Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi
Pamukkale University Journal of Engineering Sciences

Implications of intelligence engineering: Designing intelligence diplomacy through game theory, reinforcement learning, and metaheuristic algorithms

İstihbarat mühendisliği uygulamalari: Oyun teorisi, pekiştirmeli öğrenme ve metasezgisel algoritmalar yoluyla istihbarat diplomasisinin tasarimi

İlhan Sağer[1], Gültekin Özdemir[1]*

[1]Department of Industrial Engineering, Faculty of Engineering and Natural Sciences, Suleyman Demirel University, Isparta, Türkiye.
ilhan.sager@gmail.com, gultekinozdemir@sdu.edu.tr

Received/Geliş Tarihi: 10.02.2025 Revision/Düzeltme Tarihi: 17.11.2025 doi: 10.65206/pajes.56383
Accepted/Kabul Tarihi: 01.12.2025 Research Article/Araştırma Makalesi

Abstract

*Considering today's geopolitical conditions, the risks of war and global transformation increasingly highlight the importance of intelligence. Intelligence diplomacy has become a critical component of national security and foreign policy processes. Intelligence diplomacy, an attempt to reduce conflicts and wars by shaping diplomacy through intelligence activities, rather than conflicts themselves, strives to utilize not only the social sciences but also all the instruments of the field. The primary objective of this study is to demonstrate the feasibility of this field, along with its first application, by conducting an application in the field of "**intelligence engineering**," a recently discussed need for which has not yet been implemented in practice. This study designed a game theory-based engineering problem by developing a successful decision algorithm to gain an advantage over adversaries in an intelligence-based diplomacy case. Engineering methods such as artificial intelligence, heuristic and metaheuristic algorithms, and pattern-based analysis were utilized in generating these decision alternatives. Furthermore, a simulation structure consisting of 1000 games, including 75,000 iterations determined through parameter optimization, was constructed and run to investigate which strategy, and therefore which engineering approach, yielded the most successful results. However, the real significance of the study is that it provides evidence in the literature that the concept of "intelligence engineering" is not a utopian approach but a feasible systematic approach, through the first academic application of engineering-oriented scientific and "objective" approaches in intelligence science, instead of traditional social science-oriented "subjective" approaches.*

Keywords: Intelligence, Intelligence Diplomacy, Game Theory, Reinforcement Learning, Genetic Algorithm, Artificial Intelligence

Öz

Günümüz jeopolitik koşulları düşünüldüğünde savaş riskleri ve küresel dönüşüm günden güne istihbaratın önemini ortaya çıkarmaktadır. Ulusal güvenlik ve dış politika süreçlerinde istihbarat diplomasisi çok önem kazanarak kritik bir bileşen haline gelmiştir. Çatışmaların aksine istihbarat faaliyetleri ile diplomasinin şekillendirilerek çatışma ve savaşları azaltma girişimi olan istihbarat diplomasisi, yalnızca sosyal bilimler değil tüm enstrümanları kullanmaya çalışmaktadır. Buradan hareketle yola çıkan çalışmanın temel amacı literatürde son dönemlerde tartışılan gereksinimi anlatılan ama pratik uygulaması yapılamamış "istihbarat mühendisliği" alanında bir uygulama yaparak bu alanın ilk uygulaması ile birlikte uygulanabilirliğini göstermektedir. Yapılan çalışmada istihbarat temelli bir diplomasi vakasında rakiplere karşı üstünlük sağlamak için başarılı bir karar algoritması geliştirilerek oyun teorisi temelli bir mühendislik problemi tasarlanmıştır. Bu karar alternatiflerinin oluşturulmasında; yapay zeka, sezgisel ve metasezgisel algoritmalar, desen tabanlı analiz gibi mühendislik metotlarından faydalanılmıştır. Bununla yetinilmeyerek parametre optimizasyonu ile belirlenmiş 75000 iterasyon içeren 1000 oyunluk bir benzetim yapısı kurgulanarak çalıştırılmış ve hangi strateji dolayısıyla da hangi mühendislik yaklaşımının daha başarılı bir sonuç verdiği araştırılmıştır. Ancak çalışmanın gerçek önemi istihbarat biliminde geleneksel sosyal bilimler odaklı "öznel" yaklaşımlar yerine mühendislik odaklı bilimsel ve "nesnel" yaklaşımların akademik olarak ilk uygulamasının gerçekleştirilmesi aracılığıyla "istihbarat mühendisliği" kavramının ütopik bir yaklaşım değil uygulanabilir bir sistematik olduğunun literatürde kanıtı niteliği taşımasıdır.

Anahtar Kelimeler: İstihbarat, İstihbarat Diplomasisi, Oyun Teorisi, Pekiştirmeli Öğrenme, Genetik Algoritma, Yapay Zeka

1 Introduction

In world history, humanity initially struggled for existence in nature, relying on its individual abilities to survive. While using these abilities for basic activities like hunting and gathering, this process later progressed to the formation of tribes and societies. The initial struggle for existence transformed from individual efforts into a collective, social effort. The simple hunting tools needed now became instruments of war among societies, initiating an arms race that continues to this day. As technology and revolutions evolved from the spear to the destructive weapons of today, they also transformed the structure of societies and even historical eras.

The strategic arms competition that began in antiquity has persisted into the modern era, growing in complexity and scale. Sun Tzu analyzed this transformation in great detail, emphasizing its significance [1]. This evolution was not limited to physical weaponry; as Sun Tzu described, it extended to the domain of intelligence "the art of winning wars without fighting." Over time, basic espionage operations progressed beyond simple information gathering to include disinformation efforts and destabilization campaigns. Particularly during the Second World War, intelligence activities began to break down both military and sociological boundaries, generating operational impact across diverse fields including technology and economics [2]. The Cold War period subsequently introduced the world to a new form of conflict: proxy warfare.

*Corresponding author/Yazışılan Yazar

Within this framework, intelligence operations gained increasing prominence [3]. Independent of traditional war scenarios, numerous studies have demonstrated that the acceleration of technological development has negatively impacted global sustainability [4]. Moreover, the emergence of thermonuclear, chemical, and biological weapons as part of modern warfare has posed significant threats to global stability. In response, imperial powers have increasingly turned to proxy and intelligence-based warfare in an effort to avoid direct military confrontation [5].

