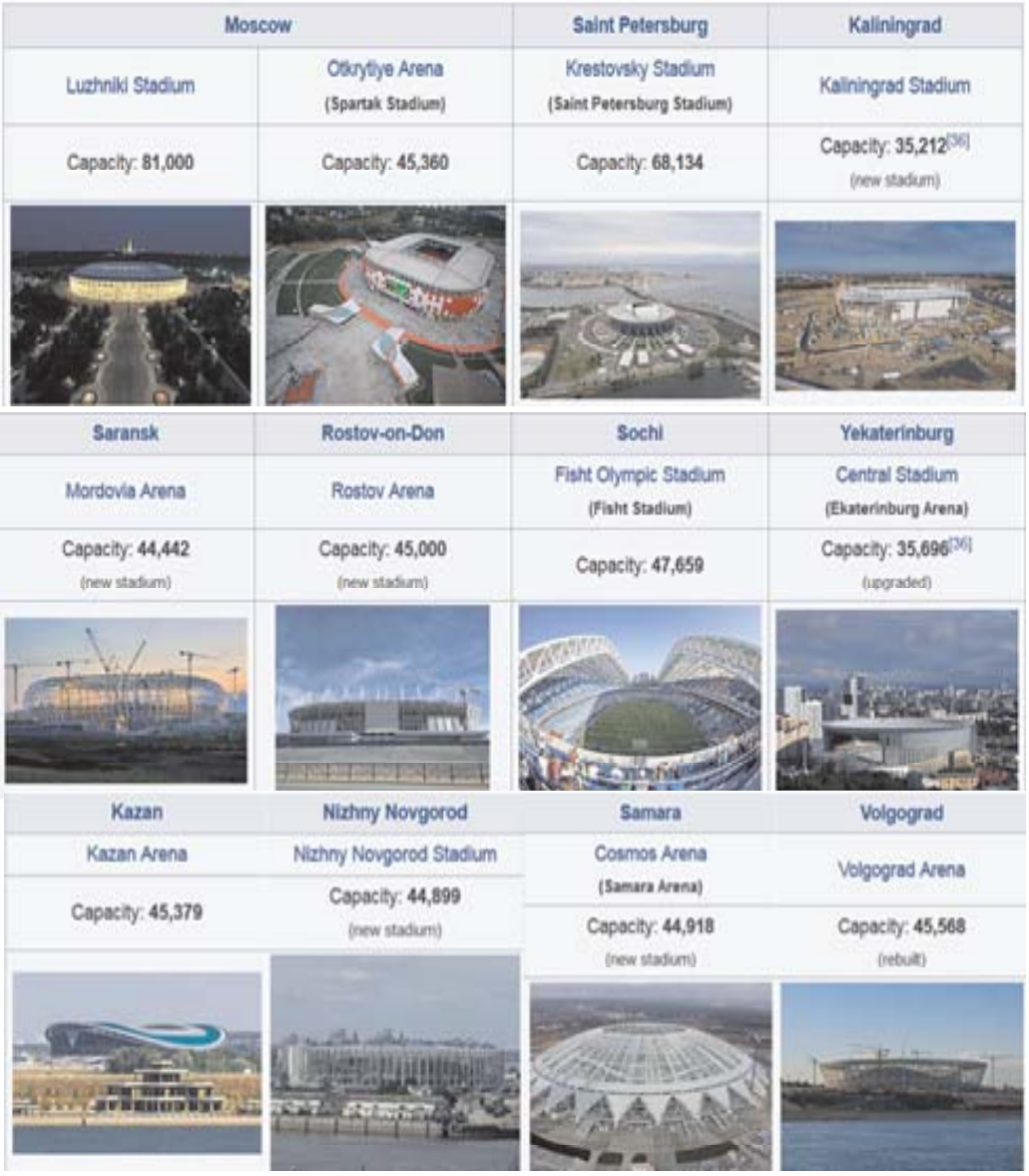
CONMEBOL (5)
- Argentina
- Brazil
- Colombia
- Peru
- Uruguay

OFC (0)
- *None qualified*

UEFA (14)
- Belgium
- Croatia
- Denmark
- England
- France
- Germany
- Iceland
- Poland
- Portugal
- Russia (hosts)
- Serbia
- Spain
- Sweden
- Switzerland

Source: "FIFA World Cup 2018", http://www.fifa.com/worldcup/archive/russia2018/index.html (accessed: 25.11.2019).

