INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 2, PP. 1-9
Manuscript received August 06, 2026; revised April, 2026. doi: 10.24425/ijet.2026.157913

A multifactor model of countering targeted attacks within the framework of an infinite antagonistic game scheme

Arkadii Chikrii, Valerii Lakhno, Volodimir Malyukov, Alona Desiatko, Inna Malyukova, Tetiana Zhyrova, and Nataliia Kotenko

***Abstract*—A multifactor model for countering targeted attacks is developed. This model considers the parties' financial resources (FRs) in an infinite antagonistic game framework. The model helps to make rational decisions on allocating FRs for cybersecurity under the threat of APT attacks. The proposed model allows for determining the game's value and assessing the degree of risk when using optimal mixed strategies for FRs. Optimal mixed strategies refer to a combination of strategies that maximize the player's expected payoff, taking into account the opponent's strategies. This concept is essential for analyzing the financial aspects of countering APT attacks. The relevance of the research is due to the growing number of targeted attacks on critical infrastructure objects. Computational experiments visualize the game's results, which is helpful for cybersecurity analysts. The solution to such a problem contributes to the analytical search for the game's meaning. It makes it possible to find the characteristics of the degree of risk of the players reaching the target when they apply optimal mixed strategies. The found solution contributes to the analysis of the situation with counteraction to the party attacking various objects, including critical ones, with the help of APT attacks.**

***Keywords*—APT attack; infinite antagonistic game; optimal strategy; financial resources; probability**

I. Introduction

TARGETED attacks, also known as Advanced Persistent Threats (APTs) [1, 2], represent one of the most severe and complex threats to modern cybersecurity (CS). These attacks are characterized by a high degree of organization, long residence times on the victim's systems, and sophisticated techniques, making them extremely dangerous to organizations of all sizes and sectors, especially critical infrastructure (CI). These attacks are often carried out by highly skilled hacker groups that may be state-sponsored or large criminal organizations. The attacker then has significant resources and may use sophisticated and costly attack methods, which significantly increases their effectiveness and difficulty of detection. This case can be referred to as an example of the use of BlackEnergy malware in attacks on energy companies in Ukraine, which led to power outages in 2015.

As information technology (IT) advances, today's cyber threat landscape becomes increasingly complex and diverse. However, traditional defenses such as antivirus programs and firewalls are often insufficient to counter targeted attacks that exploit zero-day vulnerabilities, social engineering techniques, and other sophisticated techniques. Successful APTs can remain undetected on a victim's systems for months or years, collecting sensitive data, conducting industrial espionage, or damaging critical infrastructure. For example, the hacker group APT1 (PLA Unit 61398), allegedly affiliated with the Chinese army, has conducted a multi-year cyber espionage campaign against Western companies and organizations. They successfully penetrated dozens of companies' networks and stole confidential information and intellectual property [3]. In 2013, hackers successfully breached Target's network [4], exploiting vulnerabilities in third-party systems to access Target's internal systems. The data breach compromised millions of credit and debit card data.

Researching and countering targeted attacks is paramount in the context of digital transformation and the growth of data volumes. Targeted attacks are particularly relevant in the growing dependence on businesses and government IT services. The financial, reputational, and operational risks associated with successful APTs can result in significant losses and lengthy remediation efforts. In addition, such attacks can undermine the trust of customers and partners, negatively impacting organizations' competitiveness and resilience.

Then, it is logical to ask, "What are the costs of preparing and conducting an APT attack for the attacker?". If the organization's management is aware of the threat from APT attacks and pays due attention to cyber security (CS) as a whole, then protection specialists can forecast the necessary financial and other resources to protect their information assets. For this purpose, the defense side must understand the general methodologies of APT attacks. At the same time, it is evident that the profit from a successful hack for the attackers should exceed their costs, including the time spent on the attack. We believe studying the financial aspects of countering targeted attacks through game models is critical in creating effective defense strategies. Such an approach helps balance costs and benefits, minimize economic losses, and improve an

Valerii Lakhno is with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua).

Arkadii Chikrii and Volodimir Malyukov are with Department of Optimization of Controlled Processes of the V. M. Glushkov In-stitute of Cybernetics of the National Academy of Sciences of Ukraine, Kyiv, Ukraine (e-mail: g.chikrii@gmail.com, volod.malyukov@gmail.com).

Inna Malyukova is with Rating agency "Expert-rating", Lead Analyst, Kyiv, Ukraine (e-mail: imalyukova82@gmail.com)

Alona Desiatko, Tetiana Zhyrova, and Nataliia Kotenko are with State University of Trade and Economics, Kyiv, Ukraine (e-mail: desyatko@gmail.com, zhyrova@knute.edu.ua, kotenkono@knute.edu.ua).

organization's resilience to cyber threats. Note that game models can simulate complex scenarios between attackers and defenders, for example, when allocating financial resources (FRs) between the parties to the confrontation. Each side - the defenders and the attacking hackers - allocates their FRs to achieve their own goals: the defenders invest in strengthening security measures and preventing attacks, while the attackers invest in developing and using new methods to penetrate and bypass defenses. Such models can help analyze the strategies of both attackers and defenders and predict their behavior under different conditions. All of the above predetermined our interest in this aspect of the APT attack problem.

II. LITERATURE REVIEW

Research aimed at analyzing and preventing Advanced Persistent Threat (APT) attacks has been ongoing for many years. These works cover a wide range of techniques and approaches, from early attempts to detect such attacks based on signature-based methods [5] to state-of-the-art solutions using machine learning [6, 7] and deep neural networks [8, 9]. In particular, applying graph convolutional neural networks (CNN) [10] for modeling complex relationships and detecting anomalies in network data demonstrates significant progress in this area. Hybrid analysis techniques [11] combining static and dynamic analysis [2, 12] have also proven effective in identifying complex malware associated with APT attacks [2, 13, 14].