While today's conditions still carry the risk of large-scale and destructive war, proxy conflicts and rising tensions between imperial powers have raised the strategic importance of intelligence to an even more critical level. An examination of studies in the field reveals that processes such as data collection, classification and clustering, verification, and analysis constitute the foundational structure of intelligence systems [6]. Research conducted by professionals with practical experience in this domain also highlights the decisive influence of accurate data analysis on international diplomacy [7]. As intelligence operations have grown more critical, the analysis phase within the broader intelligence process has come to the forefront [8]. Scholars have emphasized that the need for transformation within the analysis stage extends beyond a set of technical requirements, calling instead for a paradigmatic shift in perspective and cognitive frameworks [9]. The essence of this call lies in redefining intelligence not merely as a subdomain of sociology or political science, but rather as a standalone scientific discipline capable of integrating tools from the natural and applied sciences [10]. Numerous studies underscore the transformative capacity of intelligence when approached through scientific methodology [11]. In this era, often described as the age of artificial intelligence, a scientifically grounded intelligence infrastructure has emerged as a critical competitive advantage for nation-states and organizations alike [12].

Recognizing the growing need for intelligence studies to establish their own academic identity, a number of recent works have sought to develop a dedicated literature and methodology for the field [13]. This evolving perspective, characterized as “intelligence science,” has yielded conceptual frameworks intended to guide future scholarship [14]. Consequently, foundational contributions proposing a systematic approach to the field have become more widespread [15]. These efforts initially focused on counterterrorism applications [16] and subsequently expanded to include counterintelligence operations [17].

Despite this progress, a significant gap remains evident in the literature. Historically situated within the social sciences, the field of intelligence has often been regarded with skepticism by researchers in the natural and applied sciences. As a result, interdisciplinary efforts have been limited, and the demand for methodological diversification has long remained unmet.

In 2017, Adam Svendsen proposed the concept of “intelligence engineering” for the first time [18]. The 2020s, marked by rapid technological advancement and shifting geopolitical dynamics, have renewed interest in this approach, giving rise to a number of exploratory studies intended to guide future practitioners [19]. Initial applications of intelligence engineering emerged within the domain of cyber intelligence [20], and this trend has continued with the development of scenario-based cyber intelligence frameworks [21]. Alongside these developments, a broader transformation in intelligence philosophy has emerged—one that places increased emphasis on engineering-oriented methodologies and tools [22]. Contrary to the field’s overconcentration on cybersecurity and digital communication, scholars have begun to articulate a broader need for engineering-driven frameworks—particularly in light of developments in artificial intelligence [23]. Nevertheless, most existing studies have remained theoretical or narrowly focused on cyber intelligence [24]. In response to this gap, a new study conducted in Turkey in 2025 introduced a systems engineering-based intelligence engineering framework that leverages a wide range of engineering tools [25].

This study aims to demonstrate the applicability of engineering approaches within the intelligence domain not only in areas such as cybersecurity or electronic communication, but across a broader operational spectrum. By adopting and comparing multiple systems engineering methodologies in practice, it represents the first applied study of intelligence engineering in the literature. Furthermore, it offers a reference framework for future work in this emerging field. As a result of this reference study, the practical applicability of engineering instruments beyond conventional activities in the field of intelligence engineering has been demonstrated. Moreover, the findings indicate that the use of these methods can significantly contribute to this domain. In this respect, the study represents a pioneering effort in the literature.

This section introduces the topic, explaining the study's initial objectives, objectives, and significance. The second section presents the fundamental concepts discussed in this section, their theoretical explanations, and, most importantly, the literature studies that paved the way for this study. The "intelligence diplomacy" concept in the study, along with the formation of the "artificial intelligence" and "game theory" systematics used in the methods used, are explained in detail. The third section then provides the reader with a wealth of information, including the practical basis for the application, the methods used, why and how they are used, the selected parameters, and the selection method. This section provides guidance for researchers who intend to implement a similar application and provides initial settings for those who wish to replicate the application. The fourth section presents the mathematical representation of the application's hardware infrastructure, the resources used for the application, and its performance, along with the results obtained from its execution. The objective output of the results is presented here in a tabular format. And then, in the last part of the study, both the general outcomes of the study and its academic importance and originality were evaluated, based on the fiction explained since the first part and the methods explained in the following parts and their numerical findings.

2 Literature Review

This study integrates multiple disciplines. In this section, key literature from each relevant field is presented in order to establish the theoretical foundation and highlight the study’s original contribution.

2.1 Intelligence Diplomacy

Among the leading scholars who have shaped the intelligence literature, Herman examined the concept of intelligence by addressing the development of modern intelligence systems, their integrated relationship with diplomacy, and the implications of intelligence transformation on diplomatic practice [26]. Lomas provided a detailed analysis of the interactions between these two domains, emphasizing their

reciprocal influence [27]. In his study, Fidan offered an in-depth exploration of the concept of intelligence and its influence on diplomacy through the lens of the foreign policy of the Republic of Turkey, making one of the earliest contributions to the literature on the concept of "intelligence diplomacy" [7]. Kalın analyzed the formation of Turkish foreign policy, highlighting the importance of accurate data and modern institutional structures in strategic decision-making processes [28]. Similarly, Köse argued that diplomacy built upon robust intelligence foundations enhances a state's influence in international affairs [29].

Intelligence diplomacy, as defined in this study by examining leading sources in the literature, can be described as the process by which states, in addition to the special and covert intelligence activities of classical intelligence, engage in covert communication with one another, operating the diplomatic process based on intelligence outputs, and shaping open diplomacy based on these process decisions. In short, while diplomacy is an overt activity in the international arena, and intelligence is a covert activity specific to states, intelligence diplomacy can be viewed as a hybrid diplomacy model between states that operates covertly and covertly at the international level.

2.2 The Game Theory

In engineering-based economic studies, static models where decisions and outcomes across multiple decision models are treated as independent have failed to meet the growing computational demands. This limitation has created a need for a computational framework in which multiple decision-makers or alternative actions influence each other and the resulting outcomes. Game theory emerged in the 20th century as a groundbreaking solution to this need and has since been applied across a wide range of domains, from economics to politics. The theoretical foundations were laid in 1928 by the scientist John von Neumann through his formulation of the "minimax theorem," a model involving two decision-makers in a zero-sum setting where one player's gain is equivalent to the other's loss [30]. The conceptual structure of the field was further established with the publication of Theory of Games and Economic Behavior in 1948 by John von Neumann and Oskar Morgenstern, which focused on applications in economics [31]. Shortly thereafter, John Nash introduced the concept of the "Nash equilibrium," a decision point that became a cornerstone for modeling multi-player games [32]. Nash also developed the theory of "two-player cooperative games," which extended the applicability of game theory from economics into other fields such as political science [33].

At its core, game theory models interactions among multiple decision-makers by analyzing decision alternatives and the potential benefits or losses resulting from various combinations of these alternatives. Beyond its initial applications in economics, statistics, business, and engineering, game theory has also gained traction in political science, strategy, and diplomacy [34]–[37].