Fig. 3. Twelve stadiums where matches were to be played during the World Cup in Russia in 2018



Source: "FIFA World Cup 2018", http://www.fifa.com/worldcup/archive/russia2018/index.html (accessed: 25.11.2019).

3. An initial indication of uncertainty level for the examined case
The question was: "How big is the probability of a terrorist attack **at sport facilities**?".

Table 1. Statistical data

Source	**Rate I**	**Rate II**
Base rate	50%	50% × 1
Level of military security	10%	10% × 1
Russian government	10%	10% × 1
Experts	20%	20% × 3
Total / number of indicators	90% / 4	130% / 6
Probability	**23%**	**22%**

Source: own elaboration.

The authorities and services ensured that safety at the stadiums would be at the highest level (based on the assurance of the authorities about high level of security, it was assumed, regardless of the implemented preventive measures, that the probability that such an incident might occur would amount to 10% for the "level of military security" and for the "Russian government" respectively). Basically, they did not allow the possibility of a terrorist attack.

Experts claimed that safety procedures at sports facilities were at a high level and a terrorist attack was possible, but its probability was fairly low.[25] In this case, the analysis provided by experts on terrorism was used and it was assumed that the level of probability amounted to 20%. If there is enough time to prepare forecasting, such analysis can be commissioned, but one who does so must take into consideration the extension of time and the increase of costs. Table 1 provides four indicators of probability: base rate (50%) that a terrorist attack would happen on sport facilities; level of military security – 10%; Russian government – 10%, and, last but not least, experts' opinions – 20%. All indicators of probability after being added equal 90%, and the result is then divided by 4 (the number of indicators),

[25] G. Levy, *Top 10 Worst Sport Terrorism Attacks*, "Time", n.d., http://content.time.com/time/specials/packages/article/0,28804,1882967_1882966_1882958,00.html (accessed: 30.11.2019).

which gives a final result of 23% (Table 1). Additionally, one can determine the importance of the gathered statistical data by assigning proper weight function.[26] In the current case study, the data obtained from the experts are highly reliable, thus it is given weight function three. As a result, six indicators of probability are taken into consideration in the calculation: 1 × base rate (50%); 1 × level of military security (10%); 1 × Russian government (10%); and 3 × experts' opinion (20%); which is 130% in total. It is divided by six (the number of indicators), which gives a final result of 22%.

In this method, the adopted sources of information can be considered more or less valuable. The more reliable sources are taken, the more precise results are obtained. What is more, the base rate itself is of great importance: in this case, the level of probability was assumed as 50% of a chance that such phenomenon would occur, but this indicator may be of different value depending on the decision of the analyst preparing the estimation.

In the further part of the case study, the same manner of calculation was adopted; thus, a detailed description was scrapped.

The next question was: "How big is the probability of a terrorist attack **away from sport facilities**?".

Table 2. Statistical data

Source	**Rate I**	**Rate II**
Base rate	50%	50% × 1
Level of military security	40%	40% × 1
Russian government	20%	20% × 1
Experts	70%	70% × 3
Total / number of indicators	180% / 4	320% / 6
Probability	**45%**	**54%**

Source: own elaboration.

Authorities and services assured that safety during World Cup 2018 would be ensured at the highest level; however, the vastness of the area made it

[26] K. Rykaczewski, *Systemy rozmyte i ich zastosowania*, Toruń 2006, https://fulmanski.pl/zajecia/ssn/materialy/duszek.pdf (accessed: 30.11.2019).

difficult to control.[27] Past events proved that in case of mass events, the greatest emphasis should be put on the protection of transport infrastructure such as metro, railway and bus stations. According to experts, ISIS attacks were very likely due to the risk of retaliation for military operations in Syria. Experts assessed the probability of a terrorist attack on transport infrastructure at the level of 70% (Table 2). In this case, a terrorist attack launched away from sport facilities was analyzed and it was estimated on the basis of the adopted indicators that the probability of the occurrence of such an incident could amount to 45% without any weight function, and if the importance and reliability of data obtained from experts were taken into consideration, the probability would be 54%.