Game theory has significant potential for improving critical infrastructure design (CID). It represents a mathematical model for analyzing conflict and cooperation between the parties (players) involved in an APT attack or its stages. Game models allow for formalizing the interaction between attackers and defenders, which provides a deep understanding of their motivation and behavior. Many authors use game theory to analyze APT attacks in their research [15, 16, 17, 18, 19]. This approach allows modeling and predicting the actions of both attackers and defenders in different scenarios. Note that game models help to determine the optimal strategies for both sides, which is especially important in the presence of limited resources. For example, attackers can rationally allocate their resources between reconnaissance, attack, and concealment of their actions, while defenders can efficiently allocate their resources to monitoring, defense, and incident response. The use of game theory allows us to consider the dynamic and multi-stage nature of APT attacks, where each action by one party affects the possible reactions of the other. Game theory helps to develop strategies that minimize risks and losses from attacks and optimize defense costs. In addition, such models can educate cybersecurity professionals by allowing them to train in conditions as close to the real world as possible.

In [15], the authors analyzed information security using game theory methods. In particular, they investigated how companies can decide whether to invest in defense measures or insurance against losses in case of cyberattacks. The work considered different strategies of attackers and defenders and evaluated the financial costs of the parties and the potential benefits. The authors also proposed models for optimal resource allocation between defense measures and insurance, demonstrating how these decisions can affect a company's overall resilience to cyber threats.

In [16], the risk management problem in CS considers the game theory methods. The authors propose a model that helps organizations evaluate and allocate resources to defend against cyber threats. In particular, the study focuses on the interactions between attacking and defending parties by analyzing their strategies and behaviors. The model considers both direct and indirect costs of cyberattacks and potential losses and consequences for organizations.

In [17], the authors explore decision-support methods for cybersecurity investments. Using various game theory approaches and models, they examine how organizations can optimally allocate resources to defend against cyber threats. The study focuses on the cost-benefit analysis of different security strategies and the assessment of the risks and consequences of cyberattacks.

In [18], the authors conduct an in-depth study of strategies in security games by comparing Stackelberg and Nash models. The study focuses on three key aspects: interchangeability (examines whether the strategy of one model can be transformed into equivalent strategies of the other model without loss of efficiency); equivalence (studied the case where different models lead to the same results in terms of optimal strategies); uniqueness (analyzed scenarios where the solutions obtained from one model are unique. Or there are many equivalent solutions). The authors conduct a theoretical and empirical analysis, showing that the Stackelberg and Nash models can be interchangeable in some contexts but only sometimes produce the same results. They demonstrate that the choice between these models depends on the specific conditions and parameters of the security game. The study also highlights the importance of proper model selection for optimizing security strategies to provide maximum protection at minimum cost.

In [19], the authors reviewed the game theory methods applied in CS, looking at different game models and strategies used to analyze and solve problems related to cyber threats. The authors categorize the existing approaches based on various game theories, such as noncooperative games, cooperative games, Stackelberg games, and dynamic games. The authors also discuss the practical application of these techniques in real-world cybersecurity scenarios, such as protecting network infrastructure, preventing DDoS attacks, managing risks, and developing optimal defense strategies. The paper provides examples of successful applications of game-theoretic methods to improve information system protection effectiveness and minimize cyberattack risks.

In [16, 17, 18], the authors focus on the computation of Nash equilibrium in the game "attacker-defender" strategies. In [19], a rational scheme for obtaining an advantage of the defender over the attacker is described. However, these studies, like [15], do not consider how the choice of strategies for complex, long-term, and multi-stage APT attacks affects the costs of the game participants. The issue of rational investment in offense and defense needs to be addressed. This is the reason for our interest in this topic.

Our paper proposes a solution to this problem using game theory. For this purpose, we apply the method of infinite antagonistic games, which allows us to find optimal mixed strategies of players. This method allows us to adequately distribute the FRs of both the defense and attacker sides during APT attacks.

III. Aims and Objectives of the Study

This paper provides a mathematical multifactor model for countering targeted attacks, considering the parties' financial resources (FR) in the framework of an infinite antagonistic game.

To achieve the goal, the following objectives were addressed:

1. *Development of a model based on an infinite antagonistic game to search for optimal players' mixed strategies while analyzing the situation with the distribution of FRs to counter the APT attack.*
2. *Approbation of the model in the process of computational experiments.*

IV. Multifactor Model of Counteraction to Targeted Attacks Taking into Account the Financial Resources of the Parties in the Framework of an İnfinite Antagonistic Game. Problem Statement

With the continuous increase in the dependence of companies' and organizations' business processes on IT, both attackers and defenders are constantly adapting their strategies in response to each other's actions. In our view, the infinite antagonistic game model proposed below reflects this dynamic nature of the conflict, allowing players (defender and attacker) to adjust their strategies, including those based on available FRs, over time, based on observations and changes in the other side's behavior. Note that when analyzing the distribution of FRs, it is essential to consider that both attackers and defenders (i.e., players) can change their costs and investments in response to the actions of the opposing side. In this case, an infinite antagonistic game will allow us to model this iterative process of FR allocation, which will help us find the most efficient strategies to minimize costs and maximize defensive efficiency. In the infinite antagonistic game, each side must seek to mitigate losses and maximize gains throughout the conflict. This well reflects the reality of confrontation in cyberspace, where both sides constantly try to outdo each other.