In the intelligence literature, game-theoretic approaches have been applied in a limited number of studies. In [38], for instance, game theory was used to mathematically model the possible outcomes of rival decision-makers in military decision-making problems. Another study employed a game-theoretic framework to construct a decision model for national intelligence activities [39].

2.3 Artificial Intelligence & Other Algorithms

The "Boolean Algebra" approach introduced by [39] laid the foundation for digital computing and related scientific disciplines, serving as a precursor to a technological revolution that would emerge in the decades that followed. The invention of the "Turing Machine" by Alan Turing established the conceptual basis for artificial intelligence and introduced a logical framework that remains a reference standard to this day[40]. Shortly thereafter, Alan Turing posed the question "Can machines think?" in a seminal work that marked the beginning of an era-defining intellectual pursuit [41]. This trajectory culminated in the 1956 Dartmouth Conference, where the conceptual framework for artificial intelligence was formally introduced [42].

Originally developed to predict a dependent variable based on its relationship with associated independent variables, their coefficients, and constants, artificial intelligence methods expanded to include classification and clustering tasks. With the development of artificial neural networks, machine learning emerged as a computational paradigm. The scarcity of labeled data subsequently gave rise to deep learning, while advances in language modeling contributed to the evolution of natural language processing. In parallel, visual analysis led to the field of computer vision, and all of these developments collectively informed the creation of expert systems. This transformation has extended from simple machines capable of human-like reasoning to robotic systems capable of autonomous action.

Artificial intelligence, which now influences virtually every domain of modern life, has become a defining feature of the contemporary era. While applications abound across sectors, their integration into intelligence studies remains limited. Existing works in the field are largely theoretical and have yet to result in applied frameworks.

In Darıcılı's study, the integration of artificial intelligence into the Turkish intelligence system was examined, with attention to its impact on national security and foreign policy formulation[43]. In Aksu's study, artificial intelligence was proposed for use in military strategy development through the concept of "smart warfare systems" [44]. A distinct perspective on the use of AI in intelligence was presented in by Karabulut [45]. While numerous studies emphasize that the use of AI technologies in this field is not merely an option but a necessity, a persistent disciplinary divide has limited progress. Researchers from the social sciences have dominated the field, while contributions from engineering and the natural sciences have remained largely confined to domains such as signals intelligence, satellite imagery, and cybersecurity. Combined with underlying psychological and institutional biases, this has resulted in a noticeable gap in the literature [13], [23].

In 2025, a study proposed for the first time a methodological framework that advocates for the use of engineering disciplines -specifically systems engineering- in the field of intelligence [25]. This study aimed to introduce the first applied model into the literature and to serve as a reference point for future research efforts in this domain.

In achieving this goal, two points were considered. First, there is a lack of labeled and fully known data, making it impossible to speak of fully verified data in intelligence processes. Second, and more importantly, while each decision is relatively independent of previous decisions, each decision is still influenced by the sum of previous decisions and their outcome.

In this context, among the artificial intelligence learning models, the researchers deemed the use of the "reinforcement learning" model, a discrete-time learning model that is also based on Markov chains, but can work in situations where exact methods that do not require labeled data and precise information are not feasible, and aims to achieve the highest reward score.

A review of the literature reveals two distinct approaches to solving optimization problems. The first is called exact methods, which guarantee the global best result but are particularly inefficient in terms of resource and time requirements, especially for large-scale or complex problems. These approaches will not be very effective for large-scale and challenging problems like those presented in this study. The second approach is heuristic and metaheuristic, which are approximate approaches. Because this study addresses a large-scale, multi-alternative decision problem, these approaches were deemed more suitable. Among these, the "*genetic algorithm*" was deemed suitable as the primary method. "*Pattern recognition*", derived from supervised learning, a type of artificial intelligence learning model, or pattern-based analysis, was also selected as a suitable model for this study.

3 Material and Methods

In this study, a diplomacy-based game theory problem has been formulated to analyze how an intelligence agency develops policies against rival intelligence agencies, as well as the rival's unaware countermoves and the resulting outcomes. The game approaches the problem from a fundamental perspective, incorporating certain assumptions to examine which method allows for more accurate predictions of rival moves or the formulation of a more successful policy. The assumptions made in the formulated game problem are as follows:

The analysis considers only the interactions between two intelligence agencies, assuming no third-party involvement or external intervention.

Only three fundamental moves have been defined: Peace (no additional investment or action against the rival), Passive (involves counterintelligence measures against potential intelligence operations from the rival, in addition to a peace policy), and Attack (includes espionage operations against the rival in addition to the countermeasures in the passive stance).

There is no historical, ethnic, or political conflict, nor any special political trust between the rivals; the past relationship is assumed to be neutral.

Intelligence agencies are assumed to have equal power.

Based on these assumptions, the study constructs a gain-loss function, where each round involves both rivals independently selecting one of the three alternatives without prior knowledge of the other's decision. The scoring system for different scenarios is as follows:

If both players choose the peace policy, they each gain 3 points, assuming a mutual benefit without additional effort.

If one player chooses peace while the other selects passive, the peaceful player earns 2 points, while the passive player loses 1 point due to unnecessary counterintelligence efforts.

If one player chooses peace while the other selects an attack, the attacking player gains 3 points, while the peaceful player loses 1 point due to successful espionage.

If both players choose passive, neither gains any points (0 points each).

If one player chooses passive while the other selects attack, the failed intelligence attempt results in the passive player gaining 2 points, while the attacker loses 1 point.

These conditions are symmetrical, meaning the same scoring applies when the roles are reversed.

After defining the game rules, determining the players' and opponents' moves, and assigning point values to these moves, specific strategies were developed for the players. Players formulated their policies based on these strategies. Since the objective of this study is not to evaluate individual cases but rather to develop a diplomatic strategy, the key focus has been on comparing different strategic approaches. In total, 12 strategies were created, consisting of 6 fundamental psychological operations strategies and 6 advanced strategies.

Fundamental Strategies:

1. **Peaceful Strategy:** A player who always chooses the peace strategy, regardless of circumstances.
2. **Passive Strategy:** A player who always opts for the passive strategy in every round.
3. **Aggressive Strategy:** A player who consistently selects the attack strategy in all rounds.
4. **Imitative Strategy:** A player who makes a random choice in the first round and then mimics the opponent's previous move in subsequent rounds.
5. **Pragmatist Strategy:** A player who initially appears peaceful but then attempts an attack to normalize it, and after three rounds, selects the move that maximizes gains based on the opponent's behavior, exploiting its weaknesses.
6. **Revengeful Strategy:** A player inclined toward peace but, if attacked by the opponent, responds with continuous and intense aggression. When the opponent exhibits a passive stance, the player also resorts to passive defense.

