Executive Summary

This thesis has been created to analyse the concept of applying game theory to cyber warfare. Although the title includes the word simulation, the project followed a much more theoretical aspect of the problem and focus only to conceptual models. The aim of this project is to establish an overall study of game theory models and to analyse the proposed game theoretic models of cyber defence. Furthermore a construction of a new conceptual model will take place.

The rapid evolution of the technology and its advances produced the information age. The impact of this incident was the move from the conventional world to the virtual world. This change brought many advantages in the human live but unfortunately it created a new kind of warfare, the information warfare. A detailed and precise meaning of cyberwarfare is a difficult issue and that is the reason that several information security specialists gave their own explanation of what this concept encompass. It is like the effort of the blind men to discover the nature of the elephant; a blind man touched an elephant leg and called it a tree and another touched its tail and called it a rope [1].

Generally, cyberwarfare is an internet-based conflict aiming acquisition, modification or dissolve of sensitive information and services of a third party [2]. Doubtless, information and information technologies are gradually getting more and more important to national security in general and to warfare specifically [1]. Although many information security specialists are trying for more than two decades to defend their systems against potential cyber attacks, the foundation of the silver bullet is not real yet.

Game theory is a mathematical framework which analyse strategic situations. The application of game theory in many different disciplines such as economics and biology sciences had many positive outcomes [3]. The idea of applying game theory to the security of information systems looks promising and well suited. Information warfare games are modelled as two-player games of imperfect information. On the one hand, the defender is trying to protect his system and ensure its normal functionality and on the other hand the adversary aims to attack the system and corrupt its functionality, steal data, deface websites and other.

One of the most important, useful and irreplaceable characteristics of human beings, the decision making, it might be the missing component of previous security mechanisms. Game theory is a well tested and powerful methodology which is capable for analysing any kind of strategic situations. It can provide a mathematical framework capable to model: the battle fields, the players involved in the specific games, the actions available to each player, predictions of the opponent's actions et al.

The research carried out in this thesis has as main objective the study of game theory models and their application to information warfare. The basic parts of this project has studied and covered the following:

- Comprehensive analysis of game theory models and especially those related to Information Warfare.
- Analysis of game theoretic models and especially those against DoS/DDoS attacks and System's Intrusions, the fictitious strategy and the FlipIt game.
- Modelling of Information Warfare with components of Game Theory.
- Construction of a new conceptual model which rely on the studied models.
- General analysis of cyberwarfare, modelling of the attackers and propose a new conceptual defence system.

Acknowledgments

This project would not have been possible without the valuable support of many people. First, I am grateful to my supervisor Dr. Theodore Tryfonas who helped and advised me in every stage of this project. Special thanks also to Richard Craig for the interesting meetings we had discussing different aspects of the specific project.

I would also like to thank two special friends, Maria Onoufriou and Andrea Charalambous for their support during the progress of this project.

This thesis is dedicated to my parents Lefteris and Maria Panayiotou and to my brothers Mario, Frosso and Sylvia. I am very grateful to my parents who gave me the opportunity to study in the University of Bristol and had one of the best years of my life.

Table of Contents

“In our heavily networked world, cyber attacks represent a 24/7/365 threat.”
[Robert Richardson (CSI Director, USA)]

Abstract

The rapid evolution of the technology resulted to the dependence of the human majority to the machines. The scale of this dependence spans from small local companies to great imperial governments. This reliance has a large negative impact related with the incomplete security provided by the computers which can harm irreversibly any member of the human society. The new warfare, known as cyberwarfare, has created a great need for defence against information attacks. This thesis has been created to discuss and analyse game theory models and their application to this virtual battle-field. Moreover, proposed game theoretic models of information warfare have been investigated and a new conceptual model has been constructed. Objective of this study was to derive useful and helpful conclusions for this problem domain.