Let's set the stage with a problem statement about counteracting a party that seeks to damage a structure (corporation, company, etc). We'll use the OIS (object of information security) abbreviation to refer to the victim of an APT attack. The OIS, in this context, is the first player, the victim of an APT attack. The second player is the hackers who seek to damage the OIS using an APT attack. We're specifically referring to a certain number of hackers, as APT attacks are often complex and multi-step operations requiring various skills and significant resources. A single hacker rarely possesses the full range of skills and time needed to conduct such attacks. Instead, groups of hackers or teams utilize their different skills to execute the attack successfully. APT attacks typically involve specialists from various fields: reconnaissance, exploit development, malware delivery and exploitation, etc. Each task requires specific expertise, making it necessary to employ multiple hackers or even entire teams to execute the attacks effectively. As shown above, APT attacks are often supported by whole organizations or government entities that can provide the necessary infrastructure and resources, including teams of analysts, developers, operators, and other specialists working in a coordinated manner to achieve the overall goals of the APT attack. In addition, using multiple hackers in an attack helps spread the risk. If one hacker is detected or caught, it won't necessarily cause the entire operation to fail, as other participants can continue the attack or adjust the strategy in real time.

We assume that the first player (defense side) has strategies. In the context of distributing FRs to defend against APT attacks, the defense side can use multiple strategies, e.g.:

- *investments in preventive measures aimed at preventing attackers from penetrating the system (vulnerability assessment and penetration testing, etc.);*
- *investments in detective measures aimed at detecting and identifying attackers after penetration of OIS systems (implementation of Intrusion detection systems (IDS) and intrusion prevention systems (IPS), logging and monitoring, user behavior analytics (UBA), etc.);*
- *investments in reactive measures to minimize damage and rapid recovery from detecting APT attacks (funding comprehensive incident response plans, including recovery and communication scenarios, etc.).*

We also assume the second player (the attacking party - hackers) has strategies. In the context of distributing FRs to realize APT attacks, attackers can use their strategy, e.g.:

- *Multi-stage and multi-vector penetration, which involves using different attack vectors to penetrate a system gradually (this can include launching carefully planned phishing attacks to gain initial access;*
- *investing in the purchase or development of exploits for zero-day vulnerabilities that have not yet been identified and patched;*
- *penetrating through less secure partners or vendors who may have access to the target system);*
- *privilege analysis and escalation, where after the initial penetration, attackers can focus on escalating their privileges on the system (investing in malware that can stealthily operate on the system and collect data for further privilege escalation; moving between different network segments to find and exploit privileged accounts or vulnerabilities, establishing persistence, etc.);*
- *dynamic resource allocation, which implies flexible and adaptive resource allocation depending on the current situation (investing in the development of models and simulations that will help predict the behavior of the defending party and adapt attacks accordingly; using analytical tools to monitor the defending party's response and adjust the attack accordingly, etc.);*
- *the factor of human exploitation, which includes the use of social engineering techniques and other human error approaches (investing resources in bribing employees of the target organization or using blackmail to gain access to systems; hiring or manipulating internal employees to gain access or information needed to successfully conduct an attack, etc.).*

Suppose that in a situation due to a conflict (i.e., an APT attack) between the OIS and the side attacking the OIS, the second player (the hacker player) has applied his i-strategy. Using this strategy, he causes a financial loss to the first player in the amount of μ_i. Further, let the first player (the victim player, the defense side of the OIS) apply his j-strategy. Applying this strategy brings him a financial addition in the amount of η_j.

For example, organizations that effectively protect their information assets from APT attacks may become more attractive to investors, as investors prefer to invest in companies that demonstrate high protection against cyber threats.

We can explain this by the fact that the second player's FR of the second player, which goes to his expenses, will decrease by this amount. Let us denote by w_{ij}^1 the ratio μ_i / η_j, and by w_{ij}^2 the ratio η_j / μ_i. If $\mu_i = 0$ at some *i* or $\eta_j = 0$ at some *j*, we exclude such strategies from consideration. Let us denote by W_1 the matrix consisting of the elements of w_{ij}^1. The number of rows corresponds to the number of alternatives of the malicious player, and the number of each row corresponds to the corresponding alternative of the malicious player. Through W_2 we denote the matrix where the rows correspond to the options of the victim player, and the columns correspond to the alternatives of the attacker player, i.e. the elements w_{ij}^2 mean that they are in the row *j* and int the column *i*.

Let's introduce the notations:

- σ_j $(j = 1,..., m)$ - elements of the diagonal matrix Σ of order *m*: $\sigma_j \geq 0, \sum_{j=1}^{m} \sigma_j = 1$. The matrix Σ characterizes the "structure" of expenses (losses) of the second player. The element σ_j means the share of *j* component of the value of the set of incomes of the first player, which is transformed into *j* component of the value of the set of expenses of the second player. This means the following. If there is a set of incomes of the first player $(\xi_1,..., \xi_n)$, then the set of incomes of the first player equal to $\sigma_j \cdot (\xi_1,..., \xi_n)$ is "transformed" into *j* component of the value of the set of expenses of the second player;

- h_j $(j = 1,..., n)$ elements of the diagonal matrix *H* of order *n*: $h_j \geq 0, \sum_{j=1}^{n} h_j = 1$. The matrix *H* characterizes the "structure" of the income set of the first player. The element h_i means the share of *j* component of the value of the set of expenditures of the second player, which is "transformed" into *j* component of the value of the set of incomes of the first player. This means the following. If there is an expenditure set of the second player $(\theta_1,..., \theta_m)$, then the expenditure set of the second player equal to $h_j \cdot (\omega_1,..., \omega_m)$ is "transformed" into *j* component of the value of the first player's income set.

Note, if there is a set of revenues $\xi = (\xi_1,..., \xi_n)$ of the first player, then the operation $W_1 \cdot \xi$ gives the *m*-dimensional vector that would have to stand for the set of expenditures of the second player. In fact, this product makes it possible to determine only one component of this *m*-dimensional vector (the second player), since the entire vector $\xi = (\xi_1,..., \xi_n)$ will be "spent" on this component alone. For the other components of the second player's set of expenditures, there is no more set of revenues of the first player that would be "equivalent" to that component of the second player. The entire revenue set of the first player has already been spent, "gone" to "equalize" in efficiency with one component of the second player's cost set. Therefore, it is necessary to split the income set into *m* parts, so that it would be possible to "equalize" the efficiency of the second player's expenditure sets for all its components with the income shares. For this purpose, a set of elements is introduced σ_j.

