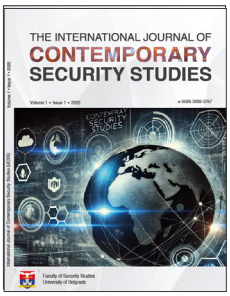
Volume 2 • Issue 2 • 2026

Faculty of Security Studies, University of Belgrade

International Journal of Contemporary Security Studies (IJCSS)



Review Article

The Delphi Method in Security Threat Assessment: Principles, Applications, and Methodological Challenges

Josef Smolík[1], Ivana Olecká[1*]

[1] Police Academy of the Czech Republic in Prague, Faculty of Security Management, Department of Security Studies, Lhotecká 559/7 143 01 Prague 4, Czech Republic; smolik@polac.cz.

[2] Police Academy of the Czech Republic in Prague, Faculty of Security and Law, Department of Criminology, Lhotecká 559/7 143 01 Prague 4, Czech Republic; olecka@polac.cz.

* Correspondence: olecka@polac.cz.

Received: 13 May 2026; Revised: 23 July 2026; Accepted: 1August 2026; Published: 24 August 2026.

ABSTRACT

This methodological review examines the Delphi method as an approach to structured expert judgement for the assessment of security threats and its potential application in defence-related decision-making. The paper is based on a narrative methodological review of the literature synthesising the principal methodological concepts, variants, procedures, strengths, limitations, and representative applications of the Delphi method in defence and security research. Particular attention is devoted to methodological requirements for expert selection, consensus assessment, uncertainty communication, and the interpretation of expert judgements in complex security environments. The article further illustrates the practical application of the method through a hypothetical Delphi study protocol and an accompanying threat assessment matrix developed for illustrative purposes. The principal contribution of the paper lies in integrating general Delphi methodology with the specific methodological and organisational challenges of defence and security research. The review concludes that the Delphi method provides a valuable framework for structuring expert judgement under conditions of uncertainty; however, its findings should be interpreted as conditional expert assessments that require careful methodological design and, where possible, validation through empirical evidence or complementary analytical approaches.

KEYWORDS

Delphi method; security threats; expert assessment; strategic decision-making; military planning

1. Introduction

The assessment of security threats is a key prerequisite for strategic decision-making within the defence environment. Contemporary threats include not only traditional military risks, but also cyberattacks, terrorism, pandemics, migration, hybrid threats, and climate change, all of which are interconnected and transcend state borders. These threats are increasingly interconnected, transnational, and multidimensional, making the traditional distinction between internal and external security progressively less relevant. The contemporary security environment is shaped by the interaction

Academic Editor:
Prof. Dr. Vladimir M. Cvetković

Smolík, J., & Olecká, I. (2026). The Delphi Method in Security Threat Assessment: Principles, Applications, and Methodological Challenges. *International Journal of Contemporary Security Studies*, 2(2), 1-22.

of military, political, economic, technological, societal, and environmental factors, requiring analytical approaches capable of addressing high levels of complexity and uncertainty (Danics, Smolík, & Strnad, 2024, p. 15).

Because the terminology used in security research is not entirely uniform across disciplines and organisations, several key concepts require clarification. In this article, a threat is understood as a potential source of harm capable of causing adverse consequences for protected assets or security interests; risk refers to the combination of the likelihood of a threat materialising together with its potential consequences, while also reflecting vulnerability and exposure. A hazard denotes a potentially damaging event or condition that may contribute to the emergence of a threat. Uncertainty refers to incomplete knowledge regarding future developments or their consequences. A forecast represents a structured expert assessment of future developments based on currently available information, whereas a prediction implies a stronger expectation that a particular future outcome will occur. A scenario is understood as a coherent and plausible description of one possible future development rather than a prediction of what will necessarily happen. The precise interpretation of these concepts varies across security studies, risk analysis, intelligence analysis, and futures research; the above definitions are adopted solely for the purposes of this methodological review.

The prediction of security threats is difficult because available data are heterogeneous and incomplete, and certain phenomena cannot be directly quantified (Mareš, 2014, p. 125; Smolík, 2018; Tetlock & Gardner, 2016; Zelinka, 2010). To address these challenges, security research combines quantitative methods, including regression analyses, time-series analysis, network analysis, and simulations, with qualitative approaches such as case studies, discourse analysis, and expert assessments to explain both actors' behaviour and the broader context of security threats (Redmiles, Acar, Fahl, & Mazurek, 2017)users will pick dancing pigs every time,\" warns an oft-cited quote from well-known security researcher Bruce Schneier. This issue of understanding how to make security tools and mechanisms work better for humans (often categorized as usability, broadly construed. Contemporary studies increasingly apply multidimensional predictive frameworks integrating demographic, institutional, socio-economic, and behavioural variables, together with hybrid approaches combining empirical evidence, data-driven predictive models, machine-learning techniques, and expert judgement to analyse complex security phenomena under conditions of uncertainty (Cvetković, Lipovac, Renner, Stanarević, & Raonić, 2025). While machine-learning techniques can identify recurring patterns in large datasets, expert-based methods remain indispensable for interpreting weak signals, emerging threats, and strategically relevant uncertainties that cannot yet be inferred from historical observations (Plamadeala, 2025).

Among the expert-based approaches, the Delphi method is particularly well suited to security-threat assessment because it combines structured expert judgement with an iterative process of controlled feedback and anonymous evaluation (Sablatzky, 2022). Other expert-oriented approaches, including expert panels, participatory methods, scenario workshops, tabletop exercises, and simulations, complement the Delphi method by enabling the modelling of crisis situations, exploring alternative scenarios, and testing decision-making under conditions of uncertainty.

This paper is a methodological review examining the use of the Delphi method for the assessment and prediction of security threats in the defence environment. Rather than presenting the results of an original Delphi survey, it synthesises current methodological knowledge, discusses the principal variants, procedures, strengths, and limitations of the method, and illustrates its potential application in security-threat assessment. The study addresses the following research question: How can the Delphi method support the assessment and prediction of contemporary security threats and under what methodological conditions can it provide a valid basis for strategic decision-making in the defence environment? The objectives of the paper are (i) to review the methodological principles of the Delphi method, (ii) to analyse its applicability to contemporary security threats, (iii) to identify its methodological strengths and limitations, and (iv) to propose recommendations for its effective use in defence-related research and practice. The original contribution of the article lies in integrating current methodological knowledge with contemporary defence applications and in providing a structured methodological framework for the use of Delphi in security-threat assessment.

2. Review Methodology

This article is based on a methodological review of the literature concerning the Delphi method and its application to security threat assessment and forecasting. Unlike a systematic review or meta-analysis, the objective was not to identify all available publications on the topic, but to synthesise the principal methodological concepts, contemporary developments, and representative applications relevant to defence and security research. The literature search was conducted using the multidisciplinary databases Scopus, Web of Science, ResearchGate, and Google Scholar. Additional sources were identified through backward citation searching and by consulting reference lists of key methodological publications. Because several influential publications on Delphi methodology are available as books or book chapters, these sources were also included where they represented seminal contributions to the development of the method. Electronic searches were complemented by manual searches of reference lists and by the inclusion of seminal methodological monographs and national publications that have played an important role in the development of Delphi methodology and forecasting research. The literature search was conducted in January 2026 and covered publications issued between 1967 and 2025. No lower publication-date limit was imposed, as seminal works documenting the origins and methodological development of the Delphi method were considered essential for the review; more recent publications were used primarily to capture contemporary methodological developments and applications in defence and security research. The review was limited to publications available in English or Czech. Following screening and assessment of eligibility, 62 sources were included in the final review. The methodological relevance of each source was evaluated according to the clarity and transparency of its description of the Delphi design, its contribution to the development or critical assessment of the method, the transferability of its methodological findings, and its relevance to forecasting, security, defence, risk assessment, or strategic decision-making. The search strategy combined keywords related to the Delphi method and security research, including Delphi method, Delphi technique, expert consensus, expert judgement, forecasting, security threats, risk assessment, security forecasting, defence, military, cybersecurity, critical infrastructure, terrorism, hybrid threats, and scenario planning. Boolean operators (AND/OR) were used to combine methodological and application-oriented search terms. The review included peer-reviewed journal articles, scholarly books, book chapters, methodological manuals, and selected institutional publications that addressed (i) the methodological principles of the Delphi method, (ii) its design and implementation, (iii) strengths and limitations, or (iv) applications in security, defence, strategic forecasting, or related fields. Seminal publications describing the original development of the Delphi method were retained regardless of publication date because of their continuing methodological relevance. Publications were excluded if they only mentioned Delphi without describing its methodology or application, focused exclusively on unrelated disciplines without transferable methodological implications, or consisted of non-scholarly sources lacking sufficient methodological transparency. The retrieved literature was screened by title, abstract, and full text for relevance to the objectives of the review. The selected publications were analysed using narrative synthesis, focusing on recurring methodological themes, procedural recommendations, areas of application, and reported advantages and limitations. Particular attention was given to studies demonstrating the use of Delphi for security forecasting, defence planning, cyber risk assessment, critical infrastructure protection, and strategic decision-making under conditions of uncertainty.