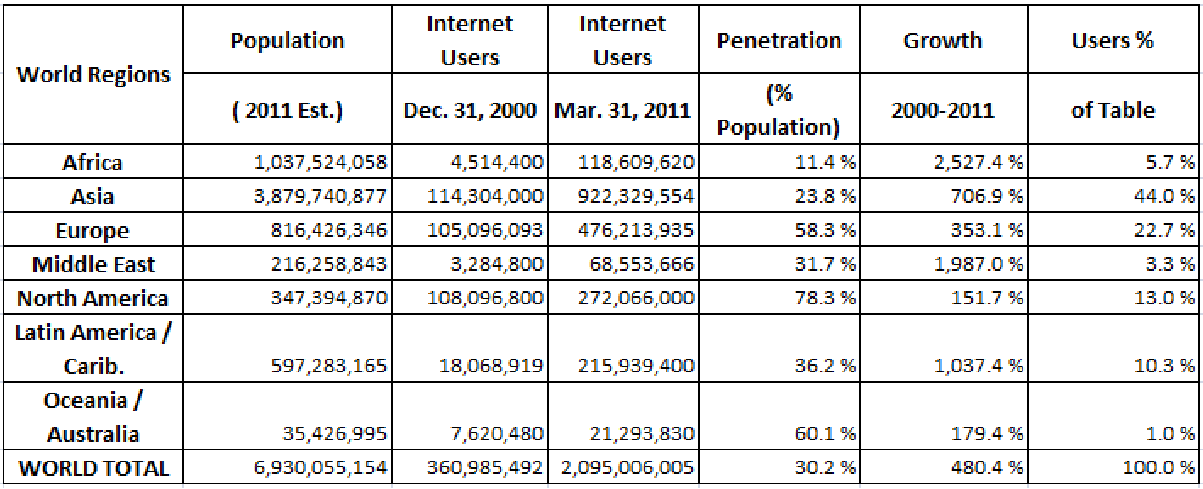
Keywords: Game Theory, Cyberwarfare, Information Warfare

1. Introduction - The Problem

Ubiquitous computers, ubiquitous wireless network connections, ubiquitous on-line services. This is a brief description of the new world of the twenty first century. The information age is real. The world has changed and also people have changed. Subsequently, the way that people interact with the world has changed. People spend more time chatting with their friends through a computer rather than gathering together in a house. People buy goods through the web rather than visiting the shops. People pay their bills using the on-line banking rather than visiting their local bank. All these great achievements flowed from the enormous development of the technology within the last two decades.

The benefits from this grand human progress are evident. Savings in money and time, easiness and mobility are some of the most important advantages of the technology which people enjoy nowadays. Technological advances have made human life easier and more pleasant. On the other hand, the high utility and reliance on the machines led people to face new challenges that must be successfully encountered because their consequences are vital. The adversary has discovered new weapons in today's world. Enemies' arsenals, are full of noiselessly and most of the times untraceable-anonymity weapons, which are possible to cause a huge damage or become catastrophic in the same degree as the weapons used in a conventional warfare.

The statistics related with the internet usage are astonishing. According to the internet world stats website (http://www.internetworldstats.com), by the end of the 2000, the world internet users were around 350 millions. In nowadays, eleven years after, the internet users have managed to exceed the gigantic number of 2 billion.



World Regions	Population	Internet Users	Internet Users	Penetration	Growth	Users %
	(2011 Est.)	Dec. 31, 2000	Mar. 31, 2011	(% Population)	2000-2011	of Table
Africa	1,037,524,058	4,514,400	118,609,620	11.4 %	2,527.4 %	5.7 %
Asia	3,879,740,877	114,304,000	922,329,554	23.8 %	706.9 %	44.0 %
Europe	816,426,346	105,096,093	476,213,935	58.3 %	353.1 %	22.7 %
Middle East	216,258,843	3,284,800	68,553,666	31.7 %	1,987.0 %	3.3 %
North America	347,394,870	108,096,800	272,066,000	78.3 %	151.7 %	13.0 %
Latin America / Carib.	597,283,165	18,068,919	215,939,400	36.2 %	1,037.4 %	10.3 %
Oceania / Australia	35,426,995	7,620,480	21,293,830	60.1 %	179.4 %	1.0 %
WORLD TOTAL	6,930,055,154	360,985,492	2,095,006,005	30.2 %	480.4 %	100.0 %

Figure 1: World Internet Usage and Population Statistics (http://www.internetworldstats.com)

The previous table clearly indicated the large degree of dependence of the civilization on the computers. According to the National Information Assurance Strategy [4] of the United Kingdom which was published in 2007, around ninety seven percent of enterprises within the United Kingdom use the internet for their activities. The majority of the world's governments, financial institutions and the general public are using the internet infrastructure to run their daily activities [5].