In this study, the fundamental strategies are not meant to represent the exact choices of an intelligence unit in real-world scenarios. Instead, they are designed based on instinctive and psychological operations principles to prevent a bias toward any particular direction. In real diplomatic processes, significantly more complex strategies are employed.

Thus, the primary focus of this study is to use algorithms and modern methodologies to predict opponent moves and develop a superior strategy. To achieve this, 6 additional advanced strategies were formulated.

Advanced Strategies:

1. **Basic Insidious Strategy:** A player who observes the opponent's moves and attempts to attack when the opponent is vulnerable while switching to defense when the opponent becomes aggressive.
2. **Insidious Strategy:** A player who observes the opponent's moves and prioritizes an attack that counters the most frequently used move of the opponent, ensuring they do not lose in the process.
3. **Genetic Algorithm Strategy:** A player who analyses the opponent's moves using a genetic algorithm, treating the pattern as a DNA sequence and attempting to create a winning move pattern.

4. **Pattern-Based Strategy:** A player who predicts the opponent's moves through pattern-based analysis and aims to develop a winning pattern.
5. **Reinforcement Learning (AI) Strategy:** A strategy based on reinforcement learning, one of the most widely used learning models in AI research when labelled data is scarce. This strategy learns the opponent's moves and attempts to predict their next moves to secure victory.
6. **Random Strategy:** A strategy in which the player randomly selects one of three different moves in each round. Of course, in real life, an intelligence agency would not act this way. This strategy serves as a benchmark because, in a few rounds, the logic behind basic strategies will be anticipated by advanced strategies, leading to dominance. Since move selection lacks logic and pattern, the opponent becomes a strong adversary, and the most sophisticated strategies will still be able to predict and counter it, making this strategy useful as a reference point.

In determining the strategies employed in this study, six fundamental strategies commonly encountered in adversarial games and relevant to the field of intelligence were initially selected as the baseline strategies. Subsequently, the design of advanced strategies was undertaken. A basic insidious algorithm, deemed suitable for modeling intelligence policies, was specifically developed for this study. Given that the outcome of a conflict is considered more critical than peacetime operations in intelligence warfare and that the scoring system was accordingly designed this bespoke insidious algorithm was tailored to align with such priorities. Furthermore, a single artificial intelligence-based strategy was incorporated, and due to the necessity of in-game learning, reinforcement learning was selected.

In accordance with the sequential pattern-based nature of the game, another strategy was included that detects and exploits repeated behavioral patterns. Next, in order to explore a complex strategy space and to identify the global optimum i.e., the absolute winning strategy several heuristic or metaheuristic algorithms were considered appropriate for constructing a hybrid strategy. Among these, the genetic algorithm was chosen due to its broad applicability, ease of integration with other algorithms, and high degree of flexibility. Finally, in consideration of real-world applicability, although not practically deployable in an operational intelligence context, a random strategy selecting among three decision alternatives entirely at random was included. This strategy was introduced primarily to serve as a performance benchmark, given its inherently unpredictable behavior and high resistance to opponent modeling or learning.

In accordance with the sequential pattern-based nature of the game, another strategy was included that detects and exploits repeated behavioral patterns. Next, in order to explore a complex strategy space and to identify the global optimum i.e., the absolute winning strategy several heuristic or metaheuristic algorithms were considered appropriate for constructing a hybrid strategy. Among these, the genetic algorithm was chosen due to its broad applicability, ease of integration with other algorithms, and high degree of flexibility. Finally, in consideration of real-world applicability, although not practically deployable in an operational intelligence context, a random strategy selecting among three decision alternatives entirely at random was included. This strategy was introduced primarily to serve as a performance benchmark, given its inherently unpredictable behavior and high resistance to opponent modeling or learning.

As a result, the game framework was constructed using a total of 12 strategies: 6 fundamental and 6 advanced. Once the strategies were established, the parameterization of the associated algorithms, particularly those used in advanced strategies, was guided by the most frequently encountered configurations in the literature. Nevertheless, the genetic algorithm displayed markedly inferior performance under default settings. This underperformance was attributed to the algorithm's three core parameters: Population Size, Generations, and Mutation Rate. Initial values were selected as (100, 100, 0.01), consistent with standard practice in the literature. However, these settings led to excessive resource consumption, prolonged execution time, and suboptimal performance. While the other algorithms were able to produce strategic responses within five moves, the genetic algorithm required blocks of 100 moves to formulate basic decisions, resulting in considerable scoring deficits.

Consequently, it was deemed appropriate to reduce both the population size and the number of generations, while increasing the mutation rate. A configuration of (10, 5, 0.2) was selected, corresponding to 10-move segments, five initial generations, and 2-move incremental corrections. Under this revised setting, the model demonstrated improved runtime performance, increased flexibility for real-time applications, and higher success rates. Accordingly, the "Genetic Algorithm" strategy within the study was executed using this optimized parameter configuration.

A bespoke software was developed in Python to implement the model, featuring a simple graphical user interface (GUI) through which the entire model could be operated. At this stage, two critical methodological questions emerged: (i) *How many iterations should a single game include?* and (ii) *How many games must be played to meaningfully assess the relative superiority of the algorithms?*

For the first question, it was concluded that the number of iterations must be sufficient to allow the performance of adaptive algorithms to converge. However, due to resource constraints, the minimum number of iterations that would still ensure meaningful results needed to be determined. Among the 12 strategies, only two Random Strategy and Reinforcement Learning were found to be directly affected by iteration count. For the Random Strategy, a sufficient number of iterations is necessary to achieve a balanced distribution across the three decision alternatives, so that true randomness can be asserted. For the Reinforcement Learning algorithm, performance is contingent on the extent of learning, particularly in the absence of labeled data.

A critical insight was that excessive iterations could lead to overfitting. Thus, two metrics were identified for close monitoring: (1) the frequency distribution of choices made by the Random Strategy, and (2) the learning rate of the reinforcement learner. The learning rate was operationalized as the proportion of moves resulting in an update to the Q-table, the mathematical structure underlying reinforcement learning.