4. Rough economic analysis of the examined case

If a terrorist attack happened, the economic position of Russia would become unstable and it could exert influence on the prices of natural resources, especially gas and oil. This would consequently have impact on the prices of those resources on the world market.

5. Chosen analytical techniques

The analysis pursued to find the answer to the posed question (in this case: "How big is the probability of a terrorist attack at sport facilities?"). In general, an analysis can be carried out with the use of available tools, for example: foreign policy analysis, averaging expert predictions, a game theory, a scenario analysis, etc.

In the described case, the following types of analysis were used: (1) averaging expert predictions; (2) scenarios analysis; (3) risk analysis.

Averaging expert predictions was based on the assessment of an initial level of uncertainty for the issue under examination (Table 1), where 23% of probability that a terrorist attack would happen was obtained.

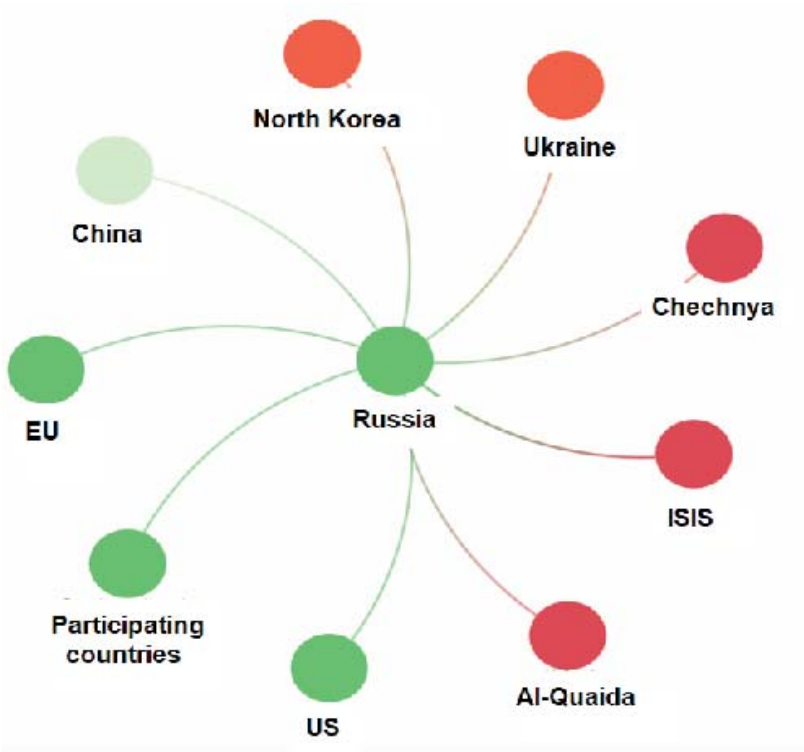
Scenarios analysis was based on indicating the probable actors participating in a scenario, determining the indicators of a terrorist attack, and creating a matrix of dependencies and influence of actors/players, which

[27] Staff Reporter, *80% chance of World Cup terrorist attack*, "Mail & Guardian", 30 May 2010, https://mg.co.za/article/2010-05-30-80-chance-of-world-cup-terrorist-attack (accessed: 30.11.2019).

consequently could lead to the determination of the level of probability that the incident could take place.

There were three steps to follow. Firstly, probable actors involved in the FIFA World Cup in Russia in 2018 were chosen (Fig. 4).

Fig. 4. Probable actors during the FIFA World Cup in Russia in 2018
(green – supporters; red – potential aggressors/actors who may increase/decrease the level of security[28])



Source: own elaboration based on the Kumo.io software.

[28] *Probable actors during the FIFA World Cup in Russia in 2018*, "Kumu", n.d., https://kumu.io/mgpilar/fifa-world-cup-2018-6510#fifa-world-cup-2018?selection=ZWRnZS1rMTNrWlM0Uw%3D%3D&focus%20=%23conn-bmjOM7Gx%20out%203 (accessed: 20.1.2020).