3. The Delphi Method – Principles and Characteristics

The Delphi method in its modern form was developed by the RAND Corporation research team in Santa Monica, particularly by Olaf Helmer, Nicolas Rescher, and Norman Dalkey, with the aim of overcoming the limitations of traditional expert conferences and systematically achieving expert consensus (Helmer, 1967; Linstone & Turoff, 1975; Manski, 2007). The name refers to its prognostic function, namely the use of expert estimates to predict future developments (Luo & Wildemuth, 2017). The method emerged within projects funded by the United States Air Force from the 1950s onwards, when it was intended to help estimate the targets of a hypothetical Soviet attack on the United States and to address the lack of reliable data through the combination of empirical informa-

tion and expert intuition (Helmer, 1967; Linstone & Turoff, 1975, p. 10; Šenovský, 2021). Its purpose was to support strategic decision-making and prepare decision-makers for possible security scenarios (Helmer, 1967), while it was also applied to the prediction of crime and other social phenomena (viz Manski, 2007, pp. 19–20). Similar methodological requirements remain relevant in contemporary strategic issues characterised by low-probability but high-consequence risks, including nuclear security and arms-control policy (Porel, 2025).

3.1. Historical development

A major milestone in the development of the method was the study Report on a Long-Range Forecasting Study, which involved 82 experts, including prominent scientists, and predicted a number of technological innovations with considerable accuracy, such as organ transplantation, centralised databases, and automatic translation systems, although some forecasts ultimately proved inaccurate (Gordon, 2009b). The success of this study contributed to the expansion of the method into numerous fields, including healthcare, technology, education, environmental studies, social sciences, and organisational management (Al-Qutaish, 2025; Buckley, 1995; Gordon, 2009b; Reichel, 2009; Weisbord & Janoff, 2010). Over time, several variants emerged, including Real-Time Delphi, Policy Delphi, Decision Delphi, Modified Delphi, and Hybrid Delphi, all of which broadened the applicability of the method across different contexts (Al-Qutaish, 2025). Despite these advantages, Real-Time Delphi also presents methodological challenges. Continuous updating of responses may encourage premature convergence, participants have less time for reflection between revisions, and reliance on online platforms may disadvantage experts with limited technological access or digital literacy.

Within the field of security studies, the Delphi method ranks among the most frequently used expert-based tools, particularly in the analysis of military threats, weapons proliferation, terrorism, and technological development (Gordon, 2009b; Plamínek, 2008; Smolík, 2018). It is applied in the military, governmental institutions, and the private sector, and since the 1990s it has also been widely used in international relations and the analysis of global risks, with its application now extending worldwide (Linstone & Turoff, 1975). The method makes it possible not only to predict future developments, but also to achieve expert consensus, establish strategic priorities, and support decision-making under conditions of uncertainty, which makes it a significant tool for the analysis of security threats within the contemporary defence environment (cf. Helmer, 1967).

3.2. Main variants of the Delphi method

Since its introduction, the Delphi method has evolved into several variants designed to address different research objectives, decision-making contexts, and practical constraints. Although all variants retain the fundamental principles of structured expert consultation, anonymity, controlled feedback, and iterative evaluation, they differ in their primary objectives, procedures, and expected outcomes (Al-Qutaish, 2025; Gordon, 2009b; Jorm, 2025a)D.C.","title":"The Delphi Method","URL":"https://www.millennium-project.org/publications/futures-research-methodology-version-3-0-2/","editor":[{"family":"Glenn","given":"Jerome C."},{"family":"Gordon","given":"Theodore J."}],"author":[{"family":"Gordon","given":"Theodore J."}],"issued":{"date-parts":[["2009"]]}},{"id":7017,"uris":["http://zotero.org/users/14502998/items/MQ2X2NLE"],"itemData":{"id":7017,"type":"chapter","abstract":"Abstract\n This chapter describes the development of the Delphi method by the RAND Corporation in the 1950s, early criticisms of the method, and its subsequent evolution and growth in use. A wide range of variants of the Delphi method have been developed, only some of which aim to establish a consensus. The chapter examines contemporary uses of the method to establish consensus, covering its uses in making judgements on facts where the evidence is imperfect, setting methodological standards, making predictions, defining foundational concepts, determining collective values, improving professional practice, and improving policy.","container-title":"Using the Delphi Method to Establish Expert Consensus","DOI":"10.1007/978-981-96-8357-4_1

","ISBN":"978-981-96-8356-7","language":"en","note":"collection-title: Advancing Methods for Interdisciplinarity in the Social Sciences","page":"1-19","publisher":"Springer Nature Singapore","-publisher-place":"Singapore","source":"DOI.org (Crossref.

Classical Delphi

The Classical Delphi represents the original form of the method developed at the RAND Corporation during the 1950s. Its principal objective is to obtain reliable expert judgements concerning future developments through several rounds of anonymous questionnaires interspersed with controlled feedback. Experts reconsider their assessments after receiving a statistical summary of the group's responses, which gradually promotes convergence towards a stable level of consensus (Gordon, 2009b; Helmer, 1967; Linstone & Turoff, 1975). Owing to its structured and iterative character, Classical Delphi remains the preferred approach for forecasting, strategic planning, and security threat assessment where empirical evidence is limited.

Policy Delphi

Unlike the Classical Delphi, the Policy Delphi does not primarily seek consensus. Instead, its purpose is to identify, clarify, and compare competing policy options by systematically examining different expert perspectives. The emphasis is placed on exploring disagreement rather than eliminating it, making this variant particularly suitable for public policy, security governance, defence planning, and other situations in which alternative strategic responses must be evaluated (Gordon, 2009a; Jorm, 2025b).

Decision Delphi

The Decision Delphi is designed to support decision-making by structuring expert judgements into a systematic evaluation of alternative courses of action. Compared with the Classical Delphi, greater emphasis is placed on selecting practical solutions than on forecasting future developments. This variant is particularly useful when organisations need to establish priorities or evaluate strategic alternatives under conditions of uncertainty (Al-Qutaish, 2025).

Modified Delphi

The Modified Delphi adapts the original procedure to improve efficiency while preserving its fundamental methodological principles. Instead of beginning with completely open-ended questions, the first round is frequently based on predefined statements derived from previous research, literature reviews, or preliminary qualitative interviews. The number of survey rounds is often reduced, making the method less demanding for participants while maintaining satisfactory levels of expert consensus (Clyne et al., 2024; Fish & Busby, 2005; Khodyakov et al., 2020; Okoli & Pawlowski, 2004).

Real-Time Delphi

The Real-Time Delphi replaces the traditional sequence of questionnaire rounds with an online platform that enables experts to review aggregated responses and revise their assessments continuously throughout the data collection period. This considerably shortens the duration of the study while preserving the iterative nature of the Delphi process. Advances in digital technologies have therefore contributed to the growing use of Real-Time Delphi in situations requiring rapid expert consultation and timely decision support (Al-Qutaish, 2025; Jorm, 2025a)early criticisms of the method, and its subsequent evolution and growth in use. A wide range of variants of the Delphi method have been developed, only some of which aim to establish a consensus. The chapter examines contemporary uses of the method to establish consensus, covering its uses in making judgements on facts where the evidence is imperfect, setting methodological standards, making predictions, defining foundational concepts, determining collective values, improving professional practice, and improving policy.","container-title":"Using the Delphi Method to Establish Expert Consensus","-DOI":"10.1007/978-981-96-8357-4_1","ISBN":"978-981-96-8356-7","language":"en","note":"collec-

tion-title: Advancing Methods for Interdisciplinarity in the Social Sciences",”page”:”1-19”,”publisher”:”Springer Nature Singapore”,”publisher-place”:”Singapore”,”source”:”DOI.org (Crossref.

Hybrid Delphi

Hybrid Delphi combines the Delphi method with complementary qualitative or quantitative approaches, including interviews, focus groups, scenario analysis, multicriteria decision analysis, or statistical modelling. Such integration enables researchers to combine structured expert judgement with empirical evidence when addressing complex research problems (Al-Qutaish, 2025; Khodyakov et al., 2023). In security research, hybrid approaches increasingly integrate Delphi with data-driven predictive methods to support the assessment of multidimensional threats characterised by high levels of uncertainty and limited empirical evidence (Plamadeala, 2025).