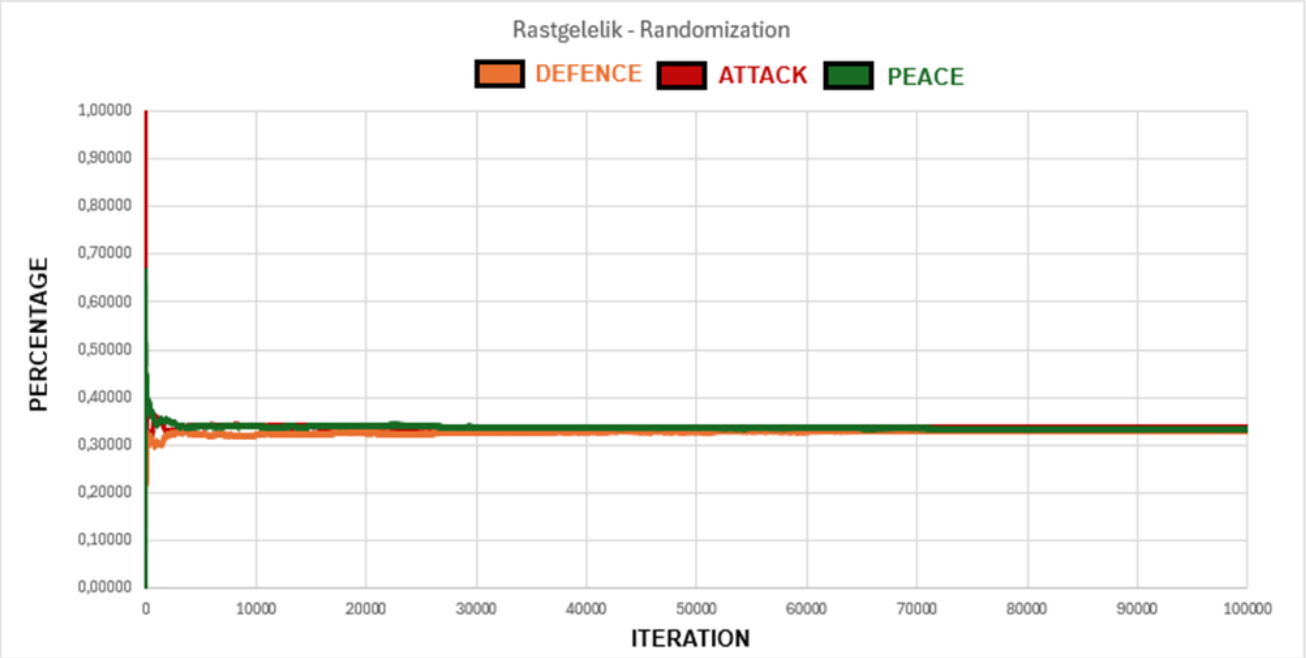

Figure 1. Randomization Graph for Random Strategy.

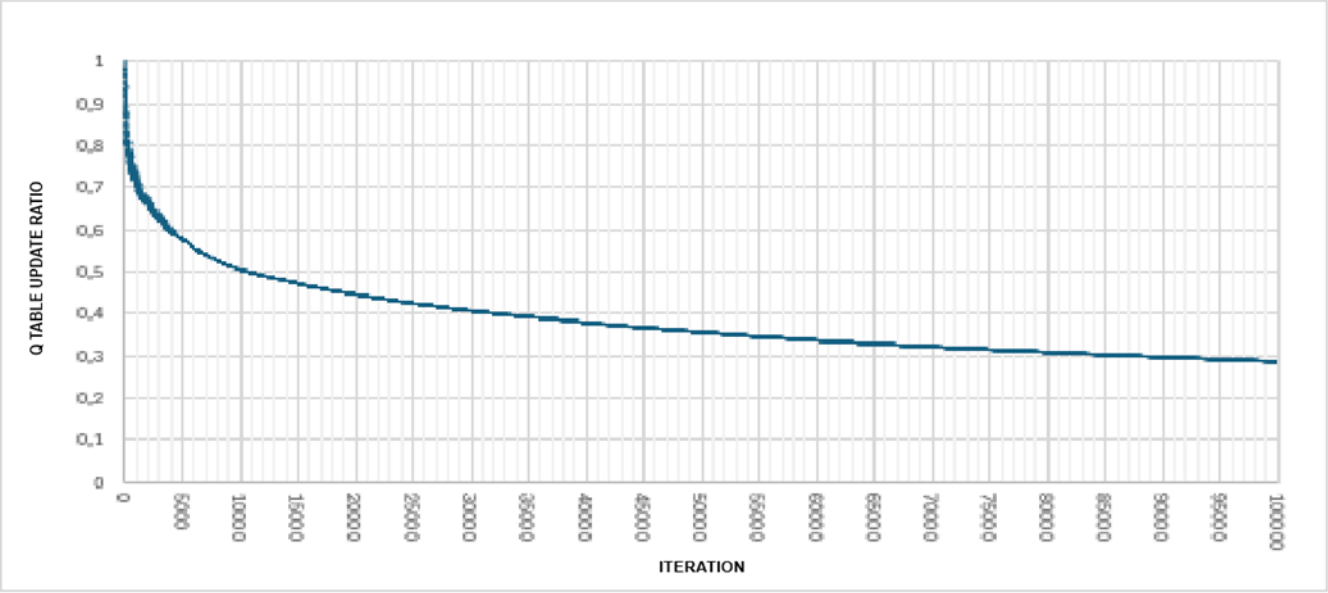

Figure 2. Learning Graph includes Updating of QTable.

If the algorithm updated the Q-table for a given move, it was considered to be learning; otherwise, it was either testing or making predictions. Therefore, the ratio of Q-table updates to total moves served as a proxy for learning progression. As expected, this ratio begins near one and decreases steadily over time. Once the ratio plateaus, it is inferred that learning has saturated and further iterations would likely induce memorization rather than generalization.

The program was modified to visualize both metrics. Experimental design was then guided by these visual indicators. Both algorithms were run for 100,000 iterations. As shown in Figure 1. Randomization Graph, after approximately 70,000 iterations, the selection probabilities of the three alternatives converged to 1/3, and no further fluctuations were observed. Similarly, Figure 2. Learning Graph illustrates that learning activity nearly ceased after 80,000 iterations, as evidenced by the flat slope of the update ratio. From these observations, the optimal iteration count was estimated to lie between 70,000 and 80,000, with 75,000 selected as a balanced figure.

Regarding the second question, initial trials were conducted with 100 games to calculate win-rate percentages, increasing in increments of 25 games to assess convergence. As depicted in Figure 3. Results Table, outcome variability diminished as the number of games increased. Beyond 800 games, changes in overall scores were observed, but the identity of the winning

algorithm remained consistent. Accordingly, the total number of games was fixed at 1,000.

