



THE APPLICATION OF INTELLIGENCE ANALYSIS IN TOURISM SECURITY MANAGEMENT

Lazar Radenović*

¹Ph.D. Student,
Singidunum University,
Belgrade, Serbia

Abstract:

This paper examines the role of intelligence analysis in the security management of tourism as an instrument that contributes to early risk detection, preventive action, and crisis response. The theoretical framework aims to integrate concepts of tourism security, security management, and intelligence analysis, while the methodology combines qualitative and quantitative approaches with illustrative case studies. Particular emphasis is placed on the intelligence cycle, data triangulation, and analytic assessment as mechanisms for reducing uncertainty and increasing decision reliability. Using evidence from effective-practice cases, most notably the coordinated response of Barcelona's tourism sector to the 2017 terrorist attack, the paper demonstrates that integrating intelligence analysis into managerial processes enables faster, more coordinated action, protects visitors, and helps safeguard destination reputation. The study also identifies persistent challenges: institutional and regulatory constraints, data overload, cognitive biases, and the limits of expert forecasting. Mitigation measures are outlined through structured analytic techniques, alternative scenario development, and improved inter-institutional coordination. The paper concludes that intelligence analysis is an essential component of a proactive and holistic approach to tourism security, one that strengthens risk governance, supports crisis management, and helps maintain destination reputation and sustained visitor confidence.

Keywords:

Intelligence analysis, Tourism security, Security management, Risk assessment, Crisis management.

INTRODUCTION

At the beginning of the 21st century, tourism experienced exponential growth and, as an economic activity, assumed a prominent position in gross domestic product, even in countries not traditionally oriented toward tourism (UNWTO, 2024). The role of tourism in the life of an average person has changed significantly over time—from a mystical and exotic activity of the 18th–19th-century aristocracy, to a privilege gradually extended, albeit in limited form, to wider social strata in the 20th century, and finally to a mass phenomenon in which approximately 65% of European Union (EU) residents take at least one trip per year (EUROSTAT, 2024). This growth has created the need to consider security in tourism, akin to industrial and corporate security, as a distinct field of security management and to integrate it into security

Correspondence:
Lazar Radenović

e-mail:
lradenovic@singidunum.ac.rs



systems both in the strict institutional sense (the domain of bodies such as the police, intelligence services, and the military) and in the broader sense (security culture and education; all societal actors that can and should contribute to maintaining security). This ensures a holistic approach.

According to recent research by the World Tourism Organization (UNWTO), several of the main factors threatening international tourism are security-related: the war in Ukraine, the conflict in the Gaza Strip, extreme weather events, and other geopolitical risks. However, the importance of economic challenges, such as travel costs, which account for the single largest proportion of tourism related constraints, should not be overlooked (UNWTO, 2025).

Like several other industries, tourism depends heavily on the stability of its security environment. Any destabilization of the security environment, especially in the form of terrorist acts, directly affects risk perception and the decisions of tourists and investors. Particularly striking are the abrupt declines in tourist traffic in Turkey and Egypt after attacks on popular destinations, as well as the severe economic losses suffered by global air transport and related sectors after the terrorist attacks of 11 September 2001.

The evolution of contemporary security threats has made concern for security more pronounced than ever. The complexity and unpredictability of today's risks have prompted organizations that traditionally did not focus on security to address it intensively. This is especially evident in the tourism sector, where security has become an inseparable part of destination management, planning, and promotion.

Considering these trends and the principles of effective management, tourism security management is one of the key factors of successful sectoral development, including the management of risks and protective measures. This paper therefore places special emphasis on intelligence analysis, whose principal contribution to tourism security management lies in its proactive function: the timely identification of risks, challenges, and threats—providing a basis for prompt action. In addition, the importance of intelligence analysis for effective crisis management is noted. Ergo, the paper aims to outline a modus for building a theoretical basis for analyzing security phenomena in tourism and for security management in tourism, and to examine concrete ways of applying intelligence analysis within security management in the tourism sector.

By analyzing selected sources, the paper examines which models of good practice exist (such as GSOC centers and threat platforms) and how different stakeholders in tourism apply intelligence methods, as well as the theoretical frameworks and recommendations for integrating intelligence analysis into the tourism security management system.

Finally, in its Code for the Protection of Tourists, UN Tourism (UNWTO) emphasizes that the main purpose of drafting and adopting this Code is to alleviate the two greatest challenges for tourism: uncertainty and lack of trust (UNWTO, 2025b). The author's position is that intelligence analysis can be one of the tools for bridging this gap between tourists and the tourism industry. In that regard, the author quotes Bajagić: *"The mission of intelligence analysis is to assess, integrate, and interpret information; provide timely warning; reduce uncertainty; offer insight into salient facts and trends concerning events and processes of relevance to policy-makers; and, where possible, indicate how they may act under given conditions"* (Bajagić, 2015).

THEORETICAL FRAMEWORK

1. Security in tourism

Proceeding from the premise that security, at its most basic, refers to the absence of threats, endangerment, and sources of threat (Stajić, 2004), tourism security is typically conceptualized on this foundation, adapted to the sector's twenty-first-century characteristics and vulnerabilities. Therefore, Tarlow defines tourism security as measures and strategies applied to protect tourists, tourism workers, and tourism infrastructure from intentional threats such as crime, terrorism, and civil unrest, with the aim of ensuring a safe and stable environment for tourism and hospitality activities (Tarlow, 2014).



