BİLGİSAYAR BİLİMLERİ
VE
TEKNOLOJİLERİ DERGİSİ
JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGIES
http://dergipark.org.tr/tr/pub/bibted

Araştırma Makalesi

Siber Saldırı ve Savunmanın Matematiksel Modellemesi

Muharrem Tuncay Gençoğlu[*1]

[1]*Fırat Üniversitesi, Teknik Bilimler MYO, Elazığ, Türkiye*

Anahtar Kelimeler:
Oyun Teorisi
Siber Savunma
Siber Saldırı
Siber Güvenlik

ÖZ

Bu bildiride, siber uzayda güvenlik oyunlarının uygulanmasında simülasyon ve oyun-teorik yaklaşımları birleştiren yeni bir oyun formülasyonu önerilmiştir. Burada sunulan model, ampirik olarak türetilmiş karşı önlem etkinlik ölçütleri bağlamında rakip ve savunucu güdülerini ve hedeflerini modelleyen bir güvenlik ekonomik yaklaşımı üzerine kurulmuştur. Yaklaşım, hem rakip hem de savunma oyuncusu için en uygun strateji seçimini belirlemede iki oyunculu bir stratejik oyuna dayanmaktadır. Ayrıca, sadece oyunun çözümü değil, aynı zamanda oyun bağlamında "ya olsaydı" senaryolarının matematiksel ve grafiksel bir temsili de verilmiştir. Bu çalışmada, oyun teorik hesaplamalarının siber savaş oyunlarında etkili stratejilerin belirlenmesinde faydalı bir araç olarak hizmet edebileceği gösterilmiştir. Derinlemesine savunma güvenlik yapılandırmasında birden çok katmana nüfuz etmesi gereken senaryolar için, saldırganın ve savunma maliyetlerinin ve sızma olasılığının hesaplanması, maliyet-fayda matrislerinin ve olasılık matrislerinin varlığını gerektirir. Matrislerin incelenmesi, oyuncuların oyun-teorik denge çözümlerine dayalı olarak tercih edilen stratejileri çıkarmasına izin verir. Matrisler ayrıca, potansiyel insan temelli savaş oyunu stratejileri ve karşı strateji seçimlerinin beklenen etkilerinin analiz edilmesine de yardımcı olur. Ayrıca matematiksel oyun-teorik bir form tanımlanmıştır. Bu makale, oyun-teorik hesaplamaların, siber savaşlar sırasında etkili karar verme için gerçekten nasıl yararlı bir araç sağlayabileceğini göstermektedir.

Mathematical Modeling of Cyber Attack and Defense

Keywords:
Game theory
Cyberdefense
Cyberattack
Cybersecurity

ABSTRACT

In this paper, a new game formulation is proposed that combines simulation and game-theoretical approaches to the application of security games in cyberspace. The model presented here builds upon a security economic approach that models the adversary and defender motives and goals in the context of empirically derived countermeasure efficacy metrics. The approach is based on a two-player strategic game to determine optimal strategy selection for both adversary and defender. Besides, not only the solution to the game but also a mathematical and graphical representation of "what if" scenarios in the context of the game.

In this study, it has been shown that game-theoretic calculations can serve as a useful tool for identifying effective strategies in cyberwar games. For scenarios that need to penetrate multiple layers in a defense-in-depth security configuration, the calculation of the attacker's and defensive costs and the probability of infiltration requires the presence of cost-benefit matrices and probability matrices. Inspection of the matrices allows players to deduce preferred strategies based on game-theoretical equilibrium solutions. The matrices also help in analyzing the anticipated effects of potential human-based choices of wargame strategies and counter-strategies. Also, a mathematical game-theoretical form has been defined. This paper shows how game-theoretical calculations can indeed provide a useful tool for effective decision-making during cyber wars.

[*]**Sorumlu Yazar**

[*](mtgencoglu23@gmail.coml) ORCID ID 0000-0002-8784-9634

e-ISSN: 2717-8579

Geliş Tarihi: 20/09/2021; Kabul Tarihi: 22/01/2022

1. INTRODUCTION

Today, the physical environment is rapidly leaving its place in cyberspace, so the dependence on time and space is greatly reduced. However, with the help of technology, people have become more dependent on cyberspace. This situation has led to an increase in the abuse of information systems for economic, social, political or ideological reasons. This situation, which is a very serious threat to the security of information, carries a risk that may cause loss of life and property and deterioration of the stability of the countries. It is important to analyze these risks and determine the measures that can be taken. Because cyberattacks are carried out against the critical infrastructures of the countries, it is vital to identify and implement the appropriate strategies by examining the strategies for the analysis of risks in determining defense methods (Eren vd., 2020).