4 Summary of Results

In this study, a problem was designed that simulated the continuous struggle between two rival intelligence agencies based on intelligence. In this problem, two different players, with three different decision alternatives, made decisions against each other, resulting in a quantitative outcome. This situation pointed the researchers to a game theory approach. In short, a two-player game model with three decision alternatives and a zero-sum reward/punishment scoring system was constructed. To solve this problem, a software program specifically for this study was developed in Python 3.10.2. The Python-based software, developed specifically for this study, was run to run 1,000 games, each consisting of 75,000 rounds, between 12 players. The simulations were run on a system equipped with an Intel(R) Core(TM) i7-5500U CPU 2.40GHz, 8GB of RAM, and the Windows 11 operating system. The total model run time was measured at 72 hours. Considering the need for iterative testing during the experimental design and software development process, the same software was recoded in TypeScript to improve system and time resources. The results were obtained in approximately 8 hours using an OOP-based structure.

When analyzing the game results, mutual reward points were revealed. For simplicity, the players' overall reward/penalty points were calculated by subtracting the number of wins from the number of losses. For example, if Player A won 600 times, tied 300 times, and lost 100 times in 1000 games against Player B, a reward of +500 was assigned from Player A to Player B, and a penalty of -500 was assigned from Player B to Player A, resulting in a zero-sum result. Based on this, it is clear that the possible value range for reward/penalty points is between -1000 and +1000. The important point here is that the selected players (and therefore the selected algorithms) who achieved a result of +1000 / -1000 demonstrate absolute and definitive superiority over each other. The game results are shown in Figure 3.

Figure 3. A simple examination of the Results Table Screenshot reveals that the first diagonal represents a battle between the same player and itself, so it is colored black and excluded from the analysis. The table (being zero-sum) yields a symmetrical result with respect to this diagonal. Green indicates the winning strategy, red indicates the losing strategy, and finally, yellow indicates a tie.

A closer examination of the **Figure 3. Results Table Screenshot** reveals even more striking results. The results of a total of six basic strategies, three uniform and three algorithmic, offer several important insights. The uniform basic strategies (aggressive, peaceful, and passive) yielded a triangular symmetry with each other. That is, each player achieved an absolute victory against one of their two opponents and an absolute loss against the other. This situation represents a combination of "Rock-Paper-Scissors" in game theory. However, real-life situations would be very different from "Rock-Paper-Scissors." The three uniform basic strategies were significantly weaker and ineffective against the three algorithmic strategies. In **Figure 3**, without considering the first column and row as the descriptive header row, it is clearly visible between rows 2, 3 and 4 and columns 2, 3 and 4 in the matrix representation in the middle.

When **Figure 3** is examined, the Imitative, Pragmatist, and Revengeful strategies achieved 6 victories, 4 of which were absolute victories, against the Aggressive, Passive, and Peaceful strategies. However, they suffered 2 defeats, 1 of which was narrow, and a draw in 1 case. This situation will yield the analyst's first outcome as follows: "It is clear that monotonous basic strategies will be weak and ineffective against basic algorithmic strategies in a battle." This is clearly evident in the matrix representation in **Figure 3**, between Rows 5, 6, and 7, and Columns 2, 3, and 4.

	Random	Aggressive	Passive	Peaceful	Imitative	Pragmatist	Revengeful	Genetic	Reinforceme	Pattern Base	Basic Insidio	Insidious
Random	X	- 1.000	68	1.000	- 16	10	- 1.000	1.000	- 1.000	2	- 16	46
Aggressive	1.000	X	- 1.000	1.000	- 35	- 1.000	1.000	1.000	- 1.000	- 1.000	- 1.000	- 1.000
Passive	- 68	1.000	X	- 1.000	36	- 1.000	- 1.000	- 1.000	- 1.000	- 1.000	- 1.000	- 1.000
Peaceful	- 1.000	- 1.000	1.000	X	- 10	- 1.000	-	- 1.000	- 1.000	- 1.000	- 1.000	- 1.000
Imitative	16	35	- 36	10	X	1.000	-	- 994	- 1.000	- 893	- 1.000	- 1.000
Pragmatist	- 10	1.000	1.000	1.000	- 1.000	X	1.000	1.000	- 1.000	346	1.000	1.000
Revengeful	1.000	- 1.000	1.000	-	-	- 1.000	X	1.000	- 1.000	- 1.000	- 1.000	- 1.000
Genetic	- 1.000	- 1.000	1.000	1.000	994	- 1.000	- 1.000	X	- 1.000	- 908	- 1.000	- 1.000
Reinforceme	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	X	1.000	1.000	1.000
Pattern Base	- 2	1.000	1.000	1.000	893	- 346	1.000	908	- 1.000	X	942	1.000
Basic Insidio	16	1.000	1.000	1.000	1.000	- 1.000	1.000	1.000	- 1.000	- 942	X	-
Insidious	- 46	1.000	1.000	1.000	1.000	- 1.000	1.000	1.000	- 1.000	- 1.000	-	X

Figure 3. Results Table Screenshot.

Following the examination of basic strategies, the competition between advanced strategies designed using the selected engineering discipline methods "***Genetic Algorithm***," "***Reinforcement Learning***," "***Pattern-Based***," "***Basic Insidious***," and "***Insidious***," as detailed in the previous section, against monotonous basic strategies is revealed in **Figure 3**. In the similar matrix analysis, in the sections of rows 8-12 and columns 2-4, 8 absolute victories and 1 absolute loss are observed. Similarly, in the similar matrix analysis in **Figure 3**, in the sections of rows 8-12 and columns 5-7, algorithmic basic strategies were also ineffective against engineering-based strategies. This situation yields the following conclusion: "Advanced engineering-based algorithms have achieved a significant advantage over basic strategies."

The evaluation of the findings thus far reveals that monotonous strategies are ineffective compared to all other strategies in basic strategies, while an algorithmic player has the advantage over these strategies. Conversely, the general superiority of players who develop strategies using engineering sciences and their methods over all others was commented on. The expected striking results of the study will emerge in the evaluation phase of this section. So, how did the engineering-based strategies that demonstrated their superiority over other strategies fare in the competition between themselves?