Although these variants differ in their procedures and intended outcomes, they all retain the fundamental principles of systematic expert consultation and structured feedback. The selection of an appropriate Delphi variant therefore depends primarily on the objectives of the research, the availability of empirical evidence, the required level of consensus, and the practical constraints of the study (Jorm, 2025a)early criticisms of the method, and its subsequent evolution and growth in use. A wide range of variants of the Delphi method have been developed, only some of which aim to establish a consensus. The chapter examines contemporary uses of the method to establish consensus, covering its uses in making judgements on facts where the evidence is imperfect, setting methodological standards, making predictions, defining foundational concepts, determining collective values, improving professional practice, and improving policy.”,”container-title”:”Using the Delphi Method to Establish Expert Consensus”,”DOI”:”10.1007/978-981-96-8357-4_1”,”ISBN”:”978-981-96-8356-7”,”language”:”en”,”note”:”collection-title: Advancing Methods for Interdisciplinarity in the Social Sciences”,”page”:”1-19”,”publisher”:”Springer Nature Singapore”,”publisher-place”:”Singapore”,”source”:”DOI.org (Crossref.

4. The Procedure for Applying the Delphi Method

The application of the Delphi method represents a systematic approach to the prediction and analysis of security threats, which has proven particularly effective in the contemporary military context. Holcr (2009) classify this method as a prognostic expert technique based on the knowledge and practical experience of specialists. The method is founded on the assumption that carefully selected experts can provide structured judgements regarding future developments and trends under conditions of uncertainty. These judgements are understood as informed expert assessments rather than objectively verifiable predictions and may draw upon tacit knowledge that cannot always be fully articulated. This approach is especially valuable in the evaluation of military threats, where the combination of theoretical expertise, practical experience, and prognostically relevant personal attributes makes it possible to identify risks, assess their probability, and estimate their potential impact on national and allied security. The procedure for applying this method is illustrated in the workflow (Table 1).

Table 1. Workflow of a Delphi Study with Iterative Feedback Loops. *Source: authors, based on the cited literature.*

Phase	Main activities	Outputs	Iteration / Feedback
1. Problem definition	Define the research problem, objectives, scope of the study, security domain, and expected outputs. Formulate the research questions and determine whether Delphi is an appropriate method.	Clearly specified research objective and study protocol.	Starting point of the process.

2. Expert panel selection	Define selection criteria, identify and recruit experts, ensure diversity, expertise, and independence, determine panel size.	Final expert panel.	Panel may be adjusted before Round 1 if necessary.
3. Questionnaire design and pilot testing	Develop questionnaire items, scenarios or statements; conduct pilot testing; revise wording and structure.	Validated questionnaire.	Pilot ⊙ revision ⊙ final questionnaire.
4. Delphi Round 1	Experts independently complete the questionnaire anonymously. Initial opinions, ratings or forecasts are collected.	Initial dataset of expert judgements.	Beginning of the iterative Delphi cycle.
5. Data analysis and controlled feedback	Statistical analysis (e.g., median, mean, IQR, percentage agreement), identification of divergent opinions, preparation of anonymous summary for participants.	Feedback report distributed to experts.	After each round.
6. Delphi Round 2 (and subsequent rounds)	Experts review the group's responses, reconsider their own assessments, provide revised ratings and justification where appropriate.	Updated expert judgements.	Repeat analysis ⊙ feedback ⊙ revision until predefined stopping criterion is met.
7. Consensus assessment	Evaluate the degree of consensus using predefined criteria (e.g., IQR, coefficient of variation, percentage agreement, Kendall's W, stability of responses). Decide whether another round is required.	Consensus achieved or decision to continue another round.	Decision node: consensus achieved? ⊙ No: return to Phase 5; Yes: continue to Phase 8.
8.Analysis and interpretation	Aggregate final responses, identify priorities, interpret expert judgements, develop scenarios and assess implications for security planning.	Final results and expert consensus.	Final analytical phase.
9.Recommendations and reporting	Prepare the final report, formulate recommendations for policy, strategic planning, defence decision-making, and future research.	Recommendations and dissemination of findings.	End of the Delphi process.

Gordon (2009b) conceptualises the Delphi method as a controlled discussion in which the arguments underlying even extreme positions are explicitly articulated and subsequently communicated back to participants in a calm and impersonal manner. At the same time, the Delphi method is associated with a strong emphasis on ethical considerations, including confidentiality, which are particularly crucial when dealing with strategic security issues (Hendl & Remr, 2017).

The method represents an organised collection of expert judgements through repeated questionnaires accompanied by feedback, enabling interaction between the researcher and the expert panel as well as the gradual refinement of opinions (Okoli & Pawlowski, 2004). Yousuf (2007) describes it as a group process involving interaction between the researcher and identified experts, typically conducted through a series of questionnaires. A key determinant of quality is the careful selection of experts with regard to their expertise (Gordon, 2009b; Helmer, 1967; Holcr, 2009, pp. 144–146; Reichel, 2009, p. 137). In addition to specialist knowledge, expert selection should consider formal educational background, scientific or professional qualifications, publication record where relevant, operational or practical experience in the field under investigation, professional reputation, integrity, the ability to critically reflect upon one's own conclusions, the degree of responsibility for presented opinions, and the capacity to perceive the problem within a broader context. The relative importance of these criteria depends on the objectives and disciplinary orientation of the study. In the field of security studies, panel heterogeneity is of particular importance: involving experts

from the military, police, intelligence services, think tanks, and academia may connect strategic, operational, and analytical perspectives while reducing the risk of institutional bias. Experts should possess not only relevant experience, but also the ability to work with sensitive information within established limits, respect the anonymity of the research process, and commit to long-term participation in repeated rounds. In most Delphi studies, anonymity is maintained between participants rather than towards the research team. Consequently, Delphi is more accurately characterised as a form of quasi-anonymity in which researchers know participants' identities for organisational purposes but ensure that individual responses remain anonymous throughout data analysis, feedback, and reporting. This arrangement requires careful management of participant identities, restricted access to identifying information, secure data storage, clearly defined retention periods, and the destruction or anonymisation of identifying records after completion of the study in accordance with applicable ethical and data-protection requirements. Collectively, these criteria enhance the credibility, transparency, and practical relevance of the resulting expert judgements. The design of the panel also includes ensuring relative independence and diversity of information sources in order to minimise the risk of systematic bias and the dissemination of inaccurate conclusions within the consensus process (Šenovský, 2021). Institutional diversity should be considered explicitly during panel composition in order to ensure balanced representation of different organisational perspectives and reduce institutional bias. Potential conflicts of interest should likewise be identified and managed before the study begins, particularly where experts represent organisations that may be affected by the study outcomes. Depending on the subject of the study, participation may also require an appropriate security clearance, while ensuring that classified information is neither requested nor disclosed during the Delphi process. In defence-related Delphi studies, additional security precautions may be necessary because information concerning expert composition, institutional affiliations, or aggregated findings may be of interest to hostile intelligence services. Researchers should therefore minimise unnecessary disclosure of participant identities and avoid collecting or disseminating classified information. Similarly, even aggregated findings should be reviewed before publication, as they may inadvertently reveal critical vulnerabilities, organisational priorities, capability gaps, or sensitive assumptions relevant to national security.

The selection of experts is nevertheless methodologically demanding, and differences in specialisation may influence the resulting consensus. Because self-assessment alone may be affected by overconfidence or underestimation of one's own expertise, it should preferably be complemented by objective indicators such as academic qualifications, publication record, professional position, years of experience, operational responsibilities, or peer nomination (Fischer, 1978; Luo & Wildemuth, 2017). In some Delphi studies, these indicators are incorporated into competence coefficients that combine self-rated expertise with documented evidence of professional knowledge or practical experience (Gordon, 2009b; Jorm, 2025a)D.C.","title":"The Delphi Method","URL":"https://www.millennium-project.org/publications/futures-research-methodology-version-3-0-2/","editor":[{"family":"Glenn","given":"Jerome C."},{"family":"Gordon","given":"Theodore J."}],"author":[{"family":"Gordon","given":"Theodore J."}],"issued":{"date-parts":[["2009"]]}},{"id":7017,"uris":["http://zotero.org/users/14502998/items/MQ2X2NLE"],"itemData":{"id":7017,"type":"chapter","abstract":"Abstract\n This chapter describes the development of the Delphi method by the RAND Corporation in the 1950s, early criticisms of the method, and its subsequent evolution and growth in use. A wide range of variants of the Delphi method have been developed, only some of which aim to establish a consensus. The chapter examines contemporary uses of the method to establish consensus, covering its uses in making judgements on facts where the evidence is imperfect, setting methodological standards, making predictions, defining foundational concepts, determining collective values, improving professional practice, and improving policy.","container-title":"Using the Delphi Method to Establish Expert Consensus","DOI":"10.1007/978-981-96-8357-4_1","ISBN":"978-981-96-8356-7","language":"en","note":"collection-title: Advancing Methods for Interdisciplinarity in the Social Sciences","page":"1-19","publisher":"Springer Nature Singapore","publisher-place":"Singapore","source":"DOI.org (Crossref. Where previous forecasting performance can be evaluated, researchers may additionally calibrate expert judgements by comparing earlier assessments with subsequently observed outcomes. Such calibration may improve interpretation of expert performance, although it is feasible only when suitable historical data are available.

When selecting experts for forecasting studies, previous forecasting performance or documented decision-making experience may also be considered as supplementary indicators of expertise where such information is available.