Next, specific indicators were adopted and specific positions were assigned to them (Table 3). Finally, a matrix was created with dependencies and impacts of individual actors/players (Table 4).

Table 3. Indicators of a terrorist attack

Position	Possible states
100	No attack
70	Low emergency state
50	Medium emergency state
30	High emergency state
0	Terrorist attack

Source: own elaboration.

Table 4. Matrix of dependencies and influence of actors/players

Actor/player	Position (P)	Salience (S)	Influence (I)	I*S	I*P	I*S*P
EU/Participating countries/China	100	30	20	600	2,000	60,000
Russia	100	100	90	9,000	9,000	900,000
USA	100	30	20	600	2,000	60,000
North Korea	50	20	10	200	500	10,000
Ukraine	70	40	30	1,200	2,100	84,000
ISIS	0	100	80	8,000	0	0
Al Qaida	30	60	50	3,000	1,500	90,000
Chechnya	30	40	50	2,000	1,500	60,000
Sum				**24,600**	**18,600**	**1,264,000**

Source: own elaboration.

In the matrix, the probable actors were given indicators in accordance with Table 3 (P – position), as well as values determining the salience (S) and the influence (I) of particular actors in the analyzed problem. The adjustment of particular values is generally a subjective assessment of the analyst, based on the available data. The next columns present the results of arithmetic functions (Table 4).

Through the analysis of the results obtained on the basis of percentage probability distribution, it was possible to calculate the probability of a given state occurrence.

In order to do so, it was required to sum the results of the formula I*S for particular positions and then divide it by the sum of all results of the formula. For position 100 (no terrorist attack), there were three actors for whom the following results of formula I*S were obtained: EU/Participating countries/China – 600; Russia – 9,000; USA – 600; the total for all three was 10,200. Next, the obtained result had to be divided by the sum of all results of formula I*S, i.e. 24,600, and it gave 41%, which meant that the probability of a terrorist attack not taking place was 41%. Such calculation was performed for all possible states (positions). The results are provided in Table 5.

Table 5. Position vs. the probability of the occurrence of a terrorist attack

Possible states	Position	Impact	Probability
No attack	100	10,200/24,600	41%
Low emergency state	70	1,200/24,600	5%
Medium emergency state	50	200/24,600	1%
High emergency state	30	500/24,600	20%
Terrorist attack	0	800/24,600	33%

Source: own elaboration.

The most important findings can be concluded as following: possible state of high readiness (high emergency state) – 20%; possible terrorist attack – 33%; a terrorist attack will not occur - 41% (Table 5).

Next, on the basis of the calculations presented in Table 4, it was possible to determine the zone of possible outcomes, namely the states that might occur. In the above presented calculation, the highest percentage value was for position 100 i.e. "no attack", and it was one of the possible states. The second state should be calculated with the use of a weighted mean: Sum(I*S*P) / Sum(I*P), i.e. 1,264,000 / 18,600 = 68. This resulted in the second position determining the scope of possible states placed between positions 100 and 68 (Table 6).

Table 6. The zone of possible outcomes

Probability	41%	5%	1%	20%	33%
Position	100 No attack	70 Low emergency state	50 Medium emergency state	30 High emergency state	0 Terrorist attack
Zone of possible outcomes	100	68			

Source: own elaboration.