The great degree of reliance on information from each part of the society makes the computers and networks that hold all this information profitable targets. The gain of the opponent data or even better, the pass of the control of an information system from the legitimate user to the opponent doubtlessly confronts an enormous advantage for the enemy [6].

Doubtlessly, the last two paragraphs pointed out that a trusted and confident virtual environment is indeed an essential requirement in order to keep the online activities safe and reliable. A number of cyber incidents have indicated the severity of such situations. Cyber attacks are capable to cost a huge amount of loss to governments (Estonia Vs Russia [7]), private enterprises [8] and more generally in the public. In addition of any possible financial losses a system can suffer, the targets can be harmed in terms of reputation and data confidentiality also. These facts have created an ongoing and pressing need for the development of countermeasures to prevent or mitigate the consequences of cyber attacks [5].

A large amount of cyber-crimes have been reported over the last two decades. On the other hand, many specialists stated that the reported incidents do not depict the real problem of cyberwarfare [9]. The society should increase its attention level, severity and awareness for the specific crime category. It is not accidentally the fact that American's Federal Bureau of Investigation (FBI) has listed the combat against cybercrime and cyber-terrorism as number three priority behind counterterrorism and counterintelligence [9]. Appendix A describes in brief fourteen severe information incidents which occurred in the last few years.

Cyber security has been pushed down the priority ladder behind the economy and health care [10]. Many surveys have shown the great impact of the cyber warfare in the economy which has cost millions of dollars for the specific attacks. An investigation on computer crime and security [11] made by the CSI in 2008 makes it clear that all the users of any kind of information system must increase their awareness about many different types of electronic breaches launched by the hackers. The next two figures display the types of incidents and the cost of these specific incidents of the 144 companies that participated in the survey.