The panel usually consists of specialists with extensive professional experience, identified on the basis of literature reviews, recommendations, or the snowball method. Rather than following a universally recommended panel size, Delphi studies should determine the number of experts according to the purpose of the study, the diversity of expertise required, the complexity of the problem under investigation, and practical considerations such as participant availability and expected attrition. Although panels comprising approximately 15–35 experts are frequently reported in the literature, both smaller highly specialised panels and substantially larger multidisciplinary panels may be methodologically appropriate depending on the research context. (Fish & Busby, 2005; Holcr, 2009, pp. 147–149). The Delphi method does not seek statistical representativeness, but rather the synthesis of expert opinions (Gordon, 2009b). Because the method requires repeated participation across several rounds, attrition should also be anticipated during study planning. Excessive participant dropout may reduce panel diversity and affect the stability of the emerging consensus.

Following the formation of the panel, the process continues with questionnaire pilot testing and the iterative collection of responses. Depending on the type of data collected, expert judgements are subsequently aggregated using appropriate statistical measures. For ordinal ratings, such as Likert-type scales commonly employed in Delphi studies, the median and interquartile range are generally preferred because they do not require interval-scale assumptions. Means and standard deviations may be appropriate only where interval-level measurement can be reasonably justified. The aggregated responses are then used to assess the degree of consensus and support the interpretation of expert judgements (Disman, 2008, p. 191; Ferjenčík, 2000, p. 231; Gordon, 2009b; Nekolová, 2006a). In the Classical Delphi, the first round frequently consists of open-ended questions designed to elicit a broad range of expert opinions, identify relevant issues, and generate questionnaire items for subsequent rounds (Gordon, 2009b; Linstone & Turoff, 1975). Questionnaires may incorporate both quantitative and qualitative variables: quantitative data may be discrete or continuous, categorical variables nominal or ordinal (requiring coding), and in the case of metric variables, exact measurement should be preferred over questionnaire-based collection wherever possible. This corresponds to different item formats, including category selection for nominal variables, Likert scales or rating scales for ordinal assessment, and direct recording of numerical estimates. Open-ended, closed-ended, semi-closed, scaling, and other types of items are also employed, including control or filter questions and projective techniques (Olecká & Ivanová, 2010). For ordinal rating scales, consensus is commonly evaluated using statistics such as the median and interquartile range, whereas arithmetic means and standard deviations should be interpreted with caution unless interval-scale assumptions are considered appropriate. Responses obtained from open-ended questions are commonly coded into thematic categories before being transformed into structured statements or rating items for subsequent Delphi rounds. In the case of complex issues, the process may be supplemented by a preparatory seminar aimed at unifying terminology and the interpretation of questions. At the same time, the organisational and temporal demands of the method must be taken into account; participation should therefore remain voluntary and based on informed consent.

The core of the method lies in iterative questioning directed towards informed consensus (Al-Qutaish, 2025). After the first round, participants receive anonymous analytical feedback containing summary statistics (e.g. mean, median, variance), which demonstrate the degree of agreement and enable respondents in subsequent rounds to revise their answers, expand their argumentation, and refine their forecasts. This process of controlled feedback constitutes one of the defining characteristics of the Delphi method, allowing experts to reconsider their judgements without direct confrontation while preserving anonymity and limiting the influence of dominant individuals (Gordon, 2009b; Linstone & Turoff, 1975). At the same time, the method protects well-justified minority opinions and limits the dominance of authorities or institutions, representing a major advantage over traditional discussions (Gordon, 2009b; Holcr, 2009, pp. 151–153; Linstone & Turoff, 1975; Nekolová, 2006a). In strategic security studies, preserving well-justified minority opinions may be particularly important because low-probability events may nevertheless have catastrophic consequences (Porel, 2025). The aggregation of responses makes it possible to evaluate consensus and work with extreme

values; for quantitative interpretation, the median is often preferred because it is robust against outliers (Ferjenčík, 2000, p. 231; Nekolová, 2006b). The iterative process continues until predefined stopping criteria are met, such as the achievement of an acceptable level of consensus, stability of responses between successive rounds, or the absence of meaningful changes following additional feedback (Gordon, 2009b; Jorm, 2025a). The outcome typically involves scenario generation: the organisational team synthesises opinions, identifies key risks, time horizons, and impacts, and provides transparent materials for strategic planning and resource allocation (Holcr, 2009, pp. 151–153; Linstone & Turoff, 1975; Reichel, 2009).

The outcome of the Delphi process is the development of security threat scenarios that identify risks, their probability, and their potential impacts, and which serve as a basis for strategic planning and resource allocation (Gordon, 2009b; Linstone & Turoff, 1975; Reichel, 2009). At the same time, the method supports consensus-building and the transparent documentation of arguments, although it may encounter organisational or motivational barriers, which has led to the development of various modifications, such as anonymous online discussions supporting expert creativity (Reichel, 2009, p. 148; Robson, 1995, pp. 77–78; Smolík, 2011). At present, both the traditional paper-and-pencil form and modern real-time Delphi variants employing computer-based systems are used, accelerating analysis and enabling more effective prediction of dynamic security threats (Gordon, 2009b; Linstone & Turoff, 1975).

5. Application in the Assessment of Security Threats

The Delphi method continues to prove exceptionally suitable for the assessment of military and security threats, particularly in situations where future developments are unpredictable and precise empirical data are unavailable (cf. Buřita, 2003). Contemporary applications of Delphi extend beyond conventional military forecasting to emerging domains such as border-security risk assessment (Plamadeala, 2025), climate-security and critical infrastructure protection (Mančić, 2025), nuclear policy and strategic deterrence (Porel, 2025), AI-enabled cyber risk management (Beriša, Cvetković, & Pavić, 2024), and multidimensional security assessment combining empirical and institutional indicators (Cvetković et al., 2025).

The method enables the synthesis of the knowledge and experience of groups of security experts and supports three closely related activities. First, it facilitates **threat identification** by recognising potential sources of harm and emerging security challenges. Second, it contributes to **risk assessment** by evaluating the likelihood and potential consequences of identified threats, thereby supporting prioritisation and decision-making. Finally, it enables the development of scenarios reflecting alternative trajectories of future threat development.

The first area – threat identification – is used to map potentially dangerous events, situations, and trends that could threaten the defence capacity of the state or allied structures (e.g. Olivero, Bertolino, Dominguez-Mayo, Matteucci, & Escalona, 2022). This approach is particularly invaluable when assessing threats for which hard data are lacking, such as new forms of asymmetric attacks or cyber incidents. Emerging AI-enabled threats are characterised by rapid technological development and limited historical evidence, making structured expert judgement an appropriate complement to technology-based analytical approaches (Beriša et al., 2024). Data-driven methods, including decision-tree models, may complement Delphi studies by providing empirical estimates of risk indicators, while expert panels contribute contextual interpretation, prioritisation, and scenario construction where historical data remain limited (Plamadeala, 2025). Whereas predictive statistical models identify significant explanatory variables from empirical datasets, Delphi studies are particularly suitable where emerging threats have not yet produced sufficient empirical observations for robust statistical modelling (Cvetković et al., 2025).

The second area – risk prioritisation (e.g. Markmann, Darkow, & Von Der Gracht, 2013) – evaluates the likelihood and potential consequences of identified threats in order to distinguish critical risks requiring immediate attention and resource allocation from those of lesser significance, thereby supporting more effective strategic planning and resource management. Consensus is common-

ly evaluated using statistical measures such as the median, interquartile range (IQR), percentage agreement, Kendall's coefficient of concordance (Kendall's W), or by assessing the stability of responses across successive rounds. The choice of indicator depends on the measurement scale and study design. Although consensus strengthens the credibility of expert judgements, it should not be interpreted as proof of objective correctness, particularly when assessing highly uncertain or unprecedented security threats. The third area involves the prediction of impacts and trends, including the construction of scenarios based on expert assessments (Önnered, Johansson, Stefan, & Fundin, 2025). Scenarios generated in this way provide decision-making bodies with relevant information concerning the probability and potential impact of individual threats, thereby supporting strategic planning, force and resource allocation, and crisis preparedness.

The outcomes obtained through the Delphi method can be directly integrated into strategic decision-making and planning. Expert panel assessments make it possible to combine qualified estimates with the practical implementation of defence strategies, thereby supporting the development of flexible scenarios and effective decision-making under conditions of uncertainty. The potential applications of the method in other areas related to security and planning are surprisingly broad. These include, for example, the collection and evaluation of current and historical data, the assessment of the significance of historical events, the determination of budget allocation priorities, and the evaluation of regional and urban planning alternatives. The method can also be employed in the design of university campuses, the development of curricula, the construction of model structures, the analysis of the advantages and disadvantages of political decisions, the mapping of causal relationships in complex economic and social phenomena, the identification of individual motivations, and the evaluation of priorities in both personal and social goals (Perveen, Kamruzzaman, & Yigitcanlar, 2017; Preble, 1983; Sitlington & Coetzer, 2015).