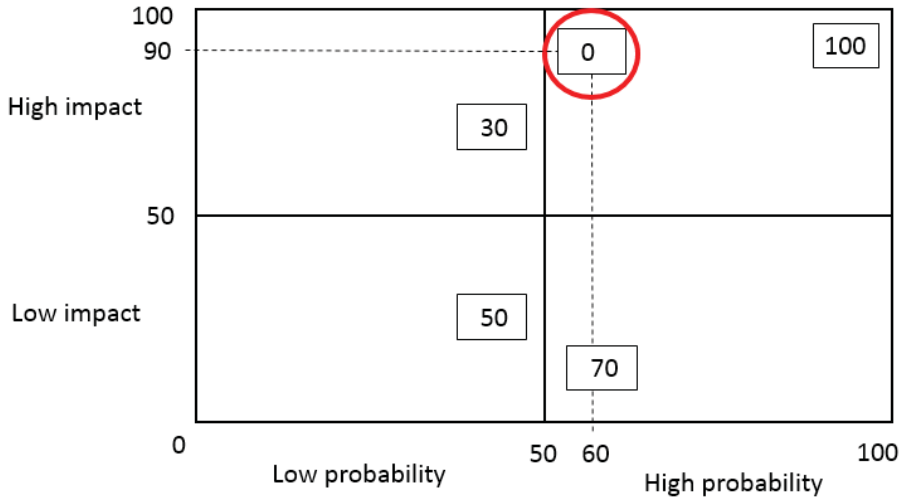
The result of the estimation indicated that the possible states included the following: "no attack" there would mean no terrorist attack with a low emergency state (position 70).

The third technique for analysis, namely risk analysis, was based on the assessment of risk using the matrix of dependencies between the probability of the occurrence of a given state and the possible influence inherent in it.[29] In this technique, the analyst takes the gathered data and assesses the probability level of the occurrence of a given state, as well as the potential damage (impact) which might take place if a given state occurs.

[29] B. Lent, *Leader, Manager, Expert, The project management system*, Warszawa 2012, pp. 254–255.

In the examined case, there was an attempt to find the value of probability for the state of a terrorist attack taking place, and it was 60%, while the impact was 90%. The results are presented on the matrix below (Fig. 5).

Fig. 5. Matrix of events in the scope of the probability of occurrence, and its impact



Source: own elaboration.

$$\text{Risk} = \text{probability} * \text{impact}$$
$$60*90 = 5{,}400 / 10{,}000 = 54\%$$

Risk or probability that a terrorist attack will happen (state 0) amounts to 54%.

6. Assessment of security level for the analyzed case

Taking into consideration the results of the three types of analysis presented above, estimation was performed in order to determine the probability of a terrorist attack taking place. In the case study examined here, the base rate equaled 50% (a terrorist attack can either take place or not), and the results were: analysis 1 (averaging expert predictions) – 23%; analysis 2 (scenarios analysis) – 33%; analysis 3 (risk analysis) – 54%. Two estimations were performed, the first one without a weight function, and the second one

indicating that analysis 1 was a reliable source; thus, the second estimation adopted weight function 3.

Table 7. Statistical data

Source	Rate I	Rate II
Base rate	50%	50% × 1
Analysis 1	23%	23% × 3
Analysis 2	33%	33% × 1
Analysis 3	54%	54% × 1
Total / number of indicators	160% / 4	206% / 6
Probability	**40%**	**34%**

Source: own elaboration.

All in all, it was estimated that the probability of a terrorist attack on sports facilities was 34% (Table 7).

7. Level of confidence in the forecast

On the basis of the above analysis, it was determined that the probability for the state of a terrorist attack occurrence was 34%.

In the case under examination, the level of confidence in the forecast lay in the probability range 20%–40%, namely "probably not", which is based on the range of probability elaborated by Tetlock and Gardner.[30]

In this case study, the level of uncertainty is Level two.[31] On this level, one can observe alternative futures which can be described as discrete scenarios (scenario one: a terrorist attack would not happen; scenario two: a terrorist attack would happen), and one can assign probability of each scenario's occurrence.

8. Possible alternative outcomes

This point presents possible alternative outcomes which stem from the analysis of the studied situation. In the examined case, it could be assumed that there might be other terrorist attacks, not at sport facilities, but in

[30] P.E. Tetlock, D. Gardner, *Superforecasting…*, *op. cit.*

[31] Vide H.G. Courtney *et al.*, *Strategy under uncertainty*, *op. cit.*, p. 4.

the cities where matches were to be held, so as to intimidate tourists and athletes who came to the World Cup.[32] According to security experts, the probability of such a threat increases with the increasing distance from well-guarded sports facilities. Thus, in this alternative outcome, "attacks away from sport facilities", there was an increased probability about 50% and it lay in a range between 40% and 60%, i.e. "chance about even" on the scale of probability.[33]

Another controversial outcome

Russia could participate in a terrorist attack not directly, but only in a way intended to change its political position in the world. While maintaining the attitude of the attack's victim, Putin could win over friends in the world, e.g. in the USA, in a fight against terrorism. In this case Russia, as the host of an international sports event, would be in the position of a victim, thus it could be forgiven some of its "sins", for example the annexation of Crimea. An analyst can decide that the probability of such a scenario is "certainly not" or "impossible" on the scale of probability[34]).