Given that the subject of this paper is intelligence analysis and its contribution to security management, which, in the author's view, is primarily reflected in enhancing preventive action (though not exclusively), the author adopts the following as the most suitable definition for the paper's theoretical framing: "Security in tourism refers to the capacity of tourism destinations and service providers to manage and reduce risks associated with terrorism, crime, and disasters, as well as to ensure a sense of safety among tourists through proactive planning" (Pizam & Mansfeld, 2006).

It should be noted that the use of the terms "*safety*" and "*security*" varies in the academic literature. According to Pizam and Mansfeld: "*security refers to protection from intentional threats, such as crime, terrorism, or sabotage, whereas safety refers to protection from unintentional harmful events, such as accidents, natural disasters, or technical failures.*" (Pizam & Mansfeld, 2006). Thus, the use of these terms more accurately describes the nature of endangerment. The same authors note that the main difference between safety and security lies in the source of danger: safety deals with unintentional threats, whereas security focuses on intentional ones (Pizam & Mansfeld, 2006). A similar distinction can be found among other authors as well. For instance, Tarlow writes: "*In the context of tourism, safety refers to the prevention of accidents and unintentional harm, whereas security relates to the prevention of intentional acts such as crime or terrorism. Both components are essential for tourist satisfaction and the competitiveness of a tourism destination.*" (Tarlow, 2014).

2. Security management

In a broader sense, security management may be defined as fact-based decision-making aimed at achieving security, that is, a process directed toward appropriate responses to potential and actual threats so as to reduce their harmful effects (Dragišić & Radojević, 2014).

According to Lakićević, security management is defined as the system and organizational arrangement for managing security operations. More narrowly, security management comprises the totality of managerial actions, measures, and procedures whose objective—alongside prevention—is to protect an organization, institution, or system against compromise, whether accidental or intentional (Lakićević, 2016).

Based on the analysis of relevant literature - and following the view of several authors that a consensus on the specific features of security management has not been reached, as these depend on the particular field of application—it may be concluded that security in tourism represents the outcome of an organized, systemic, and interdisciplinary process realized through the framework of security management. It consists of a comprehensive set of activities among which, from the standpoint of intelligence analysis as well as corporate practice¹, the author emphasizes: (1) risk identification and assessment; (2) preventive action; and (3) response in crisis situations. In this context, security management functions as an institutionalized mechanism for implementing security, aligned with standards, procedures, and cross-sector cooperation (public sector, private sector, and local communities).

3. Intelligence analysis

In their monograph, Pavlićević and Stevanović define intelligence analysis as a systematic process of collecting, processing, evaluating, and interpreting information in order to produce assessments that support decision-makers. This process uses both quantitative methods (e.g., descriptive statistics, indicators) and qualitative analysis (e.g., content analysis, scenario building), adapted to the problem and decision context (Pavlićević & Stevanović, 2025). They further note that intelligence analysis, as a multidisciplinary activity, relies, among other approaches, on probability theory, decision analysis, statistical and data analysis, signal detection theory, game theory, operational research, and qualitative analysis, in the process of drawing conclusions. (Pavlićević & Stevanović, 2025)

¹ The Hilton Group, through its Global Security Operations Centers, conceptualizes security management as comprising three core domains: (1) forecasting—systematic anticipation of potential threats based on intelligence, trend analysis, and risk indicators; (2) preventive action—proactive measures and controls designed to mitigate identified risks before they materialize; and (3) crisis response—coordinated procedures for incident containment, continuity of operations, and post-event recovery.



We adopts Bajagić's definition of intelligence analysis as the most suitable for this paper's framework, since, in the author's view, it best establishes a necessary distance (without excluding it entirely) from the understanding of intelligence analysis as an activity tied exclusively to security and intelligence services and solely in the service of political decision-makers. According to Bajagić, intelligence analysis is, in its general cognitive, methodological, and procedural elements, grounded in the methodology of scientific research, adhering to all the rules of planning and conducting scientific inquiry, with the aim of producing final results—conclusions, explanations, assessments, forecasts, and predictions. It is considerably more sensitive than analysis in other fields, as it deals with information that may often be deliberately misleading (Bajagić, 2015).

4. Functions of intelligence analysis

Pavličević and Stevanović, regarding the function of intelligence analysis—with the note that, in this context, the term “intelligence agency” can be equated with any organization (linked to tourism) that conducts intelligence analysis as part of security management—state that the function of intelligence analysis is to make sense of a complicated mass of information (in a complex and uncertain environment), to provide meaning to events, explain the current situation and anticipate the future, and to reduce uncertainty through timely, targeted, reliable, and useful information and insights—thus emphasizing the exceptional and central importance of analysis within the intelligence agency and strongly underscoring the importance of analysis as part of the decision-making process. (Pavličević & Stevanović, 2025)

The same authors cite Roger George, who emphasizes that analysts' tasks are diverse, with key ones including trend analysis, pattern recognition, and relationship identification (Pavličević & Stevanović, 2025).

Summing up the theoretical framework, the author concludes that security in tourism, security management, and intelligence analysis are closely linked concepts whose interrelations are insufficiently explored in the existing literature. Security in tourism defines what to protect and from what (tourists from challenges, risks, and threats); security management defines how to achieve that security; and intelligence analysis offers how to enhance that protection—through knowledge, information, and forecasting.

METHODOLOGICAL FRAMEWORK

The methodological approach of this paper is based on a combination of qualitative and quantitative methods to provide a comprehensive understanding of the role of intelligence analysis in the security management of tourism. This approach integrates in-depth conceptual interpretation with the analysis of measurable indicators.