Here's an example. Suppose a defender has 100 units of income, and he decides to spend all of these resources (in our variant - FR) on defense against one specific component of an attack (for example, a DDoS attack). This means that he used all of his resources (100 units) to defend against only one specific attack. Then the defender no longer has resources that he can use to protect against other types of attacks within APT attacks. And let the attacker have 200 units of resources spread across multiple attack components (e.g., DDoS attack, phishing attack, and software attack). Even if the defender successfully defends one element of the attack, the attacker still has resources for other types of attacks. Accordingly, to effectively counter all components of APT attacks, the defender needs to compartmentalize its resources to cover all kinds of attacks by the attacker. For example, a defender can divide his 100 units into four parts of 25 units each and allocate them to 4 different defense components. In this way, he will be able to defend against several types of attacks, although not as effectively as if he concentrated all his resources on a single attack. Actually, for this purpose, a set of elements (or parts) are introduced that allow the defender to break down his resources and distribute them to all components of the attacker's attacks. This allows for a more efficient use of resources and the ability to counter multiple types of attacks.

The same is true for the second player's set of costs.

The conflict interaction goes like this.

The first player, having at the moment of time $t = 0$ $\xi(0) \in R_+^n$ FRs transforms them to the value of resources $\Delta \cdot \xi(0)$. Here Δ is the matrix of transformation of FR resources of the first player of order *n*, with positive elements. Next, he makes his strategic investment move in CS resources by choosing the value of his investment $u(0) \cdot L_1 \cdot \lambda(0)$. Here $u(0)$ is the value: $0 \leq u(0) \leq 1$, which determines the share of the vector $\Delta \cdot \xi(0)$, going to the defense against APT attacks. This investment of the first player means that it allows him to compensate $\Sigma \cdot W_1 \cdot u(0) \cdot \Delta \cdot \xi(0)$ for losses from the actions of the second player.

The second player acts in the same way.

The second player, having at the moment of time $t = 0$ $\omega(0) \in R_+^m$ FRs transforms them to the value of resources $\Omega \cdot \omega(0)$. Here Ω is the FR transformation matrix of the second player of order *m*, with positive elements. Then he makes his strategic investment move by choosing the value of his investment $v(0) \cdot \Omega \cdot \omega(0)$. Here $v(0)$ is the value: $0 \leq v(0) \leq 1$, which determines the share of the vector $\Omega \cdot \omega(0)$, which goes to conduct the APT attack.

This investment of the second player means that it allows to compensate $H \cdot W_2 \cdot v(0) \cdot \Omega \cdot \omega(0)$ income of the first player (to reduce it by this value).

Then the players' FRs at time $t = 1$ satisfies the following system of equations:

$$\begin{aligned} \xi(1) &= \Delta \cdot \xi(0) - u(0) \cdot \Delta \cdot \xi(0) - H \cdot W_2 \cdot v(0) \cdot \Omega \cdot \omega(0); \\ \omega(1) &= \Omega \cdot \omega(0) - v(0) \cdot \Omega \cdot \omega(0) - \Sigma \cdot W_1 \cdot u(0) \cdot \Delta \cdot \xi(0). \end{aligned} \quad (1)$$

Let's introduce the notations:

$$M_0 = \bigcup_{i=1}^{m} \{(\xi, \omega) : (\xi, \omega) \in R^{n+m}, \xi \geq 0, \omega_i \prec 0\},$$

$$N_0 = \bigcup_{i=1}^{n} \{(\xi, \omega) : (\xi, \omega) \in R^{n+m}, \xi_i \prec 0, \omega \geq 0\},$$

$$K_0 = \{\bigcup_{i=1}^{n} \{(\xi, \omega) : (\xi, \omega) \in R^{n+m}, \xi_i \prec 0\}\} \cap \{\bigcup_{i=1}^{m} \{(\xi, \omega) : (\xi, \omega) \in R^{n+m}, \omega_i \prec 0\}\},$$

$$L_0 = R_+^{n+m}.$$

There are 4 possible cases at the time $t = 1$:

1) $(\xi, \omega) \in M_0$;
2) $(\lambda, \theta) \in F_0$;
3) $(\xi, \omega) \in K_0$;
4) $(\xi, \omega) \in L_0$.

The first case is desirable for the first player. The second case is desirable for the second player. The third and fourth cases are "neutral" for the players, i.e. they are not a priority for the players, which, as it is shown below, is expressed in the fact that the payoff function (winnings) in the considered infinite antagonistic game is assumed to be equal to zero. Players are not interested in the possibility of further interaction in time; their goals are to achieve their desired outcomes already at time *t = 1*. This means that they tend to choose their investment strategies in such a way that they can achieve their goals in a one-step interaction. To do so, they need to solve an infinite antagonistic game in standard form, which is formalized as follows. Let us denote by *U* and *V* the unit segment [0, 1] , by *F* the function on $U \times V$ with values in *R*:

$$F(u,v) = \begin{cases} +1, (\xi(u,v), \omega(u,v)) \in M_0; \\ -1, (\xi(u,v), \omega(u,v)) \in N_0; \\ else,\ 0; \end{cases}$$

Then the infinite antagonistic game is written as follows: *G = <U, V, F>*. In the game under consideration, there are no optimal pure strategies, but the value of the game obj and the optimal mixed strategy exist.