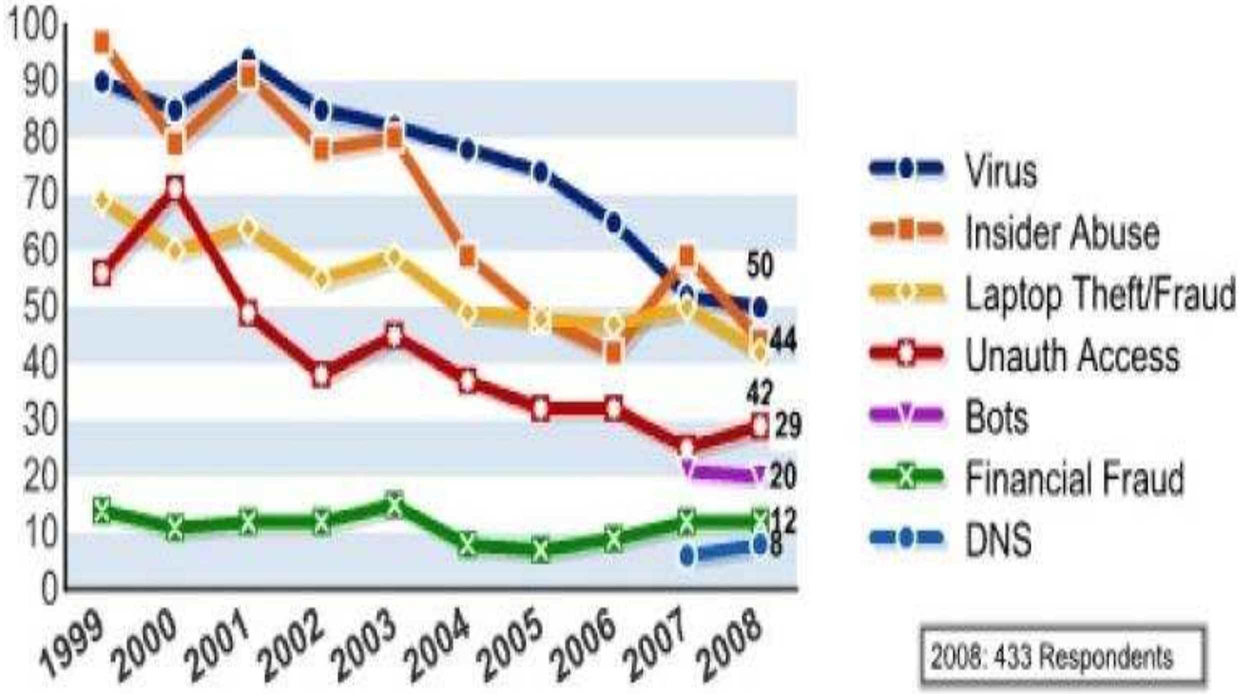


Figure 2: Percentages of Key Types of Incidents [11]

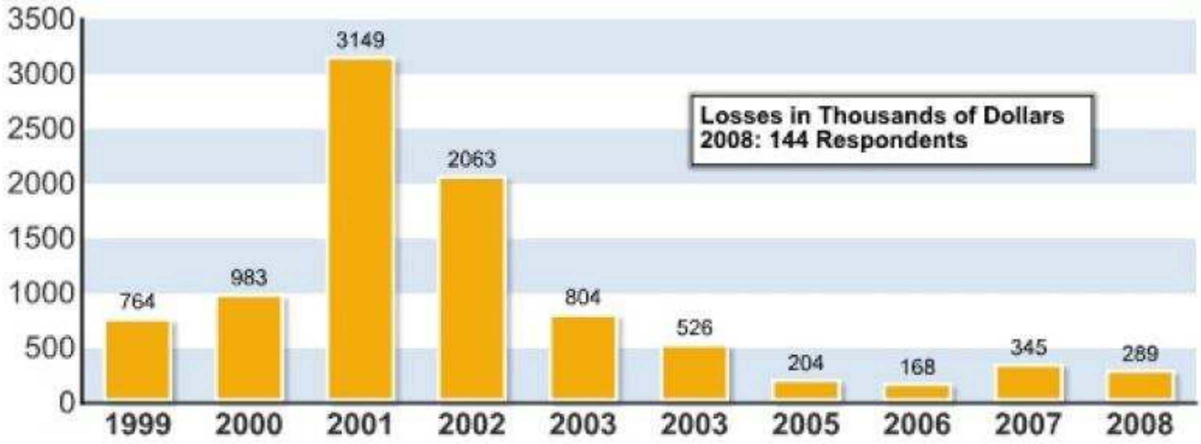


Figure 3: Average Losses per Respondent [11]

1.1 From the Conventional Battlefield to Networks [12]

Cyber warfare has its own battlefield, the network. Although cyber warfare might have similar targets like a conventional warfare, the battlefield that all the conflicts take place is totally different. The weapons used in the cyber warfare need a network in order to activate and spread their effect. The new warfare has transformed the conventional weapons to computers and from the bullets to bits. Cyber warfare attacks can cause many losses related with data:

- Confidentiality
- Integrity
- Availability
- Authenticity

1.2 Aims and Objectives

The aim of this thesis is the study of game theory models and the application of game theory to information warfare. The application of game theory to cyberwarfare will focus on denial of service attacks and unauthorised systems' intrusions. Moreover, the main objective is to construct a new game theoretic defensive model combining those that will be analysed. An analysis of attacker's modelling and a development of a conceptual defensive model will studied as well.

The rest of this thesis is divided in six main chapters. The next chapter is a comprehensive analysis of game theory models and especially those that are more related with information warfare incidents. The following chapter makes a review of proposed game theoretic models related to information warfare and in the next chapter a new conceptual model is constructed. The subsequent chapter makes a review of the modelling of internet adversaries and another conceptual security model is proposed. The same chapter contains analysis of different information warfare components as well. Afterwards, an analysis and evaluation of the application of game theory to information warfare takes place. This thesis ends with conclusions of the specific problem domain derived from the study that have been made.