The aim of the research is to determine how intelligence analysis is applied in the security management of tourism. The core research questions focus on identifying the functions of intelligence analysis in the tourism context, its contribution to risk management, and the possibilities of applying analytical techniques to the planning and implementation of security measures in the tourism sector.

The study is grounded in a qualitative analysis of relevant academic and professional literature, coupled with a quantitative analysis of statistical data that illustrates the influence of security factors on tourism. The qualitative approach enables the interpretation of complex phenomena and processes, while the quantitative approach provides an empirical basis and concrete indicators for corroborating the findings (Milosavljević & Radosavljević, 2013).



1. Data sources

The study relied on secondary data sources, including:

- Scholarly articles and monographs by domestic and international authors (Bajagić, Pavličević, Pizam, Tarlow, Lowenthal, and others),
- Official reports and statistics from international organizations (UNWTO, Eurostat) and relevant standards (e.g., ISO).
- Publications and guidelines issued by relevant institutions (e.g., Ministry of Foreign Affairs of the Republic of Serbia; Catalan Tourist Board, U.S. Justice Department).
- Open-source intelligence (OSINT) sources, specialized security/OSINT platforms, and corporate security reports (e.g., Hilton GSOC, Hozint).

The selection criteria for sources included:

- Relevance to the topic of security in tourism and to intelligence analysis (including relevance for analyzing the historical context),
- Source validity (academic institutions, official organizations, recognized experts),
- Recency of sources.

2. Research techniques

The following research techniques were applied:

- Content analysis—systematic review and categorization of relevant texts to identify key concepts and map the functions and roles of intelligence analysis in tourism;
- Statistical-data analysis—processing and interpretation of quantitative datasets for the purpose of trend identification, quantitative representation of risks, and assessment of economic impacts;
- Comparative analysis—comparing domestic and international practices and cases that demonstrate the application of intelligence analysis (e.g., Barcelona 2017; Tunisia);
- Case studies—detailed analysis of specific events in tourism (e.g., the response of Barcelona's tourism sector to a terrorist attack) to illustrate the role of intelligence analysis in practice;
- Theoretical synthesis—integrating existing models (intelligence cycle, data triangulation, risk management cycle) into a single framework applicable to the tourism sector.

3. Limitations of the study

The study relies predominantly on secondary sources and public materials, which implies limitations with respect to access to internal and confidential data from security services and corporate systems.



ROLES OF INTELLIGENCE ANALYSIS IN THE SECURITY MANAGEMENT OF TOURISM

In line with the paper's theoretical framework, this paper considers two complementary approaches to examining the role of intelligence analysis in the security management of tourism: a functional and a managerial one. The functional approach views intelligence analysis as an analytical function composed of several phases or roles within security management; it shows what intelligence analysis does and how it contributes across different phases—an essentially analyst's perspective.

Division of phases (functional approach)

1. Diagnostic role — focused on the collection, processing, and interpretation of available data with a view to timely identifying threats and risks (what is happening and why it is dangerous).
2. Prognostic role — intelligence analysis as a basis for scenarios and forecasting (what might happen and how to prepare).
3. Operational role — real-time analysis supporting decision-making during crises or high-risk situations.

The second is a managerial approach, that is, a process-oriented approach that follows the phases of classical risk management in security (Dragišić, Radojević, 2014). In this model, intelligence analysis is “embedded” into the stages of management. In this way, one can observe how intelligence analysis fits into managerial processes and structured security management, i.e., security management as a discipline. In other words, an observation from the managerial perspective.

Within such an approach, the division of phases is as follows:

1. Risk identification and assessment — intelligence analysis as a methodological framework for recognizing sources of threat and assessing the probability and the consequences of risk, using analytical models and techniques (e.g., risk matrices, indicators, scenarios).
2. Prevention and preparedness — based on identified and assessed risks, analysis provides recommendations for preventive measures, plans, procedures, and resources aimed at reducing the likelihood of incidents and mitigating their consequences.
3. Response and incident management — during a crisis, real-time analysis serves to provide timely information, assess how the situation is developing, and support decision-making (e.g., resource allocation, public communication, coordination among actors).

Although intelligence analysis is often classified among analytical methods, its contribution to security management cannot be reduced to a single instrumental function. It represents a multi-integrated, transversal analytical function that appears in various phases of security management — from risk management to crisis response and recovery. In other words, within the security management system, intelligence analysis operates as a vertical structure that connects and reinforces multiple horizontal elements of management: planning, assessment, decision-making, and communication.

Such positioning enables intelligence analysis not to be treated as an isolated method, but rather as a structural carrier that links different aspects of security management in tourism. It is precisely this multilayered nature and contextual application that form the basis for analyzing its specific roles in the continuation of this chapter.

1. Diagnostic Role / Risk Assessment

Risk assessment in a security context implies the process of identifying, analyzing, and evaluating risks that may endanger people, facilities, processes, or assets (ISO 31000, 2018). In tourism, this encompasses the safety of tourists, tourism workers, facilities (hotels, airports, museums, etc.), infrastructure, and the very image of the destination.

Intelligence analysis contributes to this process by systematizing and interpreting data from various sources, primarily open sources (OSINT), from social networks (SOCMINT) (Pavličević, 2020), but also, in limited capacities, human sources (HUMINT²) (Clark, 2013), as well as data obtained from internal security surveillance

2 While HUMINT is often immediately associated with espionage, human sources are also widely employed in civilian contexts—for example through expert consultations, structured interviews, and field observers.



systems (video surveillance, sensors, access analytics). Within the discourse, a new category/subcategory of data sources has also emerged, one that holds primary significance for tourism security — TRAVINT (Kanellopoulos, 2023), i.e., travel intelligence data.