An important element in the mathematical and scientific foundations for security is modeling the strategic use of information. In this modeling, game theory is very important as it has practical uses in determining optimal strategies (Kiekintveld vd., 2015). When we examine some theoretical game approaches that model the interaction between attacker and defender, we see that different games are used to examine the actions of the defender and the attacker (Do vd., 2017). One of the important elements in the scientific foundations of cybersecurity is the use of mathematical modeling in strategy determination.

The widespread use of information technology systems in the military field has changed the face of the battlefield and the nature of warfare. E.g.; It is possible to see the game between an attacker and a defender trying to gain remote access to computers and the strategic interaction in this area. There are many studies in the literature that game theory can be a solution to many problems in cyber defense. We even know that there is a lot of debate about how game theory can be applied in cyberspace (Sokri, 2019).

This study, where the sources of motivation are the issues mentioned above; is aimed to reveal the gains and losses by creating mathematical modeling over a cyberattack and defense scenario and determining the optimal strategies of the countries. For this purpose, game theory and some basic concepts will be explained in the second part of the study. In the third chapter, a scenario will be determined in which one of the two countries, A and B, expresses the offensive capabilities and the defense capabilities of the other and their strategies. Based on this scenario, a return matrix will be created by calculating the returns of countries with the help of a mathematical model. In the fourth part; By simplifying the calculated return matrix, the returns for the strategies of the countries in the scenario will be calculated and optimal strategies will be determined. Then, these strategies will be sorted out and mixed optimal strategy/strategies will be determined.

In the conclusion part, a mathematical model that determines the maximum earnings and minimum losses of the countries in the scenario will be presented. With the help of this model, numerical results will be given for the attack and defense.

The approach put forward in this paper provides the following contributions:

1. The detection of security economic models for both the attacker and the defender.
2. The introduction of a simple two-person strategic game-theoretic model using the security economic models.
3. Determining and applying optimal strategies.

2. GAME THEORY AND FORMULATION

Any event that involves combat is the game. Game theory deals with the analysis of games (Guseinov, 2010). The game theory examines decision-making issues with multiple interacting decision-makers, including adversarial situations where two or more agents have opposite goals (Kiekintveld vd., 2015). Game theory is used as a framework to model situations where there is more than one decision-maker (player) in many disciplines (Osborne, 2004, Shoham vd., 2009).

Game theory involves formulating a decision-making problem as a game where two or more players make decisions so that one player's decisions affect the decision of the other (Sanjay, 2015). The game is defined as a set of strategies and wins for each player. Players are assumed to be rational and their goal is to maximize the returns (utility) they get from participating in the game. All players expect other players to be rational as well. Rationality in general assumes perfect and complete information among players about each other's strategies and payoffs. Perfect knowledge refers to the ability to observe the actions of other players, while complete information refers to the recognition of the identity of other players involved and the response to specific strategies. In the context of incomplete information in which players do not know the strategies of their opponents, a Bayesian game based on the probability distribution of actions in the strategy set can be modeled (Harsanyi, 1967).

There are three types of return functions: zero-sum; fixed sum and nonzero-sum. In zero-sum games, one player's wins are the opposite of the other's losses. Whatever one player wins, the other must lose. This assumes that the opponent's evaluation functions are inverted. In fixed-sum games, only one player will have a non-zero payoff at any given time, and no restrictions are applied to the structure of the result in non-zero-sum games

(Aumann vd., 1995). He argues that zero-sum assumptions in cyber warfare are not reasonable because state actors have different goals and priorities (Hamilton vd., 2002). He suggests that the non-zero-sum model is the most realistic in the context of such a knowledge war (Burke, 1999).