Comments on the case study

This case study is a simple example, but at the same time a good sample to perform an analysis. In the process of averaging expert predictions[35], it should be noted that the first indicator as a base rate is simple to accept, because an incident can either happen or not; there is always 50% of chance. Of course, the indicator might be of different value depending on the possessed preliminary knowledge on the analyzed problem; this, in turn, contributes to a more precise initial estimation. If a given analysis is very reliable for an analyst, they can give it weight function, as in the case of Analysis 1 in Table 8.

The next analysis where the subjective indicator is taken into consideration is Analysis 3. Risk is the result of the probability components for a given occurrence as well as the outcomes of the events. In this analysis, the events (incidents) placed in the right top box in Figure 5 are the most

[32] *80% chance of World Cup terrorist attack*, *op. cit.*

[33] P.E. Tetlock, D. Gardner, *Superforecasting…*, *op. cit.*

[34] *Ibidem*.

[35] P.L. Bernstein, *Against the Gods…*, *op. cit.*, pp. 50–53.

important ones for the management of risk (Fig. 5) since the level of risk is relatively high and it brings a lot of negative effects.

Table 8. Statistical data

Source	**Rate I**	**Rate II**
Base rate	50 %	50% × 1
Analysis 1	23 %	23% × 3
Analysis 2	33 %	33% × 1
~~Analysis 3~~	~~54 %~~	~~54% × 1~~
Total / number of indicators	~~160 / 4~~ 106% / 3	~~206 / 6~~ 152% / 5
Probability	**~~40%~~ 35%**	**~~34%~~ 30%**

Source: own elaboration.

An analyst, on the basis of the gathered data, assesses the level of probability whether a given state will occur, as well as the potential damage (impact) which might take place in the event of the occurrence of a given state. In the analyzed case, the estimation of the occurrence of a terrorist attack was 54% and it was accepted as a result of Analysis 3. Of course, if one omits the indicator from Analysis 3, one will receive another score which is presented in Table 8. As it is visible, the estimation in rate I and II decreases by a few percent.

Conclusion

The topic of the estimation of security is really vital in the opinion of the author, since it provides decision makers with concise information on the probability of a occurrence of a given event, expressed in numbers or in percent at rough estimate.

The presented case study confirms the adopted hypothesis that the applied method, which enables the estimation of security level, helps to indicate the probability of the occurrence of the analyzed phenomenon in a fairly short time.

It should be emphasized that in this type of analysis, over half of the needed time is devoted to the realization of two stages, namely: framing

and gathering intelligence.[36] The stages are mainly based on gathering reliable facts, historical data, etc., thus it is extremely important to choose trustworthy data in order to obtain a reliable estimation of security.

The author had a chance and pleasure to attend a course titled "Forecasting and Political Risk Analysis" in the Institute of World Politics in Washington, and it aroused his true interest in the problem matter, encouraging him to do further research in this subject.

One of the prerequisites for the author to carry out research in this field was to elaborate an estimation method which could be applied at the operational or at the tactical level for a swift presentation of situation in military decision making[37] as well as for the analysis of threats to cybersecurity.