For security managers in tourism, the model of the intelligence cycle is also important, through which intelligence studies — and within them, intelligence analysis — demonstrate how data are collected, processed, and used in intelligence and security processes for decision-making. The intelligence cycle explains a structured process that enables the systematic transformation of data into useful intelligence insights. It consists of several phases that are cyclically repeated. The intelligence cycle is not linear but rather dynamic and flexible — the phases may intertwine or repeat depending on the situation. In the security management of tourism, this model is extremely significant both for risk identification, incident prevention, and crisis response, as well as for a comprehensive conceptual understanding of the data collection process.

Based on data and analytical models, it is possible to assess the likelihood that a particular incident will occur and the consequences it might cause. Through the use of quantitative and qualitative methods (e.g., SWOT, PESTEL, or scenario analysis), intelligence analysts provide guidelines for risk ranking while presenting case examples of implementation by major global hospitality companies (e.g., Hilton, IHG).

The analysis provides the basis for deciding what requires urgent attention and what may be addressed through routine measures. This is particularly important in resource-constrained environments, which is often the case in the tourism sector of developing countries.

1.1. Application of Triangulation

According to Pavličević and Stevanović, triangulation implies the application of multiple methods in the analysis of a single phenomenon. The mentioned authors point out theoretical positions that triangulation may include: data cross-checking, researcher duplication, triangulation of theories, and triangulation of methods. They conceptualize a theoretical frameworks which emphasize that, in the context of security research, the application of triangulation is justified and almost indispensable due to: (1) the complex and multidisciplinary nature of security phenomena; (2) the need for theoretical diversity in data interpretation; (3) the different nature of data (quantitative and qualitative); (4) the limited availability of valid information; (5) the possibility of manipulation and deception in research reality; (6) the risk of research errors under conditions of uncertainty; and (7) the influence of value and interest positions on the research process (Pavličević, Stevanović, 2025). With such an approach, the reliability of analyses increases, and a more comprehensive understanding of security processes is enabled.

1.2. Analytical Assessment

Analytical assessment represents the highest level of processing intelligence data and results in an institutional assessment of the security situation. Its reliability depends on a thorough understanding of all relevant elements that influence the area under analysis. To achieve this, it is necessary to use accurate and up-to-date data, as well as to ensure their proper interpretation and formulation (Pavličević, Stevanović, 2025).

Pavličević and Stevanović note that the assessment is based on in-depth knowledge of activities, stakeholders, methods, and objectives that affect the protected values, and as such it constitutes an analysis of conditions within a specific spatiotemporal context, serving the tasks of security providers (Pavličević, Stevanović, 2025).

The usual structure of an analytical assessment includes:

- general concept,
- analysis of relevant phenomena,
- determination of the security situation,
- evaluation and conclusions,
- forecast of the situation, and
- definition of security tasks (Dragišić, Radojević, 2014).



Sims, in describing the necessary qualities of analysts—in our case within tourism security management—emphasizes that: “analysts must be able to define the problem, analyze its components, identify causes, and clearly communicate their conclusions” (Sims, 2010).

It is worth noting that intelligence analyses focused on risk assessment are available to both organizations and individuals (tourists, travelers). As an example, we will take the Belgian company Hozint – Horizon Intelligence, which offers these services. Among the services they provide are: AI-sorted regular reporting, risk assessments, email alerts, the possibility of focusing on a specific issue, the possibility of automated monitoring, and access to a database of event history dating back up to five years.

At the national level, many countries (such as the United States, EU member states, etc.) have developed systems for profiling and assessing travel risks upon tourist entry—for example, analyses of passenger name records (PNR) and other methods of travel intelligence analysis (TRAVINT), which serve to detect potentially dangerous travelers before they set foot on the destination’s territory.

2. Prognostic Role / Risk Prevention

In the tourism sector—where even the perception of threat can lead to a significant drop in visitor numbers—preventive measures must be based on reliable information, trend analysis, and analytical insight. Against this backdrop, intelligence analysis plays a pivotal role in enabling timely planning of preventive measures. The outcome of a high-quality risk assessment consists of specific recommendations to a destination’s or company’s management: which preventive measures to introduce, what to monitor closely, and how to prioritize the allocation of security resources. Intelligence analysis also facilitates the recognition of different forms of threats—strategic, tactical, and operational alike.

Intelligence analysts employ a range of methods, including quantitative risk models, scenario analysis, SWOT and its variants, as well as qualitative expert judgments.

Additionally, by using tools such as geospatial analysis, social-media trend monitoring, and the tracking of health and crime data, it becomes possible to detect risk factors before they escalate. Of particular importance is that intelligence analysis enables trend forecasting and early warning. For example, through pattern analysis one can discern the emergence of new threats: if a series of minor security incidents is observed in a given region, intelligence analysis may indicate a developing trend that warrants heightened attention before a major incident occurs. It is precisely this proactive quality that distinguishes traditional incident response from contemporary risk management informed by intelligence.