2. Game Theory

In 1921, the mathematician Emile Borel suggested a formal theory of games which was furthered by John von Newmann in 1928 [3]. The publication of the monumental volume “Theory of Games and Economic Behaviour” in 1944 by John von Newmann and Oskar Morgenstern was the origin of the establishment of game theory as a field on its own. Game theory is the method of studying strategic situations. Strategic situations are characterised by imperfect competitions. Anything that constitutes imperfect competition is a strategic situation and the outcomes that affect one player depend not only on his own actions, but on the actions of others as well. In other words, game theory is the formal study of decision-making where several players have to make and their choices potentially affect the interest and the outcome of the other players [13].

Having in mind the nature of game theory and the components of the games that examines, it is highly noticeable that is well suited to the analysis of cyber-warfare. Game theory examines the relationships between players using models with clear statements of consequences (outcomes). The playoffs depend on actions of more than one player. Game theory is all about power and control. In a cyber conflict, the defensive and offensive player follow specific objectives and take into account both their skills and expectations of other’s player’s behaviour. The same analysis is used in game theory models. Another reason why game theory is appropriate in this kind of warfare is because in the face of opponents who carry out attacks in a postmodern fashion, conventional strategies lead nowhere [14].

2.1 Components of a Game

All the games which have been analyzed include some common characteristics. The components that represent a classic game are shown below:

1. Players: The participants of the game (who?).
2. Strategies: The moves of each player (What actions are available?).
3. Rules: The regulations of the game (How? When? What do they know?).
4. Outcomes: The results after the actions of the players are complete.
5. Payoffs: The gains/losses of each player after the actions are completed.

2.1.1 A Naive Example of the Components of a Poker Game

A typical analysis of a poker game would consist of the following components:

1. Players: Players sitting around the poker table.
2. Strategies: Check, Call, Fold, Raise.
3. Rules: Buy in, minimum/maximum raise.
4. Outcomes: Victory or defeat.
5. Payoffs: Earn the price, loss the buy in price.

2.1.2 A General Mathematical Analysis of a Strategic Game [15]

An examination of a game with a few mathematic notations that represent each element of a game is the following:

- Each game has a finite set N. This set contains all the players that participate in the game.
- For each of the players ($i \in N$) there exist a non-empty set A_i. A_i is the set of actions or strategies available to player i.
- For each of the players ($i \in N$) there exist a utility (payoff) function U_i : A → R. This function will assign a payoff value to each action or strategy that it will be gained by the player when the specific action will occur.

- Usually, a game is characterized by a triple: $\mathrm{G} = (\mathrm{N}, A_i, U_i)$.
- If A is finite, then we say that the game is finite.

2.1.3 How to play [15]

Usually a game includes the following steps. In a one-shot game, these steps occur only once in contrast with repeated games where the specific steps are repeated over time.

- Each player (decision-maker) of the game must choose one of his available actions (a_i).
- All participants make their moves simultaneously or sequentially leading to the action profile $a^* = (a_{1,}\ a_{2,}\ a_{3,\dots,}\ a_n)$.
- When the actions are completed, each player i gain the payoff $U_i(a^*)$.
- The goal of each player is to maximize his total payoff or to minimise their losses.
- Each player is aiming only for his own benefits (non-cooperative game).
- Each player must analyse each situation with any known information and choose the best possible action for him.

2.1.4 A Simple Notation Example of Two-Player Game

Suppose that a game has the following structure:
N = {Player 1, Player 2}
$\mathrm{A}_{Player\ 2}$ = {T, B}
$\mathrm{A}_{Player\ 1}$ = {L, R}
U_1(T) = x11/x12, U_1(B) = x21, x22
U_2(L) = y11/y21, U_2(R) = y12, y22

The matrix below shows the available actions and payoffs of two players in a strategic situation.

	Player 2		
Player 1	**ACTIONS**	**L**	**R**
	T	x11,y11	x12,y12
	B	x21,y21	x22,y22

Figure 4: Actions and Payoffs of a Two-Player Game.

In the above matrix, the strategies of player 1 are the rows and the strategies of player 2 are the columns. The payoff for every possible action profile is specified as a pair (x, y). The x value is the payoff for player 1 and the y value is the payoff for player 2. For example, if the game (B, L) has been played, the payoff value for player 1 is x21 and the payoff value for player 2 is y21.

2.2 Rationality [16]

One of the most important assumptions in game theory models is the fact that all the participants of a game are rational players and act rationally. Players are believed as rational and self-interested. Rationality of all players is a basic constraint in many game theory models.