The goal of the game is to find a balanced solution, that is, to find the best result or payoff for players that take into account the decisions of all other players. In classic optimization terms, this is a locally optimal solution to the problem for a player. One of the most basic solutions for a game is the minimum solution that minimizes the maximum expected loss of a player. Nash Equilibrium is achieved when a unique, optimal strategy is available for each player corresponding to each opponent's move (Gibbons, 1992). If the probability of choosing a strategy for a particular scenario is 1, the strategy is said to be pure. But in most cases, opponents do not have complete knowledge or are undecided about the nature of the game and a pure strategy is not clear. In this case, a stochastic model called a mixed strategy is used, in which a probability associated with certain strategies is defined.

Games can and may not be collaborative. Collaborative games are often modeled when mechanisms are available to implement certain behavior sets (resources). If cooperative strategies can be undertaken in cyber warfare, non-cooperative games can be modeled. Based on the results obtained from non-cooperative models, policy recommendations can be made to reduce cyberwar problems. The perfect knowledge also includes the concept of perfect recall or the historical knowledge of the strategies chosen by each player. While the process of building trust and negotiation in cyber warfare is expected to be excellent, cyber warfare strategy games are expected to have offensive and defensive capabilities to lack knowledge. It is assumed that only perfect knowledge can be simplified in modeled situations.

Generally, games are either static or dynamic. In static games, the decisions of all players are made at the same time, without knowing the decisions made by the other players. Dynamic games include a series of games in which strategies can be reassessed based on previous choices made by the players involved. In the context of cyber warfare, dynamic games can exist when attack tactics involve multiple steps and trials. At the same time, defense mechanisms can allow recognition of previous attacks to protect systems and affect future behavior. Therefore, ranking over time is an important component of cyber warfare Libicki, 1997). However, it is also reasonable to assume static games as many cyberattacks happen without the knowledge of the attack. We will use a static model for the scenario in this study. In the application of this model, the mathematical formulation used in solving 2xn games will be used (Guseinov, 2010).

3. CYBER OFFENSIVE AND DEFENSE SCENARIO

Algorithms that enable the making of cybersecurity decisions based on solid foundations and game models that allocate cybersecurity resources to different tasks have been developed (Andrew vd., 2014). In this section, we will compute the payoff matrix by creating a different game scenario.

Let there be two countries like A and B. These two countries are at war with each other in cyberspace. Country A has two cyber weapons (any cyber-attack method) and its purpose is to damage the targets of country B, provided that country A attacks and country B is the defender. Four networks can be used for this purpose. A can send both cyber weapons to B's targets using the same or different networks. Country B has four cyber defense systems. Its purpose is to protect itself from A's attacks. Defense systems detect and prevent cyber weapons from using the network on which they are located. If one of the defense systems is placed on any possible network that will be attacked, the cyber weapon using this network will be blocked by the defense system. If this network uses two cyber weapons, the defense system on it can block one of the weapons (attackers) and the other will reach the target. If there are two defense systems on the network where the attack is made, it will be blocked in two attacks and the target will be protected.

If country A reaches the target, its gain will be accepted as 1, if not, it will be considered as 0. Possible strategies to be used by A and B countries should be determined as follows;

I_1: Attacks are made from different networks.

I_2: Attacks are made from the same networks.

II_1: A defense system is placed on each network.

II_2: Two defense systems are placed on two networks, while the other two networks remain exposed.

II_3: While two defense systems are placed on a network and one defense system is placed on the other two networks, a network remains exposed.

II_4: Three defense systems are placed in a network, one defense system is placed in a network, while the other two networks remain exposed.

II_5: Four defense systems are placed on a network; the other three networks remain exposed.

To reveal which of these strategies are necessary, to find the payoff matrix of the mentioned cyber warfare game;

Case I:

Let's calculate the returns, namely g_{1j} (j=1,2,3,4,5) when country A attacks with strategy I_1.

Step 1:

If country A attacks with the I_1 strategy, it will send cyber weapons over different networks. So, since there are 4 networks in total, country A attacks using different networks;

$\binom{4}{2}=\frac{4!}{2!.2!}=6$, it can be realized in 6 different ways.