Let's introduce the notations.

$$d_i = (H \cdot W_2 \cdot \Omega \cdot \omega(0)) / (\Delta \cdot \xi(0)), i = 1,...,n;$$

$$c_j = (\Omega \cdot \omega(0)) / (\Sigma \cdot W_1 \cdot \Delta \cdot \xi(0)),\ j = 1,...,m.$$

Let condition 1 be satisfied.

Condition 1.

$$d_i \leq 1, i = 1,...,n; \quad c_j \leq 1,\ j = 1,...,m.$$

Consider a pair of equations. One equation corresponds to the i_0 component of the variable ξ, and the other equation corresponds to the j_0 component of the variable ω. Let's denote.

$$u_1^{i_0} = [1 - d_{i_0}], v_1^{j_0} = 1;$$

$$u_2^{i_0} = [1 - v_2^{j_0} \cdot d_{i_0}],\ v_2^{j_0} = [1 - u_1^{i_0} / c_{j_0}];$$

... ...

$$u_n^{i_0} = [1 - v_n^{j_0} \cdot d_{i_0}],\ v_n^{j_0} = [1 - u_{n-1}^{i_0} / c_{j_0}].$$

If condition 1 is satisfied, then the sequences $u_n^{i_0}$, $v_n^{j_0}$ will have no limit, i.e. there will be a finite number of such elements.

In case condition 2 is satisfied for some pairs of indices (i, j) : $d_i \succ 1, c_j \geq 1$ or $d_i \succ 1,\ c_j \geq 1$, then there will be an infinite number of elements $u_n^{i_0}$, $v_n^{j_0}$ and they will have limits.

It is not difficult to see that the sequences so formed are the carriers of the players' optimal mixed strategies [20, 21] and thus the inequality: $u_n^{i_0} \geq c_{j_0}$, defines the set of initial states (ξ, ω), from which the first player can reach his outcome in one step, at least with probability $1/n$, when he applies his optimal mixed strategy (probability measure) centered at the points: $u_1^{i_0}, u_2^{i_0}, \ldots, u_n^{i_0}$. The optimal mixed strategy of the second player will be the probability measure that is centered at the points: $v_1^{j_0}$, $v_2^{j_0}, \ldots, v_n^{j_0}$. In this case, the players' choice of these points is made with probability $1/n$.

It should be noted that if we subtract from this set the set of player states from which players achieve the outcome with probabilities at least: $1, 1/2, \ldots, 1/(n-1)$, then we obtain the set of states (ξ, ω), which have the property that if the interaction starts from these states, then when players apply their optimal strategies, they will obtain a result (the value of the infinite antagonistic game) equal to $1/n$.

Note that a pair of equations has been considered. Each such pair "generates" an infinite antagonistic game. There are $n \times m$ such pairs of equations. In each such infinite antagonistic game, we similarly find the optimal mixed strategies of the players and the sets in which the result is achieved with probability *1 / n*, if the carrier of the optimal mixed strategy consists of *n* points.

Note that in case the initial interaction states belong to two or more sets in which the solution of the corresponding antagonistic game is found (when considering some pairs of equations), the values of these games coincide.

To give an example, let us give an infinite antagonistic game generated by the interaction of players whose states are positive integers. Let us give the equations of interaction.

$$\begin{aligned} \xi(1) &= \delta \cdot \xi(0) - u(0) \cdot \delta \cdot \xi(0) - h \cdot w_2 \cdot v(0) \cdot \varpi \cdot \omega(0); \\ \omega(1) &= \varpi \cdot \omega(0) - v(0) \cdot \varpi \cdot \omega(0) - \sigma \cdot w_1 \cdot u(0) \cdot \delta \cdot \xi(0). \end{aligned}$$

Let's denote: $r_1 = \sigma \cdot w_1$, $r_2 = h \cdot w_2$. $g_1 = \delta$, $g_2 = \varpi$

In the case of $r_1 \cdot r_2 \prec 1$ we have:

$$v^* = \begin{cases} -1, \omega(0) \geq 0, r_2 \cdot g_2 \cdot \omega(0) \succ (1 + r_1 \cdot r_2) \cdot g_1 \cdot \xi(0), \\ -1/2, \omega(0) \geq 0, r_2 \cdot g_2 \cdot \omega(0) \leq [1 + r_1 \cdot r_2] \cdot g_1 \cdot \xi(0), r_2 \cdot g_2 \cdot \omega(0) \succ \\ \succ [1 + r_1 \cdot r_2 + (r_1 \cdot r_2)^2] / [1 + r_1 \cdot r_2] \cdot g_1 \cdot \xi(0), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -1/k, \omega(0) \geq 0, r_2 \cdot g_2 \cdot \omega(0) \leq [1 + \ldots + (r_1 \cdot r_2)^{k-1}] / [1 + \ldots + (r_1 \cdot r_2)^{k-2}] \cdot g_1 \cdot \xi(0), r_2 \cdot g_2 \cdot \omega(0) \succ \\ \succ [1 + \ldots + (r_1 \cdot r_2)^k] / [1 + \ldots + (r_1 \cdot r_2)^{k-1}] \cdot g_1 \cdot \xi(0), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0, \xi(0) \geq 0, r_2 \cdot g_2 \cdot \omega(0) \leq g_1 \cdot \xi(0), g_2 \cdot \omega(0) \geq r_1 \cdot g_1 \cdot \xi(0), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 1/k, \xi(0) \geq 0, g_2 \cdot \omega(0) \geq [1 + \ldots + (r_1 \cdot r_2)^{k-2}] / [1 + \ldots + (r_1 \cdot r_2)^{k-1}] \cdot g_1 \cdot r_1 \cdot \xi(0), g_2 \cdot \omega(0) \prec \\ \prec [1 + \ldots + (r_1 \cdot r_2)^{k-1} / [1 + \ldots + (r_1 \cdot r_2)^k] \cdot g_1 \cdot r_1 \cdot \xi(0), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 1/2, g_2 \cdot \omega(0) \geq [1/(1 + r_1 \cdot r_2)] \cdot r_1 \cdot g_1 \cdot \xi(0), g_2 \cdot \omega(0) \succ \\ \succ [1 + r_1 \cdot r_2] / [1 + r_1 \cdot r_2 + (r_1 \cdot r_2)^2] \cdot r_1 \cdot g_1 \cdot \xi(0), \\ 1, \quad \xi(0) \geq 0, g_2 \cdot \omega(0) \prec (1/(1 + r_1 \cdot r_2)) \cdot r_1 \cdot g_1 \cdot \xi(0), \\ 0, \xi(0) \prec 0, \omega(0) \prec 0. \end{cases} \quad (2)$$