Figure 3. Results Table. A similar careful examination of the relevant section of the screenshot (rows 8-12 and columns 8-12) reveals that these strategies, when examined in three groups, yielded a significant result. The metaheuristic algorithm group represented by the ***genetic algorithm*** was ineffective against the other advanced strategies. This is expected, given the structure and purpose of metaheuristic algorithms, as opposed to finding the global best, and their lack of problem specificity. In contrast, the two heuristic algorithms developed for this problem provided superiority over the genetic algorithm but were ineffective against the others. Finally, one, a "Pattern-Based Algorithm," directly suited to the problem structure, and the other, "Reinforcement Learning," independent of the game structure, and the artificial intelligence technology it represents, clearly outperformed all other strategies. So, how did these two definitively winning algorithms compare? The answer to this question is clearly evident in Figure 3. In this struggle, the "***Reinforcement Learning***"-based strategy triumphed decisively. Therefore, the final outcome of the study is as follows: "While metaheuristic methods have a positive impact on solution efficiency, study-specific heuristics yielded more successful results, and specialized models suited to the study structure naturally produced superior results. However, a sufficiently trained Reinforcement Learning model achieves superior success, including all scientific methods." In addition to the striking nature of this outcome, a specific assessment of this situation is provided in the final section of the study.

Following the evaluations, a final additional analysis was conducted. While the previous section has evaluated players acting with a basic strategy or advanced strategy and a specific mindset, a player created for this special study, which was included in the study but not considered until now, stands out. A player model called "Random Strategy" that makes a completely random (equally likely) choice among three decision alternatives stands out here. Of course, such random choices wouldn't be made in real life, especially in such a sensitive situation, but the aim here was to demonstrate the following: The winning strategy analyzed the mindset of the opposing players and developed a countermove. However, if the opposing player were a completely random player and not rational, could they even model their random choices and countermove? No matter how many times the application was run, the "***Random Strategy***," whose outcome changes with each player, loses decisively only to the "***Reinforcement Learning***" strategy across all iterations and simulations. This also yielded a final output. An AI system with a sufficiently trained and optimized "***Reinforcement Learning***" model can analyze and develop a counter-strategy even if the opposing player is not rational and makes random choices.

Based on the findings of this study, this problem, modeled on game theory and developed and compared with engineering methods, offers the reader a different perspective. It has the potential to herald a transformation in the concept of "***intelligence diplomacy***," the real-world problem on which this study focuses. Diplomacy is explicitly comprised of the decisions different players make against each other and their consequences, while intelligence diplomacy consists of the covert decisions different players make against each other and their consequences. Therefore, while basic rules and approaches may apply in diplomacy, in ***intelligence diplomacy***, the key is to predict the opponent's covert operational decisions in the face of insufficient data, calculate their consequences, and make decisions accordingly.

While this study is too small to precisely simulate the real world and generate judgments, it is a significant first step in demonstrating that artificial intelligence technologies like ***reinforcement learning*** can offer significant advantages in this field. Comments and general conclusions regarding these are presented in detail in the last part of the study.Conclusions

An examination of the study's structure, purpose, scope, content, and findings allows the reader to draw numerous detailed conclusions.

First, the study's structure allows for a micro-field assessment of the field of intelligence and diplomacy without straying from its core focus. In this context, the applicability of intelligence engineering, the study's objective, beyond conventional diplomatic fields has been demonstrated. However, because the study demonstrates its applicability in this field rather than attempting to fully reflect the conditions of contemporary intelligence diplomacy in a global environment, the conclusions drawn here are more likely to open new horizons in the field than to establish general judgments and acceptances.

The content provides a unique contribution to the literature by comparing traditional, uniform approaches, fictitious algorithmic approaches, and advanced engineering studies, and by offering many of them the opportunity to apply them for the first time in this field. Furthermore, the use of reward-punishment-based game theory and simulation engineering methods, a method first encountered in the literature, sheds light on future research.

Finally, a review of the findings reveals the ineffectiveness of uniform structures in predicting adversary behavior. It raises questions about how effective these strategies are even in global official diplomacy. Compared to these, the superiority of algorithmic strategies has emerged. However, these strategies have also been left helpless in the face of advanced engineering methods. Primarily, the superiority of the advanced engineering approach over traditional methods (within the scope of this study) is striking. Among these, while strategies developed specifically for the specific topic are relatively

prominent compared to mainstream methods, advanced strategies that perfectly meet the framework of the study have become even more prominent. And, independent of all these, the "reinforcement learning" model, which has gained a place in the literature with its effective results in cases of incomplete or unlabeled data, provides absolute superiority over all strategies. It even gains an advantage against opponents who do not behave rationally, and whose actions therefore seem impossible to predict. Its superiority in these situations has been demonstrated through quantitative data, rather than personal observations and interpretations.

In summary, the findings and conclusions obtained point to a key conclusion, considering the purpose and scope of the study. In any period when the risk of war is greater than zero, "intelligence engineering" applications equipped with engineering methods in the fields of "intelligence," "diplomacy," and "intelligence diplomacy" appear to be more than just an option, they are a crucial necessity.

While the study's originality opens a new field in the literature and pioneers and guides subsequent studies, it remains limited in some areas. Based on this study, models such as artificial intelligence and reinforcement learning can be applied to more areas, particularly big data sources such as the internet and social media. This study is modeled solely on two rival states, but in the real world, diplomacy is not between two rivals; many global stakeholders influence these processes. Therefore, the study can be expanded to include multiple players. Furthermore, the study assumes equal power between the two players. However, in the real world, states' power and influence on each other are not equal. This fact can be taken into account and the scope of the study can be expanded.

5 Author contribution statements

In the scope of this study, Author1 conceptualized the idea, developed methodology and software development, performed experimental analysis; Author2 conceptualized the idea, developed methodology, evaluated the results, wrote, visualized, reviewed; supervised and edited the article.

6 Ethics committee approval and conflict of interest statement

“There is no need to obtain permission from the ethics committee for the article prepared.”

“There is no conflict of interest with any person/institution in the article prepared.”

7 References

[1] Tzu S. *Art of War*. California, USA, Ixia Press, 2019.

[2] Andrew C. *The secret world: a history of intelligence*. Connecticut, USA, Yale University Press, 2018.

[3] Keegan J. *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. New York, USA, Vintage Books, 2004.

[4] Sağer I. Bir işletmenin çevre etkisinin ekolojik ayak izi uygulaması ile değerlendirilmesi. MSc Thesis, Pamukkale University, Denizli, Turkiye, 2019.

[5] Güven MO, "Intelligence Theory from an Epistemological Perspective". *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 4(1), 26-3, 2025.

[6] Özdağ Ü. *İstihbarat Teorisi*. Ankara, Turkiye, Kripto Kitaplar, 2008.

[7] Fidan H. Intelligence and foreign policy: A comparison of British, American and Turkish intelligence systems. MSc Thesis, İhsan Doğramacı Bilkent University Ankara, Turkiye, 1999.

[8] Marrin S. *Improving intelligence analysis: Bridging the gap between scholarship and practice (Studies in Intelligence)*. Londra, UK, Routledge, 2012.