Step 2:

If country B defends with the II_2 strategy since there will be 1 defense system on each network, 2 of the cyberweapons in each of the 6 options of country A will be blocked. So the target will be protected. In this case, country A payoff;

$$g_{11}^{A}=g^{A}(I_1II_1)=\frac{0}{6}+\frac{0}{6}+\frac{0}{6}+\frac{0}{6}+\frac{0}{6}+\frac{0}{6}=0.$$

Step 4:

If country B defends with the II_3 strategy, there will be 2 defense systems on 1 network, one defense system on the other 2 networks, and 1 network will be open. Since each cyber-attack is carried out from different networks, the target will be achieved in 3 of the 6 options of country A, and the target will be protected in 3. Country A payoff;

$$g_{13}^{A}=g^{A}(I_1I_3)=\frac{0}{6}+\frac{0}{6}+\frac{0}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}=\frac{1}{2}.$$

5. Step:

If country B defends with the II_4 strategy, the other 2 networks will be open, 1 of which will have 3 defense systems, 1 over 1 defense system. Since cyber-attacks are carried out over different networks, the target is protected in only one of the 6 possible options of A, and the target is reached in each of the other 5 options. Country A payoff;

$$g_{14}^{A}=g^{A}(I_1I_4)=\frac{0}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}=\frac{5}{6}.$$

Step 6:

If B defends with the II_5 strategy, there will be 4 defense systems on 1 network, while the other 3 networks will be open. Since each attack takes place over different networks, in each of the A's 6 options, the attack will reach the target. A payoff;

$$g_{15}^{A}=g^{A}(I_1I_5)=\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}+\frac{1}{6}=1.$$

Case II:

Let's calculate the returns, namely g_{2j} (j=1,2,3,4,5) when country A attacks with strategy I_2.

Step 1:

If country A attacks with the I_2 strategy, since it will send both of the attack weapons from the same network and there are four networks, it can do cyber-attacks in four different ways,

$\binom{4}{1}=\frac{4!}{3!.1!}=4.$

Step 2:

If country B defends with the I_{I1} strategy, it will reach the target in each of A's 4 options in both attacks, since there will be a defense system on each network. Payoff will be

$$g_{21}^{A}=g^{A}(I_2II_1)=\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=1.$$

Step 3:

If country B defends with the II_2 strategy, it reaches the target in 2 of the 4 options of A in 2 attacks and is blocked in 2. A payoff

$$g_{22}^{A}=g^{A}(I_2II_2)=\frac{0}{4}+\frac{0}{4}+\frac{1}{4}+\frac{1}{4}=\frac{1}{2}.$$

Step 4: If B defends with II_3 strategy, 3 of A's 4 options reach the attack target and 1 is blocked. The payoff of A is

$$g_{23}^{A}=g^{A}(I_2II_3)=\frac{0}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}.$$

5. Step:

If B defends with II_4 strategy, attacks are blocked in 1 of the 4 options of A, and at least one of the attacks will reach the target in 3 of them. A payoff

$$g_{24}^{A}=g^{A}(I_2II_4)=\frac{0}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}.$$

Step 6:

If country B defends with the II_5 strategy, attacks in 1 of the 4 options of A are prevented, and at least one of the other 3 options will reach the target. A payoff

$$g_{25}^{A}=g^{A}(I_2II_5)=\frac{0}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}.$$

Thus, all the payoffs of this cyber warfare scenario g_{ij}(i=1,2; j=1,2,3,4,5) will be calculated. Hence the payoff matrix of this game

It is written in the form of

$$G=\begin{array}{c c}
 & \begin{array}{ccccc} II_1 & II_2 & II_3 & II_4 & II_5 \end{array} \\
\begin{array}{c} I_1 \\ I_2 \end{array} & \begin{bmatrix} 0 & 5/6 & 1/2 & 5/6 & 1 \\ 1 & 1/2 & 3/4 & 3/4 & 3/4 \end{bmatrix}_{2x5}
\end{array}$$

3.1. Analysis of the Payoff Matrix

To simplify the payoff matrix

$$G=\begin{array}{c c}
 & \begin{array}{ccccc} II_1 & II_2 & II_3 & II_4 & II_5 \end{array} \\
\begin{array}{c} I_1 \\ I_2 \end{array} & \begin{bmatrix} 0 & 5/6 & 1/2 & 5/6 & 1 \\ 1 & 1/2 & 3/4 & 3/4 & 3/4 \end{bmatrix}_{2x5}
\end{array}$$

we will do this between the I_j strategies with the same value. Since $II_4 \geq II_5$, If extract II_5 strategy

G_1 is obtained;

$$G_1 = \begin{array}{c} \\ I_1 \\ I_2 \end{array} \begin{array}{cccc} II_1 & II_2 & II_3 & II_4 \end{array} \atop \begin{bmatrix} 0 & 5/6 & 1/2 & 5/6 \\ 1 & 1/2 & 3/4 & 3/4 \end{bmatrix}_{2x4}$$

Since II₃≥II₄ in G₁ matrix, if strategy II₄ is omitted then

$$G_2 = \begin{array}{c|ccc} & II_1 & II_2 & II_3 \\ \hline I_1 & 0 & 5/6 & 1/2 \\ I_2 & 1 & 1/2 & 3/4 \end{array}_{2x3}$$

obtained. G₂ can no longer be simplified.