In the case of $r_1 \cdot r_2 \geq 1$, the entry for the game value v^* differs only in the entry of the region in the players' FR space in which $v^* = 0$. This region will be recorded as follows:

$$\omega(0) \geq 0, \ r_1 \cdot g_1 \cdot \xi(0) \geq g_2 \cdot \omega(0), \ r_2 \cdot g_2 \cdot \omega(0) \geq g_1 \cdot \xi(0). \quad (3)$$

The optimal mixed strategies of the players will be probability measures with carriers consisting of a finite number of points. In this case, if the value of the game is equal to $\pm 1/k$, then the carrier of such probability measures counts k points. At the points, the value of each player's probability measure is equal to $1/k$.

The notation for the carrier points of these probability measures, which are the optimal mixed strategies of the players, in the case where the value of the game is positive and equal to $1/k$, is such:

$$\begin{aligned} & u_1^* = 1 - (r_2 \cdot g_2 \cdot \omega(0)) / (g_1 \cdot \xi(0)), v_1^* = 1, \\ & u_2^* = [1 + r_1 \cdot r_2] \cdot [1 - (r_2 \cdot g_2 \cdot \omega(0)) / (g_1 \cdot \xi(0))], v_2^* = \\ & (1 + r_1 \cdot r_2) - (r_1 \cdot g_1 \cdot \xi(0)) / (g_2 \cdot \omega(0)), \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & u_k^* = [1 + \ldots + (r_1 \cdot r_2)^{k-1}] \cdot [1 - (r_2 \cdot g_2 \cdot \omega(0)) / (g_1 \cdot \xi(0))], v_k^* = \\ & [1 + \ldots + (r_1 \cdot r_2)^{k-1}] - [1 + \ldots + (r_1 \cdot r_2)^{k-2}] \cdot (r_1 \cdot g_1 \cdot \xi(0)) / (g_2 \cdot \omega(0)), \ k \geq 3. \end{aligned} \quad (4)$$

If the value of the game is negative, the entry for the carrier points of optimal mixed strategies is symmetric. Namely, we need to change index 1 to 2 and variables $\xi(0)$ to $\omega(0)$ and u_k^* to v_k^*.. In the case where $v^* = 0$ optimal pure strategies exist, When

$$\begin{aligned} & r_1 \cdot r_2 \prec 1, \ g_1 \cdot \xi(0) \geq r_2 \cdot g_2 \cdot \omega(0), \ g_2 \cdot \omega(0) \geq r_1 \cdot g_1 \cdot \xi(0) \\ & u_1^* = [1/(1 - r_1 \cdot r_2)] \cdot [1 - (r_2 \cdot g_2 \cdot \omega(0)) / (g_1 \cdot \xi(0))], \\ & v_1^* = [g_1 \cdot \xi(0) / (r_2 \cdot g_2 \cdot \omega(0))] \cdot [1 - (1/(1 - r_1 \cdot r_2)) \cdot (1 - (r_2 \cdot g_2 \cdot \omega(0)) / (g_1 \cdot \xi(0))] \end{aligned} \quad (5)$$

In the same way the optimal pure strategies are determined at

$$r_1 \cdot r_2 \succ 1, \ r_1 \cdot g_1 \cdot \xi(0) \geq g_2 \cdot \omega(0), \ r_2 \cdot g_2 \cdot \omega(0) \geq g_1 \cdot \xi(0) \quad (6)$$

At $r_1 \cdot r_2 = 1$ the optimal pure strategy of the players are $u_1^* = 0, v_1^* = 0.$

Thus, we find the value of the infinite antagonistic game and optimal mixed strategies of players when the interaction of players is given by multivariate variables. For the case of univariate variables, the complete analytical solution of the problem is provided. On univariate variables (states of players, which are numbers), it is illustrated that the absolute value of the game characterizes the degree of risk of players achieving the goal when they apply optimal mixed strategies.

V. Computational Experiment

The computational experiments were performed using the PyChar distribution. For the experiment, the sizes of the set of players' strategies, the winning functions, and the rules of distribution of the defense and attackers' FRs were determined. The model was implemented in the algorithmic language Python using the libraries: NumPy, SciPy, and Matplotlib. During a series of computational experiments, data on the values of the winning functions and optimal strategies for each experiment were collected.

VI. Results of Computational Experiments

The computer simulation allowed us to visualize the results of the game. Within the framework of the article only two cases are considered: $r_1 \cdot r_2 \succ 1$ and $r_1 \cdot r_2 \leq 1.$, respectively, Fig. 1 and 2.

Case study $r_1 \cdot r_2 \succ 1.$

Figure 1 shows the sets of constants of the game value in the region where the first player has an advantage in the interaction parameters. This advantage allows him to reach his goal with some probability level, which coincides with the value of the infinite antagonistic game. The second player cannot do it in this region.