[9] Moore DT. *Critical thinking and intelligence analysis, in Occasional Paper No. 14*. Washington DC, USA, National Defense Intelligence College, 2007.

[10] Prunckun H. *Handbook of scientific methods of inquiry for intelligence analysis (no. 11)*. New Jersey, USA, Scarecrow Press, 2010.

[11] Richards J. *The art and science of intelligence analysis*. Oxford, UK, Oxford University Press, 2010.

[12] Freyn S, Hoffman F. "Competitive intelligence in an AI world: Practitioners’ thoughts on technological advances and the educational needs of their successors," *Journal of Intelligence Studies in Business*, 12(3), 6-17, 2022.

[13] Yılmaz S. *21. yüzyılda güvenlik ve istihbarat*. İstanbul, Turkiye, Alfa Yayınları, 2006.

[14] Yılmaz S. *Dünyayı Yöneten Güç İstihbarat Bilimi*. Ankara, Turkiye, Kripto Kitaplar, 2013.

[15] Yılmaz S. *İstihbarat Bilimi*. Ankara, Turkiye, Kripto Kitaplar, 2015.

[16] Wagner A. “Intelligence for counter-terrorism: Technology and methods, Journal of Policing, Intelligence and Counter Terrorism” 2(2), 48-61, 2007.

[17] Duvenage P, Von Solms, Corregedor M. "The Cyber Counterintelligence Process-a conceptual overview and theoretical proposition," *Proc. of the 14th ECCWS*, University of Hertfordshire, Hatfield, UK, 42-52, 2015.

[18] Svendsen AD. "Introducing Intelligence Engineering: Operating beyond the Conventional," *Romanian Intelligence Studies Review*, no. 17-18, pp. 205-214, 2017.

[19] Dandan S, Svendsen AD. "Intelligence Engineering: The Spymaster’s Guide To the 21st Century." https://nationalinterest.org/blog/buzz/intelligence-engineering-spymasters-guide-21st-century-143522 (accessed 27.04.2025.

[20] Svendsen AD, Garvey B. "Generating Cyber Intelligence (CYBINT) scenarios & solutions to address uncertainty for decision-advantage: Using Intelligence Engineering & Strategic Options Analysis," Available at SSRN 4495254, 2022.

[21] Svendsen AD, Garvey B. "A Macro Cyber Scenario Case Study using Intelligence Engineering and Strategic Options Analysis Methods," Available at SSRN 4495298, 2022.

[22] Yılmaz S. *Postmodern İstihbarat*. Antalya, Turkiye, İlkim Ozan Yayınları, 2021.

[23] Şen YF, Yurtoğlu D. "The Importance of Artificial Intelligence in Intelligence Analysis in the Context of Technology and Security Relationship," *Journal of Security Studies*, 22(1), 2020.

[24] Garvey B. Svendsen AD. *Intelligence Engineering-Led Set-up of Generic Strategic Options Analysis Problem to Solution Spaces: Cyber Example Demonstration*, Navigating Uncertainty Using Foresight Intelligence: A Guidebook for Scoping Scenario Options in Cyber and Beyond, 53-66, NYC, USA, Springer, 2024

[25] Sağer I, Özdemir G. "İstihbaratın Bilimsel Bir Disiplin Olarak Yeniden Doğuşu İstihbarat Mühendisliği," *Anadolu Strateji Dergisi*, 7(1), 73-86, 2025.

[26] Herman M. "Diplomacy and intelligence," *Diplomacy and statecraft*, 9(2), 1-22, 1998.

[27] D. W. Lomas, Intelligence and Diplomacy: changing environment, old problems, New perspectives on diplomacy: a new theory and practice of diplomacy, (55-76), Oxford, UK, Oxford University Press, 2021.
[28] Kalin I. "Turkish foreign policy: Framework, values, and mechanisms," *International Journal*, 67(1), 7-21, 2012.
[29] Köse T. *Stratejik Derinlik ve Düzen Kurucu Dış Politika*. Editors: T, Köse, A, Okumuş ve B, Duran. Stratejik Zihniyet: Kuramdan Eyleme Ahmet Davutoğlu ve Stratejik Derinlik. 189-219, İstanbul, Turkiye, Küre Yayınları, 2014.
[30] Von Neumann J. "Zur theorie der gesellschaftsspiele," *Mathematische annalen*, 100(1), 295-320, 1928.
[31] Von Neumann J, Morgenstern O. *Theory of games and economic behavior*, New Jersey, USA, Princeton University Press, 1944.
[32] Nash Jr JF, "Equilibrium points in n-person games," *Proceedings of the national academy of sciences,* 36(1), 48-49, 1950.
[33] Nash J, "Two-person cooperative games," *Econometrica: Journal of the Econometric Society*, 128-140, 1953.
[34] Büyüktuna M, Görür AK. "Hybrid model chipless RFID tags based on the integration of filter theory and multi-resonator circuit," *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 30(2),196-201, 2024.
[35] Ceylan AM. "Set theory interpretation for exponential approximation of time-ordered integral," *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 30(6),785-789, 2024.
[36] Debnath S, Kamacı H. "Hypersoft game theory models and their applications in multi-criteria decision making," *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 29(7),680-691, 2023.
[37] Ozan YA. "Flow structure along the cross-section of an open-channel caused by patch of submerged vegetation," *Pamukkale University Journal of Engineering Sciences*, 23(6), 726-731, 2017.
[38] Ravid I. "Military decision, game theory and intelligence: An anecdote," *Operations Research*, 38(2),260-264, 1990.
[39] Munton D, Fredj K. "Sharing secrets: A game theoretic analysis of international intelligence cooperation," International Journal of Intelligence and CounterIntelligence, 26(4),666-692, 2013.
[40] Turing AM."Turing machine," *Proc London Math Soc*, *242*),230-265, 1936.
[41] Turing AM. "Mind," *Mind*, 59(236),433-460, 1950.
[42] J. McCarthy, N. Rochester, and C. Shannon, "Dartmouth workshop," 1956.
[43] Darıcılı AB. "The impact of artificial intelligence management upon international security," *Savunma Bilimleri Dergisi*, 19(37),49-72, 2020.
[44] Aksu D. "Yapay Zeka Destekli Akıllı Savaş Stratejilerinin Ulusal, Bölgesel ve Küresel Güvenlik Çalışmalarına Etkisi," *Türkiye Siyaset Bilimi Dergisi*, 7(1),1-14, 2024.
[45] Karabulut A, Değer F. *İstihbaratta Yapay Zeka Teknolojisi ve İletişim Güvenliği İstihbarat Dünyası*. Ankara, Turkiye, Kripto Yayınevi, 2015.