It is standard practice for most ministries of foreign affairs worldwide to issue traveler-facing reports based on risk assessment and preventive action. The Ministry of Foreign Affairs of the Republic of Serbia, on its website, has a section titled “Visas and Travel Advice,” which lists all countries with individual risk assessments and preventive guidance. The suitability of a given country for travel is presented on a graded scale:

1. Free travel with routine caution
2. Travel with additional precautions
3. Travel only in cases of absolute necessity
4. Not recommended

In addition, the advisories provide an assessment of the security situation, the public-health situation, and other relevant notes. (Ministry of Foreign Affairs RS, 2025)

Today, security services and intelligence activities—and thus intelligence analysis—have become commercial services. The exclusivity of “state affairs” across spheres of global society is disappearing (examples range from private healthcare and education to private flights and space exploration), and we are witnessing the “privatization of security.” Avant (2005) writes that “*The privatization of security refers to the transfer of traditional state security functions—such as protection, surveillance, and intelligence—to private firms operating on a for-profit basis*” (p. 16).



Since security has entered the commercial arena, there is even a growing practice of the state delegating security functions to private entities. Building on Avant's (2005) account of security privatization, the delegation of state security functions increasingly involves contracting private actors to undertake roles once reserved for public agencies—ranging from critical-infrastructure protection and intelligence analysis to surveillance, threat assessment, and, in some cases, direct participation in armed conflicts (Avant, 2005).

The use of intelligence analysis in risk assessment has enabled tourism organizations that integrate intelligence reports into their planning processes to better prepare their staff and infrastructure. For instance, airlines and tour operators rely on so-called travel risk intelligence systems that monitor global security trends and issue travel risk alerts for countries worldwide. Such intelligence services analyze data on crime, terrorism, conflict, health, and other risks, and assign safety ratings to destinations.

Ultimately, intelligence analysis empowers decision-makers to manage resources proactively—decisions regarding the deployment of additional security staff, the installation of surveillance cameras, the establishment of checkpoints, or adjustments in logistical planning can be made based on data and forecasts generated through analytical processes.

Many international companies—such as Hilton—have developed Global Security Operations Centers (GSOCs) that use intelligence platforms for risk monitoring. These centers operate 24/7, tracking political developments, public-health crises, criminal activity, and natural hazards worldwide.

For example, if the analytical team detects a rise in anti-government demonstrations in a destination such as Barcelona while a large sporting event is scheduled near the hotel, the GSOC can proactively alert hotel management to reinforce physical security, organize internal guest communications, or propose alternative movement routes.

In smaller tourism destinations/localities, where centers such as GSOCs do not exist, the relevant authorities can use commercial or publicly available intelligence tools—such as Global Incident Map, Crisis24, or the Event Information Service (EIS)—to assess the security situation. These tools allow local authorities and operators—who may not have the resources for dedicated intelligence centers—to access real-time information on incidents, risks, and emerging threats. By integrating such platforms into operational planning, they can enhance situational awareness, improve risk prevention strategies, and better inform both staff and travelers about potential hazards.

3. Operational Role / Managing Security Incidents

The role of the intelligence analyst at this stage is to contribute—through their expertise and analyses—to the decision-makers' decision-making process. We cite former CIA Deputy Director Douglas MacEachin: *"The role of the analyst in the policy process is akin to that of a scout to a football coach. The scout's task is not to predict the final score in advance, but to assess the opponent's strengths and weaknesses so that the coach can craft a winning strategy. Thereafter, the scout sits in the box with a powerful pair of binoculars and reports on specific weak points the coach can exploit"* (Pherson, Heuer, 2020).

A particularly significant contribution of intelligence analysis to the management of security incidents lies in its standards, which in crisis situations regulate the flow of information directed toward decision-makers. In this way, decision-making can be based on information of the highest possible reliability—while at the same time acknowledging the limiting factors inherent in perceiving events as they unfold in real time.

The idea of standards in intelligence analysis is grounded in the principle that information must meet specific criteria to be considered useful. Trbojević and Malbašić emphasize that "at the core of the intelligence-security cycle lies information. For a piece of data to be recognized as information of security relevance, it must meet the following characteristics: certainty (it must be objective), completeness, compatibility, and interpretability (there must be a possibility of verifying all of its elements), attributability (it must be linked to an identified source), timeliness, localization (it must be defined in time and space), and actuality (it cannot refer to previously known facts but must contain previously unknown elements, in whole or in part)" (Trbojević, Malbašić, 2022).



This framework ensures that intelligence analysis does not simply accumulate raw data but transforms it into information that is structured, verifiable, and actionable for decision-makers.

According to Lowenthal (2017), intelligence information should meet four key standards:

- Timely – delivered on time and in an appropriate format, even if not entirely complete.
- Tailored – focused on the specific needs of policymakers or management, without loss of objectivity or politicization.
- Digestible – concise in form and length; the message should be clear and easily understandable with minimal effort.
- Clear – explicitly distinguishes what is known, unknown, and inferred through analysis, while also indicating the degree of confidence.

The terrorist attack carried out on 17 August 2017 in Barcelona—on La Rambla, one of the city’s busiest tourist areas—stands as a representative example of real-time challenges in security management in tourism. At the moment of the incident, the operational use of intelligence analysis played a critical role—not only in the rapid recognition of the attack pattern and potential accomplices, but also in assessing the risk of secondary attacks and managing the information flowing in from the field. In this context, intelligence analysis functioned as a tool for real-time decision support, enabling security structures to prioritize objectives, quickly identify the most vulnerable zones, allocate resources efficiently, and coordinate communication among police, health, and tourism services. In doing so, it helped minimize consequences and prevent broader escalation (Huertas, Oliveira, 2019).