Now let's calculate the payoffs φ for country A's hybrid strategy $x = (x, 1-x) \in x_2, x \in [0,1]$ and country B's pure strategy IIⱼ (j=1,2,3) $\varphi_j(x) = g(x, II_j)$;

$$\varphi_1(x) = g(x, II_1) = 0.x + 1.(1-x) = 1-x, \quad x \in [0,1]$$

$$\varphi_2(x) = g(x, II_2) = \frac{5}{6}.x + \frac{1}{2}.(1-x) = \frac{1}{2} + \frac{1}{3}x, \quad x \in [0,1]$$

$$\varphi_3(x) = g(x, II_3) = \frac{1}{2}.x + \frac{3}{4}.(1-x) = \frac{3}{4} - \frac{1}{4}x, \quad x \in [0,1].$$

Step 1:

Let's graph the functions $\varphi_j(.) : [0,1] \to R, \ j = 1,2,3$

$\varphi_1 : Y = 1 - x$

$\varphi_2 : Y = \frac{1}{2} + \frac{1}{3}x$

$\varphi_3 : Y = \frac{3}{4} - \frac{1}{4}x$.

The graph of their functions is given in figure 1.

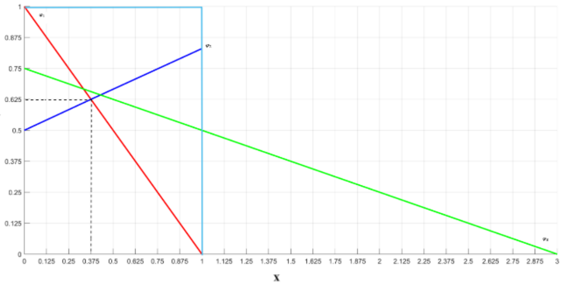

Figure 1. The graph of $\varphi_j(.)$ functions

Step 2:

For $\forall x \in [0,1]$

Let's draw a graph of the function $\psi(.) : [0,1] \to R$ with $\psi(x) = min_{j=1,2,3}\varphi_j(x)$.

$$\psi(x) = \begin{cases} \varphi_2(x), & x \in \left[0, \frac{3}{8}\right] \\ \varphi_1(x), & x \in \left[\frac{3}{8}, 1\right] \end{cases}$$

$$\psi(x) = \begin{cases} \frac{1}{2} + \frac{1}{3}x, & x \leq \frac{3}{8} \\ 1 - x, & x > \frac{3}{8} \end{cases}$$

the function is a polygonal line. The graph of this function is shown in figure 2.

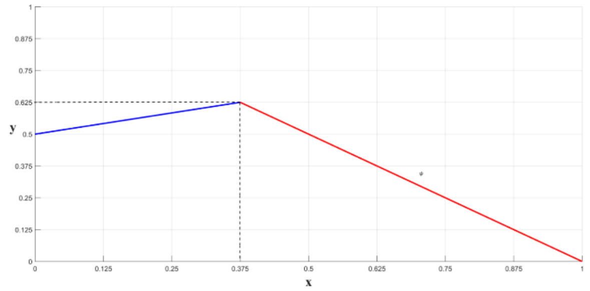

Figure 2. The graph of $\psi(x)$ function

Step 3:

$\psi(.) : [0,1] \to R$ Using the graph of the function (Figure 2), we can calculate the maximum of this function; so, let's find the value of

$V = max_{x \in [0,1]}\psi(x)$. This value is $y = \frac{5}{8}$ for $= \frac{3}{8}$.

Step 4:

Let's find the number $x^* \in [0,1]$ which gives the maximum value of $[0,1] \to R$ in [0,1]. This value is $x = \frac{3}{8}$. Thus, the optimal strategy of country A is its point (3/8, 5/8), which is the peak of the ψ function.