Every player in the game is rational and every player thinks that every other player is rational. Also, every player thinks that every player thinks that every player is rational, and so on. In such situations, each player's beliefs about other players' choices of actions are not taken as correct but they are constrained by considerations of rationality. Consequently, every player of the game believes that the actions taken by every other player is a best response to some belief. Furthermore, each player assumes that every other player reasons in this way and hence thinks that every other player believes that every other player's action is a best response to some belief, and so on.

Consider a strategic game $\mathrm{G}\ (\mathrm{N}, \mathrm{A_i}, \mathrm{u_i})$. N is the set of players of the game, A_i is the set of actions of player i and u_i is the payoff function of player i. Player i consider all the other players j of the game rational. Having this rationality on mind, player i should be able to rationalize his belief μ_i about how the other players should act as follows:

For every action of the rest players j, where the belief μ_i of player i assigns a positive probability, then the specific actions should be a best response to a belief of player i. Furthermore, if player i thinks that every other player j, thinks that every player $h \neq j$ (including the player i as well) is rational, then player i, should be in the position to determine player j's view about player h's beliefs.

An action $\mathrm{a_i} \in \mathrm{A_i}$ is rationalizable in the strategic game $(\mathrm{N}, \mathrm{A_i}, \mathrm{u_i})$ if there exists:

- a collection $\left((\mathrm{X_j^t})\mathrm{j} \in \mathrm{N}\right)_{\mathrm{t}=1}^{\infty}$ of sets with $\mathrm{X_j^t} \subseteq \mathrm{A_j}$ for all j and t,
- a belief μ_ι^1 of player i whose support is a subset of $\mathrm{X_{-i}^1}$ and
- for each $j \in N$, each $t \geq 1$, and each $\mathrm{a_j} \in \mathrm{X_j^t}$, a belief $\mu_\mathrm{j}^{\mathrm{t}+1}(\mathrm{a_j})$ of player j whose support is a subset of $\mathrm{X_{-j}^{t+1}}$.

Such that

- $\mathrm{a_i}$ is a best response to the belief μ_i^1 of player i.
- $\mathrm{X_i^1} = \emptyset$ and for each $\mathrm{j} \in \mathrm{N} \setminus \{\mathrm{i}\}$ the set $\mathrm{X_j^1}$ is the set of all $\mathrm{a_j^{'}} \in \mathrm{A_j}$ such that there is some $\mathrm{a_{-i}}$ in the support of μ_i^1 for which $\mathrm{a_j} = \mathrm{a_j^{'}}$.
- For every player $\mathrm{j} \in \mathrm{N}$ and every $\mathrm{t} \geq 1$ every action $\mathrm{a_j} \in \mathrm{X_j^t}$ is a best response to the belief $\mu_\mathrm{j}^{\mathrm{t}+1}\ (\mathrm{a_j})$ of player j.

2.3 Important Characterisations of Games [3, 17, 18]

A Game is a proper model of an interactive situation and can be described formally at various levels of detail, structures, rules et al.

2.3.1 Static Games

This kind of games is characterised as one-shoot games. Each player has to choose a strategy simultaneously with the other players. None of the player has the knowledge of the actions that have been chosen by his opponents. Once a player has chosen his action he is not able to alter his choice. After the pre-selected actions of each player are completed, the outcome is been determined immediately hence the payoffs of each player as well. Games which are simultaneous are represented by the normal form and are solved using the Nash equilibrium concept.

2.3.2 Dynamic Games

A dynamic or repeated game is the game where each player makes more than one move. In such games, the players take into consideration the history of the game (their opponent's previous moves) which might reveal them some information about their opponents' strategies. Repeated games are illustrated using extensive form.

2.3.3 Cooperative and Non-cooperative Games

There are two main categories of games description known as Cooperative (coalitional) game and non-cooperative games. A cooperative game is a high level description game and it only specifies what the payoffs of each group will be by the collaboration of its member. The process followed by each group it is not made explicit. Usually, this type of game is investigated with respect to the relative amount of power held by various players or how a successful group should divide its proceeds. Non-cooperative game theory concerns with the analysis of strategic choices. The term non-cooperative indicates that in this type of game the participants (players) are making their choices out of their own interest. It is critical for the decision-maker to understand that details of the ordering and timing of players' choices are essential and effectively influence the outcome of the game.