Of particular relevance to the topic of this paper is the reaction of the tourism sector in Barcelona, which illustrates coordinated crisis management and serves as an example of good practice (Cristófol, de-San-Eugenio-Vela, Paniagua-Rojano, 2020):

- Tourism organizations and hotels in the La Rambla zone immediately activated emergency protocols for crisis situations (evacuation, guest accounting).
- According to the Catalan Tourist Board, within the first 60 minutes of the attack, tourist information centers in Barcelona began translating and distributing safety instructions in English, French, German, and Chinese.
- Tour operators cooperated in real time with the Mossos d’Esquadra (police) and CECAT (Emergency Coordination Center).
- Travel agencies were granted access to updated data and maps of restricted areas to inform their guests.
- Unlike Paris in 2015 and Brussels in 2016—where tourists were left without information for hours—Barcelona avoided chaos by providing timely updates.
- A special call center for tourists with multilingual support was launched within just two hours of the attack.
- The Visit Barcelona web portal and official social media profiles immediately switched to crisis communication mode, in contrast to Brussels, where many tourists received their first information from the media rather than institutions.
- Hotels in Barcelona organized temporary gathering areas for tourists and facilitated communication with embassies.
- Mobile teams for psychological support were deployed on the same day, unlike in Paris, where such services were delayed by several days.



CHALLENGES AND LIMITATIONS OF USING INTELLIGENCE ANALYSIS IN TOURISM

The use of intelligence analysis in security management in tourism is an important instrument for preventing, assessing, and managing risks that may endanger tourist destinations, tourists, and the tourism industry as a whole. Nevertheless, in practice, a number of challenges and limitations arise that can reduce the effectiveness of this process.

Data Processing and Overload

In the modern era, the very activity of data collection—regardless of its sources—no longer represents a great challenge. The main obstacle lies in data processing, the well-known dilemma of “knowing what we know.” As early as the beginning of this century, this problem had already become evident and was documented in many studies and reports (U.S. Department of Justice, 2004). Today, with the development of advanced technologies such as artificial intelligence, robotics, and the general trend of replacing human labor with technology, this problem has become even more pronounced.

Gilli and Phythian argue that, despite the spread of sophisticated surveillance technologies and information systems, intelligence work remains fundamentally an intellectual endeavor. Software can connect disparate datasets and build large “data warehouses,” but deriving meaning from these interconnected data requires human judgment and reasoning. Facts do not speak on their own; analysis hinges on testing competing explanations against the available evidence—i.e., on abductive inference (Gill & Phythian, 2018).

Institutional and Normative Framework

Effective use of intelligence analysis in tourism requires the existence of clearly defined institutional mechanisms and a normative framework that regulate the collection, processing, and exchange of data. In many countries, the tourism sector is not sufficiently integrated into national security systems, which leads to data fragmentation and inconsistencies in the application of analytical procedures. A flagrant example of this challenge is the terrorist attack in Sousse, Tunisia, in 2015. The investigation showed that the consequences of this attack—and possibly the attack itself—could have been avoided through better coordination between the tourism sector and the security sector (Agarwal, Stephen, Mawby, 2021).

An additional challenge is cross-border cooperation: different legal systems, levels of data protection, and procedural differences can slow down or even prevent the timely exchange of relevant information. In the context of tourism, where threats can spread rapidly across borders, this factor gains particular importance.

Without an adequate institutional and normative framework, even the most advanced analytical techniques have limited reach, as continuity in data access and verification is lacking.

Disruptive Factors

Within tourism security management, the process of intelligence analysis represents a key instrument for risk assessment and for the adoption of preventive and reactive measures. However, this process is not immune to the influence of cognitive mechanisms that may compromise the objectivity of conclusions. As research in this field shows (Pavličević, Radenović, 2020a), the most significant disruptive factors include:

- confirmation bias – the tendency to favor information that confirms pre-existing assumptions;
- anchoring effect – excessive reliance on initial data when assessing risk;
- stereotyping and generalization – oversimplifying complex phenomena in tourism based on preconceived notions;
- recency and primacy effects – overvaluing the most recently or initially obtained information compared to its actual relevance.

In the context of tourism, these factors can lead to underestimation or overestimation of certain threats, which directly affects the quality of tourism security management. As mitigation mechanisms, the use of structured analytical techniques and data triangulation is recommended, as these reduce subjectivity and increase the reliability of recommendations.



Limitations of Expert Judgment and Prediction

Although expert assessment and the experience of analysts are of great importance in managing security risks in tourism, research shows that there are natural limitations in their ability to reliably predict the course of complex events.

One of the key problems is the paradox of expertise, where highly experienced analysts often unconsciously favor established models and previous experiences, while neglecting new or unconventional sources of information (Pavličević, Radenović, 2020b). This can lead to overlooking “weak signals” that indicate emerging security risks in tourism.

Another challenge is the uncertainty of human behavior—since a large number of stakeholders (tourists, tour operators, hoteliers, local authorities) make decisions under the influence of economic, social, cultural, and political factors, as well as unforeseen circumstances such as security incidents or global health crises.

A third problem is reliance on the “most likely” scenario, which can result in neglecting less probable but high-risk events.

To mitigate these limitations, the following measures are recommended:

- development of multiple alternative scenarios specific to the tourism sector;
- regular updating of assessments in line with new information;
- teamwork and the exchange of expert opinions from different fields;
- the application of a “red teaming” approach to test existing assumptions.

Such approaches enable tourism security management to maintain flexibility and effectiveness in conditions of a dynamic and often unpredictable environment.