$X^* = (\frac{3}{8}, \frac{5}{8})$

5. Step:

The optimal strategies of country B are found as $g(x^*, II_1) = g(x^*, II_2) = \frac{5}{8}$ by making use of figure 2. So II₁, II₂ strategies will be considered as required strategies for B, while II₃ strategies will be considered as unnecessary strategies.

In this case, country B's hybrid optimal strategy is $Y^* = (y_*, 1-y_*, 0)$. Also, since A's optimal strategy is $X^* = (\frac{3}{8}, \frac{5}{8}) \in x_2$, A's required strategies are I₁ and I₂.

Since V = 5/8, $g(I_1, y^*) = g(I_2, y^*) = \frac{5}{8}$.

$g(I_1, y^*) = 0.y_* + \frac{5}{6}(1-y_*) + \frac{1}{2}.0 = \frac{5}{6} - \frac{5}{6}y_*$

Since $g(I_2, y^*) = 1.y_* + \frac{1}{2}(1-y_*) + \frac{3}{4}.0 = \frac{1}{2} + \frac{1}{2}y_*$

$\frac{5}{6} - \frac{5}{6}y_* = \frac{5}{8}$

$\frac{1}{2} + \frac{1}{2}y_* = \frac{5}{8}$

From any of the above equations we find $y_* = \frac{1}{4}$. So, $Y^* = \left(\frac{1}{4}, \frac{3}{4}, 0\right)$ hybrid strategy becomes the optimal strategy of country B in the G₂ payoff matrix. Thus, the triple

$(X^*, Y^*, V) = (\left(\frac{3}{8}, \frac{5}{8}\right), \left(\frac{1}{4}, \frac{3}{4}, 0\right), \frac{5}{8})$ is obtained, which is expressed in the G₂ payoff matrix as the solution of the game. Hence, the solution of the G payoff matrix is also

($\left(\frac{3}{8},\frac{5}{8}\right),\left(\frac{1}{4},\frac{3}{4},0,0\right),\frac{5}{8}$).

3.2. Explication

Country A will attack targets of country B 300 times with the I_1 strategy and 500 times with the I_2 strategy. In other words, it will send its cyber weapons over different networks in 300 out of 800 attacks and over the same network in 500. Country B will defend 200 times with the II_1 strategy and 600 times with the II_2 strategy. In other words, it will try to prevent attacks by placing a defense system on each network 200 times against 800 attacks, placing two defense systems on both networks 600 times and leaving the other two networks open. The countries and strategies for the 800 attacks are shown in Table 1.

Table 1. The countries and strategies

Strategies	I_1	I_2	II_1	II_2	II_3
Countries					
A	300	500			
B			200	600	

According to this table, the possible attack and defense pairs will be as follows;

$$\{(I_1,II_1),\ (I_1,II_2),\ (I_2,II_1),\ (I_2,II_2)\} \qquad \textbf{(1)}$$

Case I:
When A attacks 300 times by sending cyber weapons from different networks, B blocks 200 times by placing a defense system on each network.
Case II:
When A attacks 300 times by sending cyber weapons from different networks, B defends 600 times by placing two defense systems on the two networks and leaving the two networks open.
Case III:
When A attacks 500 times by sending cyber weapons through the same networks, B defends 200 times by placing a defense system on each network.
Case IV:
When A attacks 500 times by sending cyber weapons from the same network, B places two defense systems on each of the two networks and blocks them 600 times, leaving the two networks open.

In the total of these cases, A was successful in 500 of the attacks, while B was successful in 300. In other words, while A reached the target 500 times, B blocked 300 times.