2.3.4 Games' Representations

Normal and extensive forms are the two main ways of describing a game. Normal form is also known as strategic form. A game in a strategic form record the strategies followed by each player and the payoff that result from each possible combination of choices. The records of strategies and payoffs are displayed in a matrix. The payoff (utility) is a number indicating how much the player likes the outcome. The disadvantage of the specific form is the fact that some information of the game might get lost (compared to extensive-form). A game in normal form is ideally for quick identification of strictly dominated strategies Nash equilibrium. An example of a game in normal form is shown below:

	Prisoner 2		
Prisoner 1		**Cooperate**	**Defect**
	Cooperate	2, 2	0, 3
	Defect	3, 0	1, 1

Figure 5: The Prisoner's Dilemma Game in Normal Form.

The extensive form (game tree), is more comprehensive than the strategic form of game. This form of game has a detailed description of how the game is played over time. It describes the order in which players take actions, the information that players have at the time they must take those actions and the times at which any uncertainty in the situation is resolved. The next figure depicts the prisoner's dilemma game in its extensive form.

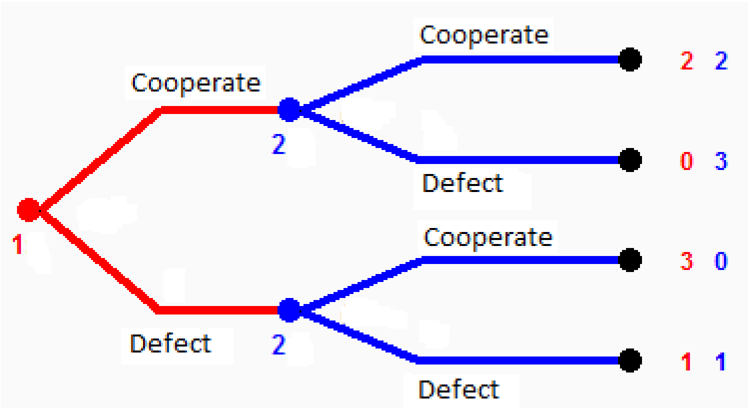


Figure 6: The Prisoner's Dilemma Game in Extensive Form.

2.3.5 Knowledge

- Complete Information: All the participants of a strategic situation know the structure of the game. The structure of a game consists of the players, actions (strategies of all the players), rules, outcomes and payoffs.

- Incomplete Information: Is the kind of games where the participants have different secrets (private information) related with their preferences and abilities.

- Perfect Information: A game is in perfect information if all players know the history move of the game. When a player wants to move, the time he is ready to choose an action, he is informed about what moves the other players did in the past.

- Imperfect Information: Is the kind of games where one or more participants of the game do not know the full history of the game (actions that were completed in the past).

- Common Knowledge: Information is said to be common knowledge if all players know the structure of the game, all players know all players know the structure of the game, all players know all players know that all players know the structure and so on.

2.3.6 Zero-Sum Games [3, 14]

Zero-sum games (special case of constant-sum games) represent the class of games where the participants of the specific game have fully opposed interests. All the participants have diametrically opposed objectives and one player can gain only at the expense of another player. No matter what the outcome of the game is, the winnings of one player are exactly balanced by the losses of the other player. If from the sum of the payoffs of one player is subtracted the sum of the losses of the other player, the answer should be zero. This kind of games can be used to strategically model the computer science concept of “demonic” non-determinism. Demonic non-determinism is based on the assumption that if a set of events are not ordered, the player should assume that the worst possible sequence will take place. The next figure depicts a zero-sum game.

	Player 1		
Player 2		**Action A**	**Action B**
	Action A	2, -2	1, -1
	Action B	3, -3	0, 0

Figure 7: A Zero-Sum Game.