In practice, modified Delphi studies are being used with increasing frequency, for example with a smaller number of rounds supplemented by qualitative interviews or online questionnaires (Clyne et al., 2024; Fish & Busby, 2005; Khodyakov et al., 2020, 2023). This approach enables faster data collection and evaluation and is particularly useful for predicting future developments or assessing emerging practical issues, such as security threats, crisis management, or cybersecurity. The combination of a shortened Delphi survey with qualitative methods may facilitate the effective involvement of personnel from the General Staff of the Armed Forces of the Czech Republic, military headquarters, or specialised units in the process of expert assessment without placing a disproportionate burden on their routine operational duties. This approach may prove particularly valuable in evaluating the future development of military capabilities, identifying emerging threats, planning defence measures, and supporting decision-making processes at both the strategic and operational levels of command.

To illustrate the practical application of the Delphi method in security research, the following hypothetical illustrative example presents a Delphi study designed to assess emerging cyber threats targeting hospital critical infrastructure. This example was deliberately selected because cyberattacks against critical infrastructure represent one of the most prominent contemporary security challenges, characterised by high uncertainty, rapidly evolving threat dynamics, and limited availability of empirical data, thereby making structured expert judgement particularly valuable. Furthermore, the protection of healthcare infrastructure has gained increasing strategic importance following recent cyber incidents and the growing recognition of health systems as elements of national critical infrastructure. The example demonstrates the complete methodological sequence of a Delphi study, from the design of the study protocol and expert elicitation process to the synthesis of the final results into a threat assessment matrix. The specific application presented is purely illustrative; in practice, Delphi studies should always be adapted to the objectives, available expertise, and specific characteristics of the security problem under investigation (Table 2).

Table 2. Illustrative Delphi Study Protocol for Assessing Emerging Cyber Threats Targeting Hospital Critical Infrastructure

Component	Illustrative specification
Research objective	Identify, prioritise, and assess emerging cyber threats that are expected to affect hospital critical infrastructure over the next ten years, and formulate recommendations to strengthen preparedness and organisational resilience.
Expert panel	22 experts representing complementary domains: cybersecurity specialists (6), hospital IT and clinical systems managers (5), healthcare administrators (3), intelligence analysts (3), AI and digital security researchers (2), emergency management specialists (3). Participants should have at least five years of professional experience and no direct reporting relationship to ensure independence of judgement.
Round 1	Anonymous open-ended questionnaire designed to identify emerging threats, vulnerable assets, technological and organisational drivers, possible consequences, and early warning indicators. Responses are qualitatively coded and merged into a consolidated list of threats for subsequent rounds.
Illustrative Round 1 questions	1. Which cyber threats are most likely to affect hospitals within the next decade? 2. Which hospital systems or services are expected to become the most vulnerable? 3. Which technological developments (e.g., AI, Internet of Medical Things, cloud services) are likely to create new attack opportunities? 4. Which organisational factors may increase cyber risk? 5. Which indicators could provide early warning of an emerging cyber threat?
Round 2	Experts independently evaluate each identified threat using structured rating scales. They may provide optional justification for exceptionally high or low ratings.
Rating scales	Likelihood (1 = very unlikely; 5 = very likely); Potential impact (1 = negligible; 5 = catastrophic); Confidence in judgement (1 = very low; 5 = very high).
Controlled feedback	Before Round 3, participants receive an anonymous summary including group medians, interquartile ranges, distribution of responses, and selected anonymised comments explaining divergent opinions. Experts are invited to reconsider their previous ratings but are not required to change them.
Round 3	Experts review the controlled feedback and submit revised ratings where considered appropriate. Remaining disagreements are documented rather than eliminated.
Consensus criteria	Consensus is considered achieved when the median rating is ≥ 4, the interquartile range is ≤ 1, and Kendall's coefficient of concordance (W) is ≥ 0.70. Threats not meeting these criteria may be discussed in an additional Delphi round or reported as areas of continuing uncertainty.
Participant attrition	Participation rates are monitored after each round. Experts who fail to complete a rating round are excluded from subsequent statistical analyses, while reasons for withdrawal are documented to assess potential attrition bias.
Expected outputs	Ranked list of emerging cyber threats, assessment of expert consensus and uncertainty, threat assessment matrix, future threat scenarios, early warning indicators, and strategic recommendations for improving cyber resilience in healthcare organisations.

Following completion of the hypothetical Delphi study outlined in Table 2, the synthesised expert judgements may be presented in the form of a threat assessment matrix. Rather than serving as a direct output of the Delphi process itself, the matrix represents a structured synthesis of the expert consensus and provides a practical decision-support tool for security planning. By integrating assessments of the likelihood, potential impact, confidence, uncertainty, anticipated time horizon, early warning indicators, and recommended response measures for each identified threat, the matrix enables decision-makers to compare emerging threats systematically and to prioritise preparedness and resilience measures. Such matrices may support strategic planning, capability development, re-

source allocation, and the identification of areas requiring further monitoring or expert reassessment as the threat environment evolves. The resulting illustrative threat assessment matrix is based on the hypothetical Delphi study described above. The matrix is included to bridge the gap between the methodological discussion presented in this paper and its practical application in security research. By providing a fully hypothetical example, it illustrates how expert judgements generated through a Delphi study may be synthesised into a structured threat assessment that can support strategic analysis and decision-making. The example is purely illustrative and does not represent the findings of an empirical investigation (Table 3).

Table 3. Illustrative Threat Assessment Matrix for Emerging Cyber Threats Targeting Hospital Critical Infrastructure

Threat description	Time horizon	Probability	Impact	Confidence	Uncertainty	Warning indicators	Recommended response
Increasing use of AI-assisted ransomware capable of adapting attacks to hospital information systems and disrupting clinical operations.	1–3 years	High	Very high	High	Low	Growing number of AI-enhanced ransomware campaigns targeting healthcare organisations; increasing sophistication of autonomous malware.	Strengthen cyber resilience through network segmentation, offline backups, AI-assisted detection and incident response capabilities.
Expansion of vulnerable Internet of Medical Things (IoMT) ecosystems creating new attack surfaces across connected medical devices.	3–6 years	Medium	Very high	Medium	Medium	Rapid deployment of network-connected medical devices without corresponding security improvements; increasing disclosure of critical vulnerabilities.	Introduce secure lifecycle management for medical devices, continuous vulnerability assessment and network segmentation.
Increasing dependence on AI-supported clinical decision systems creating opportunities for manipulation of diagnostic or treatment recommendations.	4–7 years	Medium	High	Medium	High	Widespread adoption of clinical AI applications combined with growing reports of attacks against AI models and healthcare data integrity.	Establish governance for trustworthy AI, continuous validation of AI outputs and secure AI model management.
Growing dependence on third-party software suppliers and cloud services increasing the risk of supply-chain compromise affecting multiple hospitals simultaneously.	2–5 years	High	High	High	Medium	Increasing number of software supply-chain attacks affecting healthcare providers and technology vendors.	Strengthen supplier assurance, third-party security audits and software integrity verification.

Convergence of cyberattacks with broader hybrid campaigns aimed at disrupting healthcare delivery during major crises or armed conflict.	5–10 years	Medium	Very high	Medium	High	Escalation of geopolitical tensions accompanied by coordinated attacks on healthcare infrastructure and public services.	Integrate cyber preparedness into national emergency planning and conduct cross-sector resilience exercises.

6. Advantages and Limitations of the Method

In the field of security threat assessment, the Delphi method represents an effective tool for the synthesis of expert knowledge and the support of decision-making, particularly in environments where reliable data are unavailable or, conversely, where the volume of data is too extensive to be processed effectively through traditional methods (Šenovský, 2021). The method provides a structured framework for comparing and synthesising diverse expert judgements through iterative anonymous feedback, enabling both areas of agreement and well-founded differences of opinion to be identified and interpreted. This is particularly valuable in defence and security research, where justified minority views may represent important early warnings or alternative strategic perspectives. The military context, characterised by the high dynamism and uncertainty of threats such as cyberattacks, hybrid operations, or asymmetric threats, is therefore particularly well suited to the application of the Delphi method.

At the same time, when considering the use of the Delphi method, it is necessary to bear in mind its specific limitations and organisational demands. The method is not intended for precise quantitative analysis, but rather for collective expert judgement and the synthesis of experience. Its results are fundamentally dependent on the quality and motivation of the experts involved in the panel. Consequently, the outputs of the method always reflect the character and quality of expert opinions rather than objective empirical data. This means that the Delphi method is particularly strong in situations where data are absent or incomplete, but less suitable where robust quantitative models are available — for example, in the precise estimation of probabilities or exact numerical forecasting.