In the second case, see Fig. 2, the case $r_1 \cdot r_2 \leq 1$ considers such a set of input data: $\xi^*(0) = 1, \quad \omega^*(0) = 13, \quad g_1 = 2, \quad g_2 = 1/4,$ $r_1 = 1/2, \quad r_2 = 1 \cdot$

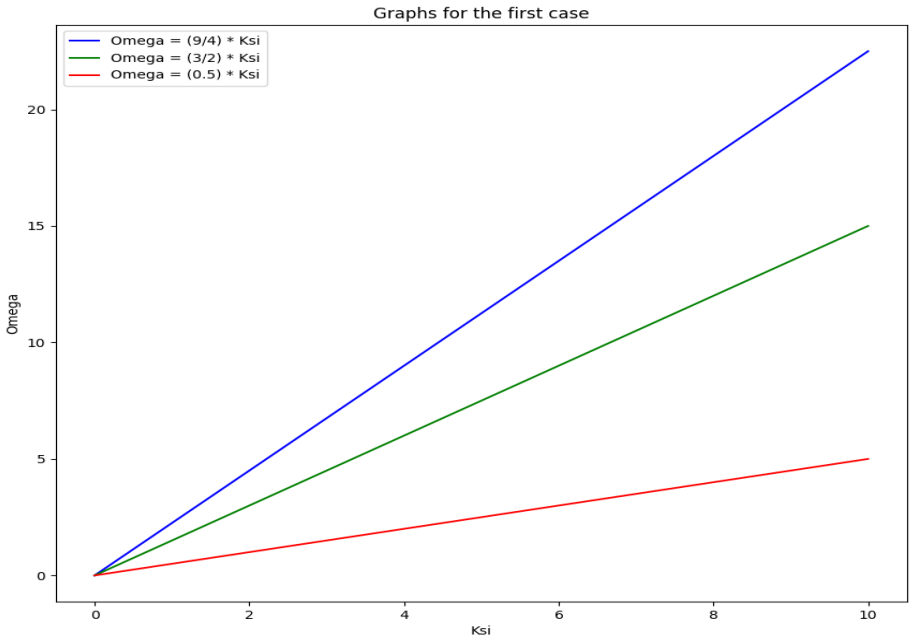

Fig. 1. Case study $r_1 \cdot r_2 \succ 1.$ (Source: created by the author)

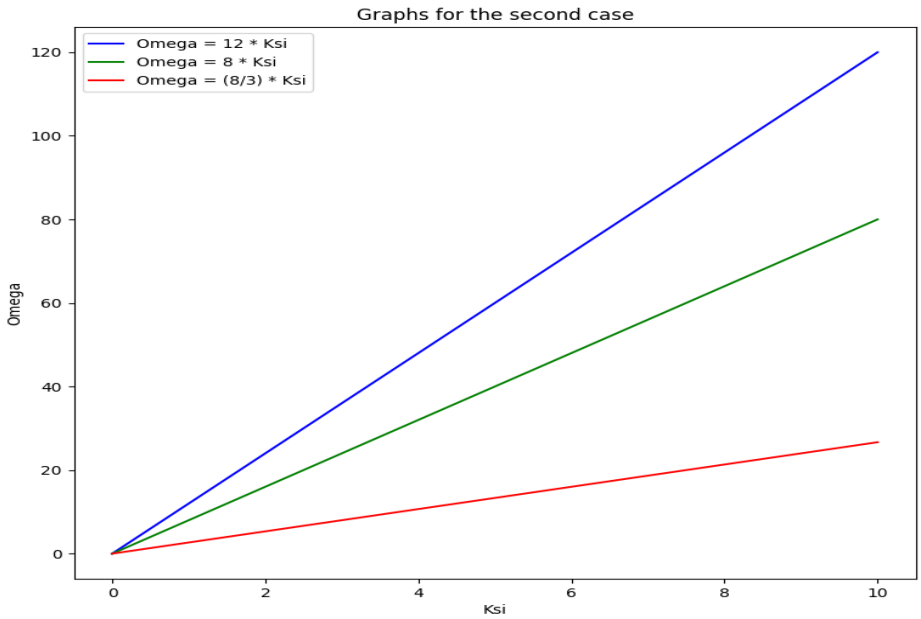

Fig. 2. *Case study* $r_1 \cdot r_2 \leq 1.$ *(Source: created by the author)*

Within the framework of the paper, we considered the situation when, in the case of a multifactor problem, predetermined by the dimensionality of the FR, it was possible to find a solution to an infinite antagonistic game in analytical form. The sets of constants of the value of the game, in this case, are "constructed" in multidimensional spaces, which is not a simple task; however, as well as finding optimal mixed strategies. When illustrating the work results, we stopped only on two cases in the two-dimensional case because they represent the most common situations in the parties' interaction in APT attacks. Note that the results of the interaction of players depend on many parameters. If the obtained result does not satisfy the players, they can change the strategy to get an acceptable result or change the interaction parameters.

VII. Discussion of the results of experimental studies

Figure 1 illustrates a situation in which the first player cannot find the optimal pure strategy that will allow him to achieve his goal with probability 1. However, he has an optimal mixed strategy that will allow him to achieve it with probability ½.

For every set of constant game values, players have optimal mixed strategies. For example, if there is the following set of input data: $\xi^*(0)=7,\ \omega^*(0)=4,\ g_1=3,\ g_2=4,$ $r_1=2,\ r_2=1$, then given this set of inputs, players have optimal mixed strategies μ^*,η^*. The measure μ^* is centered at the points: $u_1^*=5/21,\ u_2^*=5/7.$ The measure η^* is centered at the points: $v_1^*=1,\ v_2^*=3/8.$ The measures μ^*,η^*. take a value equal to (1/2) at these points. The value of the game v^*, when players apply optimal strategies, is (1/2).