CONCLUSION

Tourism, as an industry of global significance, increasingly depends on a stable and secure environment. Contemporary security challenges—from terrorism and political crises to natural disasters and health threats—create the need to shift from a reactive to a proactive approach in security management. As Dragišić and Radojević note, good management above all requires a proactive approach, specifically the anticipation of problems and timely preparation for their resolution (Dragišić, Radojević, 2014). This paper has shown that intelligence analysis represents a key instrument in this process, enabling the timely detection and assessment of risks, the planning of preventive measures, and the effective management of security incidents.

The analysis of theoretical and practical frameworks has shown that intelligence analysis in tourism is not an isolated function but an integrated element of the phases of tourism security management—from risk identification and prevention to crisis response. Its use, through models such as the intelligence cycle, data triangulation, and analytical assessments, increases the accuracy of information, reduces uncertainty, and enables decision-makers to allocate resources optimally.

Examples of good practice, such as the crisis response of Barcelona’s tourism sector after the 2017 terrorist attack, demonstrate that integrated intelligence analysis allows for faster and more coordinated reactions, reducing damage and restoring tourist confidence. While presenting case examples of implementation by major global hospitality companies (e.g., Hilton, IHG), the paper highlights the new window of opportunity to tourism organizations, destinations and other tourism stakeholders, for applying intelligence-based approaches in practice. As stated previously, “privatization of security” has enabled, to a much broader specter of clients/tourism stakeholders (even those with minimal resources), availability of intelligence analysis via: private companies that specialize in intelligence analysis, a much less constricted market for hiring experts and ex-intelligence officers, even both subscription-based and free-to-access websites publishing intelligence analysis and security advices. Supplementary, current challenges in the use of this approach are examined—from institutional and normative limitations to the need for greater capacities and improved training of analysts.



From the standpoint of scientific contribution, this paper seeks to conceptualize the foundations that bring together the concepts of tourism security, security management, and intelligence analysis into a unified analytical framework—something that has not previously been attempted in domestic literature. Practically, the findings can serve as a basis for developing guidelines and procedures that will enable tourist destinations and organizations to systematically apply intelligence analysis in the everyday management of risks.

It is the author's belief that, amid growing threat complexity, sustainable tourism development requires a holistic approach to safety and security, with intelligence analysis playing a prominent, preventive role reinforced by organizational learning. Modernity has expanded our toolkit, but intelligence remains the decisive edge—the tip of the spear for safety and security. Only through the systematic, proactive use of analytical methods can destinations ensure stability, competitiveness, and long-term trust.

To conclude, the author cites Gill and Phythian: “The traditional analytical approach to risk is based on calculating probability $\times$ impact, through quantitative analysis, but if you are able to make such a calculation—then, in fact, you do not need intelligence activity. Intelligence work, on the contrary, operates precisely where unknowns and uncertainty prevail, transforming them into risks that can be more easily managed and mitigated.” (Gill & Phythian, 2018).

REFERENCES

- Agarwal, Sheela, Page, Stephen J. and Mawby, Rob (2021) *Tourist security, terrorism risk management and tourist safety*. Annals of Tourism Research, 89: 103207. Retrieved date of access 26.08.2025. from: <https://uhra.herts.ac.uk/id/eprint/9041/> ISSN 0160-7383
- Avant, D. D. (2005), *The Market for Force: The Consequences of Privatizing Security*, Cambridge University Press, Retrieved date of access 22.08.2025. from: https://www.researchgate.net/publication/227389719_The_Market_for_Force DOI:10.1017/CBO9780511490866
- Bajagić, M. (2015). *Metodika obaveštajnog rada*. Beograd: Kriminalističko-policijska akademija.
- Clark R. (2013), *Intelligence Collection*, Washington D.C CQ Press.
- Cristófol, F.-J., de-San-Eugenio-Vela, J., Paniagua-Rojano, F.-J. (2020). *Active listening in the management of crisis communication: Case study of the 2017 terrorist attack in Barcelona*. Communication & Society, 33(4), 61-74. Retrieved date of access 17.08.2025. from: <https://doi.org/10.15581/003.33.4.61-74> , DOI: 10.15581/003.33.4.61-74
- Dragišić, Z., Radojević K. (2014). *Bezbednosni menadžment*. Beograd: Fakultet bezbednosti.
- EUROSTAT (April 2025). Tourism statistics, Retrieved date of access 01.08.2025. from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Tourism_statistics#Highlights
- Gill, P., Phythian, M. (2018). *Intelligence in an Insecure World*. Cambridge: Polity Press. Retrieved date of access 19.08.2025. from: https://www.researchgate.net/publication/27247055_Intelligence_in_an_Insecure_World
- Hilton Group (June 2022), *Global safety&security team brochure*. Retrieved date of access 02.08.2025. from <https://travelwithpurpose.hilton.com/wp-content/uploads/sites/3/2022/06/Safety-and-Security-Department-Brochure-2022.pdf>
- Hilton Group (March 2025), *Global safety and security team overview*. Retrieved date of access 01.08.2025. from https://cr.hilton.com/wp-content/uploads/2019/05/Hilton_Safety_Security.pdf
- Hozint – Horizon Intelligence Srl (September 2025). *Hozint Brochure*. Retrieved date of access 03.09.2025. from: https://www.hozint.com/platform/#download_brochure
- Huertas, A., Oliveira, A. (2019). *How tourism deals with terrorism from a public relations perspective: A content analysis of communication by destination management organizations in the aftermath of the 2017 terrorist attacks in Catalonia*. Catalan Journal of Communication & Cultural Studies. 11. 39-58. Retrieved date of access 11.08.2025. from: https://www.researchgate.net/publication/333606490_How_tourism_deals_with_terrorism_from_a_public_relations_perspective_A_content_analysis_of_communication_by_destination_management_organizations_in_the_aftermath_of_the_2017_terrorist_attacks_in_Catal , DOI: 10.1386/cjcs.11.1.39_1.
- ISO - International Organization for Standardization (June 2018). *IEC 31010, Risk management — Risk assessment techniques*. Retrieved date of access 01.08.2025. from: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:vl:en>