Panel composition should be guided primarily by the objectives and complexity of the study, ensuring appropriate representation of the relevant expert domains and institutional perspectives. Rather than adhering to a predefined number of participants, Delphi studies seek to achieve an appropriate balance between diversity of expertise, feasibility, and the quality of expert judgement. If the experts are overly homogeneous, or conversely too divergent in their areas of specialisation, the resulting consensus may become distorted or difficult to achieve. Moreover, there is no universally accepted objective method for selecting panellists or defining who qualifies as an "expert", which may lead to selection bias if the criteria for inclusion are not sufficiently transparent and justified. The appropriate selection of specialists, their experience, their capacity to evaluate available information objectively, and their willingness to cooperate all fundamentally influence the reliability of the resulting predictions. The Delphi method is specifically designed to reduce the risk of groupthink by ensuring anonymous participation during the initial rounds, thereby limiting conformity pressures, authority effects, and the dominance of influential individuals (Hayes, 2022). Controlled feedback further encourages participants to reconsider their judgements in light of the anonymised views of the panel while preserving the independence of individual assessments. Nevertheless, neither anonymity nor controlled feedback completely eliminates cognitive or institutional biases, and excessive convergence towards the emerging group opinion may still occur if minority views are insufficiently explored or documented.

In defence and national security applications, however, anonymity must be carefully balanced against confidentiality requirements. While anonymous participation reduces the influence of authority, organisational hierarchy, and institutional pressure, security-related Delphi studies frequently involve experts with access to classified or otherwise sensitive information that cannot be

fully disclosed within the research process. Consequently, questionnaires and feedback procedures often need to be designed in a way that allows experts to express informed judgements without revealing classified sources, operational details, or intelligence capabilities.

Security and defence applications also face additional methodological challenges arising from strategic and institutional influences on expert judgement. Experts may be affected by cognitive biases, organisational culture, or institutional priorities that shape their perception of threats and acceptable response options. Moreover, deliberate strategic deception and disinformation—whether originating from adversarial actors or reflected in incomplete situational awareness—may further complicate expert assessments. For this reason, particular attention should be paid not only to achieving consensus but also to documenting persistent minority opinions, as these may represent alternative scenarios or early warnings that are overlooked by the majority yet subsequently prove to be strategically significant.

Among the principal advantages of the method is its capacity to systematically obtain information concerning future trends, estimate priorities and potential impacts, and synthesise different expert perspectives and experiences. The method also makes it possible to identify potential disagreements among experts and clarify the reasons underlying them, thereby supporting a deeper understanding of complex security situations. In the context of military decision-making, this means not only the identification and prioritisation of threats, but also the development of scenarios that may be used for crisis planning, force and resource allocation, or strategy formulation. Development of plausible scenarios informed by synthesised expert judgements; expert consensus serves as one input to scenario construction but does not itself constitute a scenario.

On the other hand, certain limitations of the method must also be taken into account. (adapted from Nasa, Jain, & Juneja, 2021; Smolík, 2011; Williamson, 2002; Rowe & Wright, 1999). The reliability of the results depends to a considerable extent on the composition of the panel, the formulation of questions, and the number of iterations. An unsuitable combination of these factors may lead to biased responses, insufficient consideration of expert consensus, or distortion of the results. The evaluation of responses, particularly open-ended and elaborated answers, is highly demanding and requires careful methodological preparation.

A major weakness of the Delphi method lies in its time-consuming and organisationally demanding nature. Frequent group meetings are inefficient in terms of both time and cost, while potential disagreements or politically sensitive conflicts among participants require anonymity and a structured communication process to ensure that no relevant opinion is overlooked (Linstone & Turoff, 1975). In practice, it may take several weeks or even months to achieve a sufficient degree of consensus or response stabilisation, which may prove problematic in rapidly changing security environments where swift decision-making is required. A single round usually lasts approximately three weeks, while a three-round process, including preparation, analysis, and the production of the final report, generally requires between three and six months. Financial demands may likewise be substantial, particularly when the panel is large or involves international expertise.

Another challenge arises from expert judgements that are insufficiently substantiated or influenced by cognitive, institutional, or strategic biases, as these may affect the quality of the collective assessment. However, strongly divergent opinions should not be dismissed solely because they differ from the majority view, as they may identify low-probability but high-impact threats or alternative interpretations that warrant further consideration. Moreover, the Delphi method often does not allow direct interaction between experts, since it is conducted anonymously and primarily through written communication. Although anonymity reduces group pressure and the dominance of individuals, it simultaneously prevents spontaneous exchanges of views, the immediate clarification of ambiguities, and debates that may lead to a deeper understanding of complex issues. This may limit the panel's capacity to develop more refined or multidimensional arguments, which is particularly significant in the assessment of multifactorial security phenomena.

The very definition and quantification of consensus may also be subjective and dependent upon selected threshold values or statistical criteria. Consensus does not necessarily reflect a true or objectively correct conclusion, but rather an agreed compromise among expert opinions, which must

be taken into account when interpreting the results, particularly in the context of strategic decision-making related to national security (Jorm, 2025b). At the same time, it is important to emphasise that the aim of the method is not always to achieve complete consensus. Contemporary approaches to the Delphi method focus more on the synthesis of perspectives, which may reflect both areas of agreement and the crystallisation of divergent viewpoints together with their underlying arguments (Nekolová, 2006a).

A further risk involves participant attrition, namely panellists who withdraw during the iterative process for various reasons. This may weaken the representativeness of the panel and consequently reduce the quality of the results. In longer or more demanding Delphi studies, participant motivation may decline, as may the quality of responses in subsequent rounds, again diminishing the reliability of the achieved consensus. A summary of the advantages and limitations of the Delphi method is presented in the corresponding table (Table 4).

Table 4. Advantages and Limitations of the Delphi Method. Source: authors, based on the cited literature.

	Advantage / Limitation	Description	Example of a Global Security Threat
Advantage	**Synthesis of structured expert judgement**	Integrates diverse specialist knowledge into a structured assessment of complex security issues under conditions of uncertainty.	Assessment of emerging cyber threats targeting critical infrastructure.
	Structured examination of divergent expert judgements	Anonymous, iterative feedback enables experts to reconsider their assessments while preserving justified minority opinions and systematically examining divergent viewpoints.	Evaluation of alternative assessments of hybrid threats and disinformation campaigns.
	Support for structured expert consultation	Facilitates systematic comparison of expert perspectives and, where appropriate, the identification of areas of agreement or persistent disagreement.	Prioritisation of military and civilian preparedness measures during complex crises.
	Assessment of emerging trends and uncertainties	Supports the identification of plausible future developments and weak signals where empirical evidence is incomplete or rapidly evolving.	Assessment of future pandemic risks and their geopolitical implications.
	Support for scenario development	Provides structured expert input that can subsequently be integrated into scenario planning and strategic analysis.	Climate-security interactions and migration-related security challenges.
	Flexibility of application	Applicable across diverse security problems characterised by uncertainty, limited evidence, or complex multidisciplinary knowledge.	Assessment of future defence capabilities and emerging technologies.
Limitation	**Dependence on expert selection**	The quality of expert judgements depends on the expertise, diversity, independence, and motivation of the selected panel.	Limited representation of cybersecurity expertise may influence the assessment of cyber threats.
	Questionnaire design	Poorly formulated questions may bias responses, constrain expert reasoning, or introduce ambiguity into subsequent rounds.	Ambiguous questions concerning climate-security risks may result in inconsistent expert assessments.
	Time-consuming iterative process	Multiple questionnaire rounds, controlled feedback, and response analysis require substantial time and organisational effort.	Strategic assessment of long-term migration and security trends.

Limitation	**Susceptibility to cognitive and institutional bias**	Expert judgements may be influenced by cognitive biases, organisational priorities, institutional culture, or strategic interests despite the use of anonymity.	Assessment of defence priorities influenced by organisational or national interests.
	Conditional nature of expert assessments	Delphi findings represent structured expert judgements rather than objectively verified predictions and should be interpreted together with explicit uncertainty and, where possible, validated using complementary evidence.	Long-term assessment of hybrid threats and emerging military technologies.
	Organisational and resource demands	Coordination of expert panels, secure communication, feedback preparation, qualitative analysis, and participant retention require considerable organisational resources.	International assessment of cyber resilience and critical infrastructure protection.

The military and security context particularly benefits from these characteristics of the Delphi method because they enable analysis and planning in environments characterised by high uncertainty and complex interactions. It is evident that this process involves an excessive number of unknown variables, which are themselves interconnected through complex relationships that are difficult to capture analytically (Parízek & Ditrych, 2019). The principal contribution of the method lies in the objective and structured processing of expert opinions, its capacity to identify key threats, estimate their impacts, and develop predictive scenarios that support strategic decision-making. At the same time, the limitations of the method must be carefully acknowledged and compensated for through the careful selection of the panel, precise formulation of questions, appropriate determination of the number of iterations, and expert evaluation of the results in order to ensure the validity and practical applicability of the conclusions within the context of military planning.

In defence and security research, particular attention should therefore be devoted to balancing expert anonymity with information security requirements, minimising cognitive and institutional biases, and ensuring that well-argued minority opinions are systematically documented rather than suppressed in pursuit of consensus.