This means that, given specific parameters and strategies, the defender can achieve his goal with a probability that corresponds to the value of the infinite antagonistic game. The particular task of analyzing and allocating FRs in dealing with the threat of APT attacks can be explained as follows: In a domain where the defender has an advantage, it can allocate its FRs with utmost efficiency. This advantage may manifest in more efficient use of available means to prevent or minimize damage from APT attacks, ensuring the defender's preparedness. The ability to achieve its goal with some level of probability means that the defender can predict the success of its defensive measures. This prediction is based on the value of the infinite antagonistic game, which reflects the effectiveness of the defender's optimal strategies against the attacker's possible actions. The value of the infinite antagonistic game helps the defender determine the optimal strategy for allocating his FRs. This includes both allocating FRs to cyber defense enhancements and investing in threat detection and response systems.

Figure 2 illustrates a situation where the second player achieves his goal by applying his optimal pure strategy.

In this case, the players have optimal pure strategies. The first player's optimal pure strategy is . The second player's optimal pure strategy is . The second player's significant advantage in FR and the combination of parameters explain their optimal pure strategies. The second player reaches the goal with probability 1. His advantage in the value of FR was the main factor contributing to this.

Within the framework of the paper, we considered the situation when, in the case of a multifactor problem predetermined by the dimensionality of the FR, it was possible to find a solution to an infinite antagonistic game in analytical form. The sets of constants of the value of the game, in this case, are "constructed" in multidimensional spaces, which is not a simple task. However, it also involves finding optimal mixed strategies. When illustrating the work results, we stopped only on two cases in the two-dimensional case because they represent the most common situations in the parties' interaction in APT attacks. Note that the results of the interaction of players depend on many parameters. If the obtained result does not satisfy the players, they can change the strategy to get an acceptable result or change the interaction parameters.

Conclusion

A multifactor model is developed to counter targeted attacks, considering the parties' financial resources (FRs) in an infinite antagonistic game framework. The model helps to make rational decisions on allocating FRs for cybersecurity (CS) under the threat of APT attacks. Based on the infinite antagonistic game, it finds optimal strategies for players to utilize the financial resources of information security entities efficiently. The model allows us to determine the value of the game and estimate the degree of risk in using optimal mixed strategies for FRs. This is useful for analyzing the financial aspects of countering APT attacks on information security objects. The computational experiments visualize the game's results, which is valuable for cybersecurity analysts.

References

[1] Askar, A. J. (2019). Healthcare management system and cybersecurity. International Journal of Recent Technology and Engineering, 237-248.

[2] Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing, 14(7), 9355-9381.

[3] Avram, M. C. (2014). AN Open source analysis regarding the latest developments in china 's cyberwarfare and espionage strategy. The complex and dynamic nature of the security environment, 356.

[4] Plachkinova, M., & Maurer, C. (2018). Security breach at target. Journal of Information Systems Education, 29(1), 11-20.

[5] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877.

[6] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.

[7] Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137.

[8] Shang, L., Guo, D., Ji, Y., & Li, Q. (2021). Discovering unknown advanced persistent threat using shared features mined by neural networks. Computer Networks, 189, 107937.

[9] Alrehaili, M., Alshamrani, A., & Eshmawi, A. (2021, December). A hybrid deep learning approach for advanced persistent threat attack detection. In Proceedings of the 5th International Conference on Future Networks and Distributed Systems (pp. 78-86).

[10] Li, Z., Cheng, X., Sun, L., Zhang, J., & Chen, B. (2021). A hierarchical approach for advanced persistent threat detection with attention-based graph neural networks. Security and Communication Networks, 2021(1), 9961342.

[11] Chakkaravarthy, S. S., Vaidehi, V., & Rajesh, P. (2018). Hybrid analysis technique to detect advanced persistent threats. International Journal of Intelligent Information Technologies (IJIIT), 14(2), 59-76.

[12] Su, Y., Li, M., Tang, C., & Shen, R. (2015, December). A framework of APT detection based on dynamic analysis. In 2015 4th National Conference on Electrical, Electronics and Computer Engineering (pp. 1047-1053). Atlantis Press.

[13] Laurenza, G., Lazzeretti, R., & Mazzotti, L. (2020). Malware triage for early identification of advanced persistent threat activities. Digital Threats: Research and Practice, 1(3), 1-17.

[14] Chen, W., Helu, X., Jin, C., Zhang, M., Lu, H., Sun, Y., & Tian, Z. (2020). Advanced persistent threat organization identification based on software gene of malware. Transactions on Emerging Telecommunications Technologies, 31(12), e3884.

[15] Grossklags, J., Christin, N., & Chuang, J. (2008, April). Secure or insure? A game-theoretic analysis of information security games. In Proceedings of the 17th international conference on World Wide Web (pp. 209-218).

[16] Musman, S., & Turner, A. (2018). A game theoretic approach to cyber security risk management. The Journal of Defense Modeling and Simulation, 15(2), 127-146.

[17] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision support systems, 86, 13-23.

[18] Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., & Tambe, M. (2011). Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. Journal of Artificial Intelligence Research, 41, 297-327.

[19] Wang, Y., Wang, Y., Liu, J., Huang, Z., & Xie, P. (2016, June). A survey of game theoretic methods for cyber security. In 2016 IEEE First International Conference on Data Science in Cyberspace (DSC) (pp. 631-636). IEEE.

[20] Lakhno V., Malyukov V., Malyukova I., Akhmetov B., Alimseitova Z., Ogan A., A neuro-game model for analyzing strategies in the dynamic interaction of participants of phishing attacks, (2024) Telkomnika (Telecommunication Computing Electronics and Control), 22 (3), pp. 645 - 656. https://doi.org/10.12928/TELKOMNIKA.v22i3.25938

[21] Chikrii A.A. Conflict controlled processes. Dordrecht; Boston; London: Springer Science and Business Media, 2013, 424 p.