References

1. Ascher W., Overholt W.H., *Strategic planning forecasting. Political risk and economic opportunity*, New York 1983.
2. Bernstein P.L., *Against the Gods: the remarkable story of risk*, New York 1998.
3. Bonanno G., *Game theory*, second edition, "Department of Economics – University of California", 2018, http://faculty.econ.ucdavis.edu/faculty/bonanno/PDF/GT_book.pdf (accessed: 17.1.2020).
4. Bremmer I., Keat P., *Fat tail. The power of political knowledge in an uncertain world*, New York 2009.
5. *Cambridge international dictionary of English*, New York 1995.
6. Courtney H.G., Kirkland J., Viguerie S.P., *Strategy under uncertainty*, "McKinsey Quarterly", 1 June 2000, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/strategy-under-uncertainty (accessed: 15.12.2019).
7. "FIFA World Cup 2018", http://www.fifa.com/worldcup/archive/russia2018/index.html (accessed: 25.11.2019).
8. Glancy D., materials from Professor David Glancy presented during course IWP 667 *Forecasting and Political Risk Analysis*, The Institute of World Politics, Washington 2017.

[36] J.E. Russo, P.J.H. Schoemaker, *Winning decisions…*, *op. cit.*

[37] G. Pilarski, *The concept of recommender system supporting command and control system in hierarchical organization*, [in:] *1st European network intelligence conference ENIC. IEEE Computer Society*, Wroclaw 2014, pp. 138–141, DOI 10.1109/ENIC.2014.9.

9. Goodman M., *Systems thinking: what, why, when, where, and how?*, "Systems Thinker", n.d., https://thesystemsthinker.com/systems-thinking-what-why-when-where-and-how (accessed: 20.11.2019).
10. Kim D.H., *Systems thinking tools. A user's reference guide*, Waltham 1994.
11. Lantis J.S., Beasley R., *Comparative Foreign Policy Analysis*, "Oxford Research Encyclopedia – Politics", May 2017, DOI 10.1093/acrefore/9780190228637.013.398 (accessed: 15.1.2020).
12. Lent B., *Leader, Manager, Expert, The project management system*, Warszawa 2012.
13. Levy G., *Top 10 Worst Sport Terrorism Attacks*, "Time", n.d., http://content.time.com/time/specials/packages/article/0,28804,1882967_1882966_1882958,00.html (accessed: 30.11.2019).
14. *Longman dictionary of contemporary English*, Barcelona 2001.
15. MacKay R., McKiernan P., *Scenario Thinking: A Historical Evolution of Strategic Foresight (Elements in Business Strategy)*, Cambridge 2018, DOI 10.1017/9781108571494 (accessed: 20.1.2020).
16. Pilarski G., *The concept of recommender system supporting command and control system in hierarchical organization*, [in:] *1st European network intelligence conference ENIC. IEEE Computer Society*, Wroclaw 2014, pp. 138–141, DOI 10.1109/ENIC.2014.9.
17. *Probable actors during the FIFA World Cup in Russia in 2018*, "Kumu", n.d., https://kumu.io/mgpilar/fifa-world-cup-2018-6510#fifa-world-cup-2018?selection=ZWRnZS1rMTNrWlM0Uw%3D%3D&focus%20=%23conn-bmjOM7Gx%20out%203 (accessed: 20.1.2020).
18. *Prognozowanie w naukach społecznych: wymiar narodowy i międzynarodowy*, H. Świeboda (ed.), Warszawa 2018.
19. Russo J.E., Schoemaker P.J.H., *Winning decisions: Getting it right the first time*, New York 2002.
20. Rykaczewski K., *Systemy rozmyte i ich zastosowania*, Toruń 2006, https://fulmanski.pl/zajecia/ssn/materialy/duszek.pdf (accessed: 30.11.2019).
21. Schoemaker P.J.H., *Scenario planning: a tool for strategic thinking*, " MIT Sloan Management Review", Winter 1995, vol. 36, no. 2, pp. 24–40.
22. Staff Reporter, *80% chance of World Cup terrorist attack*, "Mail & Guardian", 30 May 2010, https://mg.co.za/article/2010-05-30-80-chance-of-world-cup-terrorist-attack (accessed: 30.11.2019).

23. Tetlock P.E., Gardner D., *Superforecasting: the art and science of prediction*, New York 2015.
24. Toksöz M., *Guide to country risk. How to identify, manage and mitigate the risks of doing business across borders*, London 2014.

Cite this article as:
G. Pilarski, *How to estimate security – problem analysis*, "Security Dimensions", 2020, no. 33, pp. 217–240, DOI 10.5604/01.3001.0014.2678.