7. Recommendations for Effective Use in the Defence Environment

The Delphi method may be employed in the military sphere for forecasting the nature of future conflicts and operations, as well as the possible development and deployment of armed forces. For example, researchers at the University of Defence in the Czech Republic have long engaged with this issue and argue that the future operational environment will become increasingly complex and multidimensional (Galatík, 2008). For this reason, it is important to seek methods capable of improving understanding and prediction of these complex processes, including command and control, operational management, and risk assessment. This naturally also applies to methods designed to support such understanding, including the effective application of the Delphi method.

The effective application of the Delphi method in the defence environment requires careful planning of the entire process, from the selection of experts to the evaluation of results. Where required, ethical approval and institutional authorisation should be obtained before data collection begins, particularly when experts represent governmental, military, intelligence, or other security organisations. A key prerequisite is the careful selection of members of the expert panel, who must possess not only specialist knowledge of the security issues under examination, but also the capacity to critically analyse complex scenarios and cooperate within an anonymised collective process. The selection of experts should reflect diversity of professional background, practical experience, and knowledge of related disciplines, enabling the panel to address a broad spectrum of military and security threats, ranging from traditional military risks to emerging phenomena such as cyberattacks, hybrid threats, and climate- or migration-related crises.

The proper formulation of questions represents another essential factor in successful implementation. Consensus criteria, stopping rules, and the statistical measures used to evaluate agreement should be defined before the first Delphi round to ensure methodological transparency and consistency. Questions must be clear, unambiguous, and supplemented with examples derived from real-world contexts in order to enable experts to assess the probability, impacts, and time horizon of various security threat scenarios. The quality of responses may be further enhanced through supporting materials, such as analytical studies, statistical data, or maps, as well as through the organisation of short seminars or briefings that ensure a shared understanding of selected definitions and the broader context of the problem. These procedures are particularly important when evaluating phenomena characterised by a high degree of uncertainty, such as unexpected cyberattacks, the escalation of hybrid operations, or dynamic changes in the security situation within politically unstable regions.

The selection of an appropriate form of data collection is equally critical. When sensitive security topics are examined, data collection should be conducted through secure communication platforms with appropriate access controls, encrypted data transmission where necessary, and procedures ensuring controlled anonymous feedback throughout successive Delphi rounds. The Delphi method may be implemented in paper-based form, electronically through specialised platforms, or through a combination of personal consultations and online questionnaires. Electronic formats enable the rapid compilation of responses and iterative real-time data processing, which is particularly advantageous when assessing rapidly evolving threats, such as cyber incidents or the spread of infectious diseases with security implications. Researchers should also anticipate participant attrition across successive rounds, monitor response rates, document reasons for withdrawal where available, and assess the possible implications of attrition for the interpretation of the findings.

To increase the validity and reliability of results, it is recommended that the Delphi method be combined with other analytical tools and scenario-planning techniques. To strengthen the credibility of the findings, Delphi results should, where possible, be validated against empirical evidence and combined with complementary analytical approaches, including incident databases, intelligence assessments, simulations, horizon scanning, structured analytical techniques, quantitative risk models, and scenario-planning methods. Such an approach makes it possible to connect qualified expert estimates with impact modelling, the testing of alternative scenarios, and the assessment of risks associated with individual strategies. Security planning thereby gains not only a synthesis of expert knowledge, but also a practical framework for decision-making that reflects the uncertainty, complexity, and interconnected nature of global security threats.

Overall, the successful use of the Delphi method in the defence environment is based on the harmonious combination of a high-quality expert panel, precise questionnaire preparation, supporting materials, appropriate data collection procedures, and the integration of results into a broader strategic framework. Such a structured approach makes it possible not only to identify and prioritise key threats, but also to support decision-making and scenario-building processes that reflect the complex character of the contemporary and future security environment. Final reports should communicate not only areas of expert consensus but also remaining uncertainty, confidence in expert judgements, and well-founded minority opinions, particularly where these concern low-probability but high-consequence security threats.

Selected international studies employ the Delphi method for forecasting in the fields of technological development and strategic defence decision-making. Defence technologies represent a key area of technological forecasting, as states and organisations seek to maintain long-term technological competitiveness in the domain of national security. In this context, the Delphi method serves as a tool for the systematic collection of expert estimates, enabling the identification of developmental trends and stages of technological advancement within the defence sector. The Delphi method is also used as part of broader analytical frameworks for defence policy.

Future Delphi studies in defence should increasingly integrate AI-supported analytical tools, cyber-risk intelligence, and expert judgement into unified decision-support frameworks (Beriša et al., 2024).

8. Conclusion

The quality and usefulness of Delphi-based assessments depend on the design of the study, including the selection of experts, the formulation of questions, the feedback process, and the criteria used to evaluate consensus. As illustrated by its long-standing application in security forecasting, the Delphi method represents a valuable approach for supporting the assessment of complex and uncertain security problems through the structured elicitation and synthesis of expert judgement. Rather than producing definitive predictions, the method provides informed, conditional assessments that can support strategic thinking, scenario development, and preparedness planning in areas where empirical evidence is limited, incomplete, or rapidly evolving. This is particularly relevant for contemporary security challenges such as cyber threats, hybrid operations, pandemics, migration, and climate change.

The future application of the Delphi method in defence and security research offers considerable potential, particularly when combined with complementary analytical approaches, scenario-planning techniques, quantitative models, and continuously updated intelligence or empirical data. Further methodological development may focus on improving expert elicitation techniques, supporting iterative processes through digital technologies, and integrating real-time information into expert assessments. However, Delphi findings should be interpreted as structured expert judgements rather than objective forecasts and, whenever possible, should be validated against empirical evidence, operational experience, or alternative analytical methods. Used in this way, the Delphi method remains a flexible and valuable tool for supporting decision-making under conditions of uncertainty while recognising the inherent limitations of expert-based assessment.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no competing interests.

Funding: The authors received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions: Conceptualization: I.O.; Methodology: J.S., I.O.; Investigation: J.S., I.O.; Formal analysis: I.O.; Validation: I.O.; Writing – original draft: J.S., I.O.; Writing – review & editing: J.S., I.O.; Visualization: I.O.; Supervision: J.S. All authors have read and approved the final version of the manuscript.

Declaration of Generative AI and AI-Assisted Technologies: During the preparation of this manuscript, the authors used ChatGPT (OpenAI) and DeepL solely for language editing, translation support, and improving the clarity and readability of the text. These tools were not used to generate scientific content, data, analyses, interpretations, or references. The authors critically reviewed and edited all AI-generated output and accept full responsibility for the content of the final manuscript.

9. References

1. Al-Qutaish, R. E. (2025). Delphi Method: A Comprehensive Literature Review. *International Journal of Software Engineering*, *12*(1), 1–15.
2. Beriša, H., Cvetković, V., & Pavić, A. (2024). Implications of Artificial Intelligence and Cyberspace on Risk Management Capabilities. *International Journal of Disaster Risk Management*, *6*(2), 279–295. https://doi.org/10.18485/ijdrm.2024.6.2.18
3. Buckley, C. (1995). Delphi: A methodology for preferences more than predictions. *Library Management*, *16*(7), 16–19. https://doi.org/10.1108/01435129510093737
4. Buřita, L. (2003). Prognostické metody a jejich využití v resortu MO. *Obrana a strategie*, 3(1), 47–60.