- Kanellopoulos, A. (2023). *Travel intelligence as a tool for counterintelligence and border security*. Security and Defence Quarterly. 45(1), Retrieved date of access 04.08.2025. from: https://www.researchgate.net/publication/376026877_Travel_intelligence_as_a_tool_for_counterintelligence_and_border_security , DOI: 10.35467/sdq/174523.
- Lakićević, R. (2016). *Bezbednosni menadžment*. Niš: Visoka škola strukovnih studija za kriminalistiku i bezbednost.
- Lowenthal, Mark M. (2017), *Intelligence: from secrets to policy*, Los Angeles: CQ Press, SAGE Publications. Retrieved date of access 02.08.2025. from: https://archive.org/details/intelligencefrom0000lowe_7edi/page/n5/mode/2up
- Milosavljević, S., Radosavljević, I. (2013). *Osnovi metodologije političkih nauka*, Beograd: Službeni glasnik.
- Ministry of Foreign Affairs of Republic of Serbia (September 2025). *Visas and Travel Advice*. Retrieved date of access 06.09.2025. from: <https://www.mfa.gov.rs/en/citizens/travel-abroad/visas-and-states-travel-advisory>
- Pavlićević, P. (2020). *Analitika u funkciji nacionalne bezbednosti*, Beograd: Akademija za nacionalnu bezbednost.
- Pavlićević, P., Radenović, L. (2020), *Remetilački faktori u procesu obaveštajne analize: kognitivni mehanizmi u fokusu*, Nacionalna bezbednost, br. 12/2020, Beograd: Akademija za nacionalnu bezbednost. 11–34.
- Pavlićević, P., Radenović, L. (2020). *Obaveštajna analiza i ekspertsko mišljenje*, Novi Sad: Kultura polisa. br. 43., 305–319.
- Pavlićević, P., Stevanović, M. (2025). *Savremena obaveštajna analiza: Teorijski osnovi, metode i problemi institucionalnog prepoznavanja istine*, Beograd: Institut za političke studije
- Pherson R., Heuer R. (2020), *Structured Analytic Techniques for Intelligence Analysis*, Washington D.C.: CQ Press.
- Pizam, A. (2010), *International Encyclopedia of Hospitality Management*, Oxford: Butterworth-Heinemann, Oxford. Retrieved date of access 04.08.2025. from: https://lambtonhat.weebly.com/uploads/4/4/1/3/4413567/international-encyclopedia-of_hosp_man.pdf
- Pizam, A., Mansfeld, Y. (2006). *Tourism, Security and Safety: From Theory to Practice*, Oxford: Butterworth-Heinemann. Retrieved date of access 11.08.2025. from: https://nibmehub.com/opac-service/pdf/read/Tourism-%20Security%20and%20Safety%20_%20from%20theory%20to%20practice.pdf
- Sims, Jennifer E. (2010), Decision Advantage and the Nature of Intelligence Analysis, In Loch J. (Ed.), *The Oxford Handbook of National Security Intelligence*, New York: Oxford University Press.
- Stajić, Lj. (2004), *Osnovi bezbednosti*. Beograd: Policijska akademija.
- Tarlow, P. E. (2014), *Tourism Security: Strategies for Effectively Managing Travel Risk and Safety*, Oxford: Elsevier. Retrieved date of access 07.08.2025. from <https://dl.acm.org/doi/pdf/10.5555/2843510> ISBN: 978-0-12-411570-5
- Trbojević, M., Malbašić, Z. (2022), *Bezbednosno-obaveštajni sistemi država postjugoslovenskog prostora*, Beograd: Akademija za nacionalnu bezbednost.
- U.S. Department of Justice (July 2024). *The 9/11 Commission Report: Executive Summary*, Retrieved date of access 07.08.2025. from: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/911-commission-report-executive-summary>
- UN Tourism (May 2025). *World Tourism Barometer*. Volume 23. Issue 2. Retrieved date of access 02.09.2025. from: <https://www.untourism.int/un-tourism-world-tourism-barometer-data>
- UNWTO – processed by Our World in Data (September 9, 2025). “Share of GDP from tourism” [dataset]. UNWTO, “Tourism direct GDP as a proportion of total GDP” [original data]. Retrieved date of access 01.09.2025 from <https://archive.ourworldindata.org/20250909-093708/grapher/tourism-gdp-proportion-of-total-gdp.html>
- World Tourism Organization (2022). *International Code for the Protection of Tourists*, UNWTO, Madrid, Retrieved date of access 19.08.2025. from <https://doi.org/10.18111/9789284423361> , DOI: 10.18111/9789284423361
- World Tourism Organization (2024). *International Tourism Highlights, 2024 Edition*. UN Tourism, Madrid. Retrieved date of access 21.08.2025. from <https://doi.org/10.18111/9789284425808> , DOI: 10.18111/9789284425808