4. PROPOSED MATHEMATICAL MODEL FOR THE GAIN-LOSS RELATIONSHIP

A's hybrid strategy;

$$\varphi_1(x) = 1 - x, x \in [0,1] \qquad \textbf{(2)}$$

B's hybrid strategy;

$$\varphi_2(x) = \frac{1}{2} + \frac{1}{3}x, x \in [0,1] \qquad \textbf{(3)}$$

The equation expressing the gain of A and the loss of B, since it is expressed by the line equations (2) and (3); obtained from the product of equations $\varphi_1(x)$and $\varphi_2(x)$

$$F(x,y) = 6y^2 - 2x^2 + 4xy - 9y - 3 \qquad \textbf{(4)}$$

is a closed function.
In this case, $x \in [0,1], y \in [0,1]$ (4) is the model expressing the gain-loss relationship in which the gain of A is maximum and the loss of B is minimum.
Let us determine which of the attack and defense pairs expressed by equation (1) will be optimal with (4) a mathematical model.
If we calculate the values of {F (1,1), F (1,2), F (2,1), F (2,2) in the function (4), we find the values of F = {- 5, -8, 8, 7}.
$max\ F = 8 \Rightarrow$ corresponding strategy (I_2, II_1)
$\min F = -5 \Rightarrow$ corresponding strategy (I_1, II_1) found that; It is concluded that the optimal strategies of this scenario are {(I_1, II_1), (I_2, II_1)}.

5. CONCLUSION

In the scenario we are dealing with, the gain-loss situations of the countries have been determined through the model we propose. This model has been constructed on a 2x5 type of return matrix as per our scenario and it is possible to generalize it. It can be generalized over a 2xn return matrix using the Python programming language. Therefore, we can say that the proposed gain-loss model can also be generalized.

Considering the results obtained with this modeling;

I. If the optimal hybrid strategy for countries (I_1, II_1) is, country A will send each of its two cyber weapons from a separate network, and country B will install a defense system on each network.

II. If there is an optimal hybrid strategy for countries (I_2, II_1), country A will send both cyber weapons over the same network, while country B will install a defense system in each network.

In other words, case I, is an attack-defense strategy with a minimum win-loss relationship, whereas II. the situation is the strategy in which the gain-loss relationship is maximum. This proposed model will be useful in determining the optimal strategies in cases where there are n two sides. As a result, the proposed model will speed up the decision-making process in a possible cyberwar and ensure that the gain is maximum and the loss is minimum.

KAYNAKÇA

Eren, H. Gençoğlu, M. T. Yenal, S. (2020)Strateji ve Güvenlik Alanında Temel ve Güncel Yaklaşımlar "Siber Savaş". Nobel Yayınları.

Do, C. T. Tran, N. H. Hong, C. Kamhoua, C. A. Kwiat, K. A. Blasch, E. Ren, S. Pissinou, N. Iyengar, S. S. (2017) Game theory for cybersecurity and privacy. *ACM Computing Surveys (CSUR), 50*(2), 30.

Sokri, A. (2019) Game Theory and Cyber Defense. Games in Management Science (pp. 335-352). Springer.

Guseinov, K.G. Akyar, E. Düzce, S.A. (2010) Oyun Teorisi. Seçkin yayınları.

Kiekintveld, C. Lisy, V. Pibil, R. (2015) Game-theoretic foundations for the strategic use of honeypots in network security. In *Cyber warfare* (pp. 81–101). Springer.

Osborne, M. J. (2004) An Introduction to Game Theory. Oxford University Press.

Shoham Y.and Leyton-Brown. K. (2009) MultiagentSystems: Algorithmic, Game-Theoretic, and Logical Foundations. Cambridge University Press.

Harsanyi, J. (1967) Games with Incomplete Information Played by Bayesian Players, I-III, Part I, the Basic Model", Management Science, Vol 14(3), pp. 159–182.

Aumann, R. and Maschler M. (1995) Repeated Games with Incomplete Information, MIT Press.

Hamilton, S. N. Miller, W. L. Ott, A. Saydjari, O. S. (2002) The role of game theory in information warfare. 4th Information survivability workshop (ISW-2001/2002). Vancouver, Canada.

Burke, J. (1999) Robustness of Optimal Equilibrium Among Overlapping Generations, Economic Theory, Vol. 14, pp. 311–330.

Gibbons, R. (1992) Game Theory for Applied Economists, Princeton University Press.

Libicki, M. (1997) Defending Cyberspace, and Other Metaphors, National Defense University.

Andrew, F. Emmanouil, P. Pasquale, M. Chris, H. Fabrizio, S. (2014) Game Theory Meets Information Security Management, IFIP International Information Security Conference SEC 2014: ICT Systems Security and Privacy Protection(pp.15-29).

Sanjay, G. and Yuan, H. (2015) Cyber War Games: Strategic Jostling Among Traditional Adversaries. Cyber Warfare, Advances in Information Security 56.