5. Clyne, B., Sharp, M. K., O' Neill, M., Pollock, D., Lynch, R., Amog, K., … Tricco, A. C. (2024). An international modified Delphi process supported updating the web-based 'right review' tool. *Journal of Clinical Epidemiology*, *170*, 111333. https://doi.org/10.1016/j.jclinepi.2024.111333
6. Cvetković, V. M., Lipovac, M., Renner, R., Stanarević, S., & Raonić, Z. (2025). A Predictive Framework for Understanding Multidimensional Security Perceptions Among Students in Serbia: The Role of Institutional, Socio-Economic, and Demographic Determinants of Sustainability. *Sustainability*, *17*(11), 5030. https://doi.org/10.3390/su17115030
7. Danics, Š., Smolík, J., & Strnad, Š. (2024). *Aspekty bezpečnostní politiky* (1st ed.). Praha: Policejní akademie České republiky v Praze.
8. Disman, M. (2008). *Jak se vyrábí sociologická znalost: Příručka pro uživatele*. Praha: Karolinum.
9. Ferjenčík, J. (2000). Úvod do metodologie psychologického výzkumu: Jak zkoumat lidskou duši. Praha: Portál.
10. Fischer, R. G. (1978). The Delphi method: A description, review and criticism. *Journal of Academic Librarianship*, *4*(2), 64–70.
11. Fish, L. S., & Busby, D. M. (2005). The Delphi technique. In D. H. Sprenkle & F. P. Piercy (Eds.), *Research methods in family therapy* (2nd ed., pp. 238–253). New York, NY: Guilford Press.
12. Galatík, V. (Ed.). (2008). *Principy obrany České republiky "2030"*. Brno: Univerzita obrany.
13. Gordon, T. J. (2009a). Real-time Delphi. In J. C. Glenn & T. J. Gordon (Eds.), *Futures research methodology* (Version 3.0). Washington, DC: The Millennium Project. Retrieved from https://www.millennium-project.org/publications/futures-research-methodology-version-3-0-2/
14. Gordon, T. J. (2009b). The Delphi method. In J. C. Glenn & T. J. Gordon (Eds.), *Futures research methodology* (Version 3.0). Washington, DC: The Millennium Project. Retrieved from https://www.millennium-project.org/publications/futures-research-methodology-version-3-0-2/
15. Hayes, N. (2022). *Základy sociální psychologie* (8th ed.; I. Štěpaníková, Trans.). Praha: Portál.
16. Helmer, O. (1967). *Analysis of the future: The Delphi method*. Retrieved from https://www.rand.org/content/dam/rand/pubs/papers/2008/P3558.pdf
17. Hendl, J., & Remr, J. (2017). *Metody výzkumu a evaluace* (1st ed.). Praha: Portál.
18. Holcr, K. (2009). *Kriminologie*. Praha: Leges.
19. Jorm, A. (2025a). Origins and uses of the Delphi method. In A. Jorm, *Using the Delphi method to establish expert consensus* (pp. 1–19). Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-96-8357-4_1
20. Jorm, A. (2025b). *Using the Delphi method to establish expert consensus: A practical guide*. Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-96-8357-4
21. Khodyakov, D., Grant, S., Denger, B., Martin, A., Peay, H., & Coulter, I. (2020). Practical Considerations in Using Online Modified-Delphi Approaches to Engage Patients and Other Stakeholders in Clinical Practice Guideline Development. *The Patient - Patient-Centered Outcomes Research*, *13*(1), 11–21. https://doi.org/10.1007/s40271-019-00389-4
22. Khodyakov, D., Grant, S., Kroger, J., Gadwah-Meaden, C., Motala, A., & Larkin, J. (2023). Disciplinary trends in the use of the Delphi method: A bibliometric analysis. *PLOS ONE*, *18*(8), e0289009. https://doi.org/10.1371/journal.pone.0289009
23. Linstone, H. A., & Turoff, M. (Eds.). (1975). *The Delphi method: Techniques and applications*. Reading, Mass: Addison-Wesley Pub. Co., Advanced Book Program.
24. Luo, L., & Wildemuth, B. M. (2017). Delphi Studies. In B. M. Wildemuth, *Applications of social research methods to questions in information and library science* (2nd ed., pp. 81–90). Santa Barbara, California: Libraries Unlimited, an imprint of ABC-CLIO, LLC.

25. Mančić, T. (2025). Climate Change as a Security Challenge, Risk and Threat of the 21st Century and Its Consequences on Critical Infrastructure. *International Journal of Contemporary Security Studies*, *1*(1), 191-204. https://doi.org/10.18485/fb_ijcss.2025.1.1.14

26. Manski, C. F. (2007). *Identification for prediction and decision*. Cambridge, Mass: Harvard University Press.

27. Mareš, M. (2014). Vybrané predikce terorismu. In R. Svatoš & J. Kříha (Eds.), *II. kriminologické dny* (pp. 125–133). České Budějovice: Česká kriminologická společnost & Vysoká škola evropských a regionálních studií.

28. Markmann, C., Darkow, I.-L., & Von Der Gracht, H. (2013). A Delphi-based risk analysis—Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment. *Technological Forecasting and Social Change*, *80*(9), 1815–1833. https://doi.org/10.1016/j.techfore.2012.10.019

29. Nasa, P., Jain, R., & Juneja, D. (2021). Delphi methodology in healthcare research: How to decide its appropriateness. *World Journal of Methodology*, *11*(4), 116–129. https://doi.org/10.5662/wjm.v11.i4.116

30. Nekolová, M. (2006a). Metoda Delphi. In M. Potůček (Ed.), *Manuál prognostických metod* (1st ed., pp. 180–186). Praha: Slon.

31. Nekolová, M. (2006b). Participativní metody. In M. Potůček (Ed.), *Manuál prognostických metod* (1st ed., pp. 28–44). Praha: Slon.

32. Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, *42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

33. Olecká, I., & Ivanová, K. (2010). *Metodologie vědecko-výzkumné činnosti* (1st ed.). Olomouc: Moravská vysoká škola Olomouc. Retrieved from https://is.muni.cz/el/phil/podzim2015/MVK_23/um/54991882/Metodologie_vedecko-vyzkumne_cinnosti.pdf

34. Olivero, M. A., Bertolino, A., Dominguez-Mayo, F. J., Matteucci, I., & Escalona, M. J. (2022). A Delphi study to recognize and assess systems of systems vulnerabilities. *Information and Software Technology*, *146*, 106874. https://doi.org/10.1016/j.infsof.2022.106874

35. Önnered, S., Johansson, P. E., Stefan, I., & Fundin, A. (2025). Emerging threats to energy security—A Delphi study. *Energy Policy*, *206*, 114735. https://doi.org/10.1016/j.enpol.2025.114735

36. Parízek, M., & Ditrych, O. (2019). Předpovědní metody. In V. Beneš & P. Drulák (Eds.), *Metodologie výzkumu politiky* (pp. 229–254). Praha: Sociologické nakladatelství (SLON).

37. Perveen, S., Kamruzzaman, Md., & Yigitcanlar, T. (2017). Developing Policy Scenarios for Sustainable Urban Growth Management: A Delphi Approach. *Sustainability*, *9*(10), 1787. https://doi.org/10.3390/su9101787

38. Plămădeală, C. (2025). From Operational Experience to Predictive Models: A Decision Tree Approach to Traveler Risk Assessment at Border Crossing Points. *International Journal of Contemporary Security Studies*, *1*(2), 119-136. https://doi.org/10.18485/fb_ijcss.2025.1.2.8

39. Plamínek, J. (2008). *Vedení lidí, týmů a firem: Praktický atlas managementu* (3., aktualiz. a rozš. vyd). Praha: Grada.

40. Porel, T. (2025). A Nuclear Policy Framework: Identifying Challenges and Ways to Solutions. *International Journal of Contemporary Security Studies*, *1*(2), 9-24. https://doi.org/10.18485/fb_ijcss.2025.1.2.2

41. Preble, J. F. (1983). Public sector use of the Delphi technique. *Technological Forecasting and Social Change*, *23*(1), 75–88. https://doi.org/10.1016/0040-1625(83)90072-0

42. Redmiles, E. M., Acar, Y., Fahl, S., & Mazurek, M. L. (2017). *A summary of survey methodology best practices for security and privacy researchers*. College Park, MD: University of Maryland, Department of Computer Science. https://doi.org/10.13016/M22K2W
43. Reichel, J. (2009). *Kapitoly metodologie sociálních výzkumů*. Praha: Grada Publishing.
44. Robson, M. (1995). *Skupinové řešení problémů* (1st ed.). Praha: Victoria Publishing.
45. Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting*, *15*(4), 353–375. https://doi.org/10.1016/S0169-2070(99)00018-7
46. Sablatzky, T. (2022). The delphi method. *Hypothesis: Research Journal for Health Information Professionals*, *34*(1). https://doi.org/10.18060/26224
47. Šenovský, P. (2021). *Modelování rozhodovacích procesů* (5th ed.). Ostrava: VŠB – Technical University of Ostrava. Retrieved from https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/modelovani_5vyd.pdf
48. Sitlington, H., & Coetzer, A. (2015). Using the Delphi technique to support curriculum development. *Education + Training*, *57*(3), 306–321. https://doi.org/10.1108/ET-02-2014-0010
49. Smolík, J. (2011). *Využití delfské metody ve zpravodajské činnosti: Popis, aplikace, silné a slabé stránky metody*. Brno: Masarykova univerzita.
50. Smolík, J. (2018). Prognostics methods of security phenomena. *Vojenské rozhledy*, 27(1), 3–23. https://doi.org/10.3849/2336-2995.27.2018.01.03-24
51. Tetlock, P. E., & Gardner, D. (2016). *Superprognózy: Umění a věda předpovídání budoucnosti* (F. Drlík, Trans.). V Brně: Jan Melvil Publishing.
52. Weisbord, M. R., & Janoff, S. (2010). *Future search: Getting the whole system in the room for vision, commitment, and action* (3rd ed.). San Francisco, CA: Berrett-Koehler.
53. Williamson, K. (2002). The Delphi method. In *Research Methods for Students, Academics and Professionals* (pp. 209–220). Elsevier. https://doi.org/10.1016/B978-1-876938-42-0.50020-4
54. Yousuf, M. I. (2007). Using experts' opinions through Delphi technique. *Practical Assessment, Research & Evaluation*, 12(4), 1–8. https://doi.org/10.7275/rrph-t210
55. Zelinka, P. (2010). Prediktivní metodologie ve zpravodajských službách. *Vojenské Rozhledy*, *19*(1), 29–39.