2.3.7 Non-Zero Sum Games (Positive Sum and Negative Sum Games) [14]

The game where a player can benefit from the actions taken by other players is called as positive sum game. In this situation, a player might benefit more than the others, and it can also result with one player losing and the other gaining with an overall gain. In positive sum games the gains exceed the losses. On the other hand, a negative sum game is the game where action of one player result to looses for both themselves and the others. In negative sum games the losses exceed the gains. The next figure depicts a non-zero sum game.

	Player 1		
Player 2		Action A	Action B
	Action A	2, 1	1, 0
	Action B	4, -1	0, 0

Figure 8: A Non-Zero-Sum Game.

2.4 Preferences (analysis of the player behaviour) [19]

Each player has a set of options and he is forced to choose one of his available options. Imagine there is a set S which consists by a player’s available actions. The elements of this set are said to be mutually exclusive. This means that a player, by choosing the action X, automatically implies that he rejects the rest available options.

- A strict preference implies that one option X is strictly preferred to an option Y: X > Y.
- A weak preference implies that an option X is weak preferred to an option Y: X>=Y.
- When player is in indifferent between option X and Y means that he does not have a preference between the two actions: X~Y.

Preferences are asymmetric: This means that from the set of available options, it is not possible that a pair of actions X and Y have the properties: X>Y and Y>X.

Preferences are negatively transitive: This means that if from the set of options, an action X>Y it implies that for any third element Z, either X>Z or Z>Y or both.

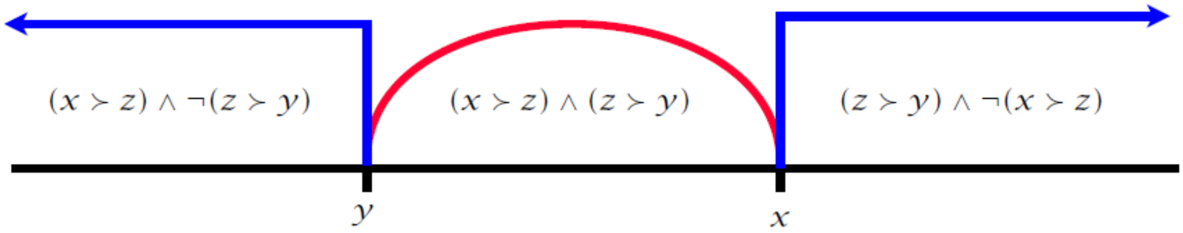

$(x \succ z) \wedge \neg(z \succ y)$
$(x \succ z) \wedge (z \succ y)$
$(z \succ y) \wedge \neg(x \succ z)$
y
x

Figure 9: Illustration of Negative Transitivity. [19]

If ‘>’ is asymmetric and negatively transitive, then (Proof in [19])

- $\geq$ is complete: For all $x, y \in S, x \neq y$, either $x \geq y$ or $y \geq x$ or both;
- $\geq$ is transitive: If $x \geq y$ and $y \geq z$, then x ≥ z;
- ~ is reflexive: For all $x \in S$, x ~ x;
- ~ is symmetric: For all $x, y \in X$, x ~ y implies y ~ x;
- ~ is transitive: If $x \sim y$ and $y \sim z$, then $x \sim z$;
- If $w \sim x$, $x > y$, and $y \sim z$, then $w > y$ and $x > z$.

2.4.1 Rational

The preference relation ≥ is rational if it is complete and transitive. This definition implies that when a player has two options available, he is able to determine whether he likes one at least as much as the other (completeness). Also, there is not a case where any possible sequence of pair-wise choices can result in a cycle (transitivity).

2.4.2 Utility Representation

Let S be the set with all the available options of a player. A utility function $u(x)$ represents the function which is responsible to assign a numerical value to $x \in S$ in a way that the rank ordering of the available actions can be preserved. A function $u : X \rightarrow R$ is a utility function representing preference relation ≥ if the following holds for all $\mathrm{x}, \mathrm{y} \in \mathrm{X}$: $\mathrm{x} \geq y \Leftrightarrow \mathrm{u(x)} \geq u(y)$. A preference relation ≥ can be represented by a utility function only if it is rational.

2.4.3 Choices under Uncertainty

The most interesting applications of game theory are in situations where the player is uncertain about the consequences of his choice at the time the decision is made. The player is facing a game with a number of risky alternatives. Each available action can cause a number of different outcomes but the player is not able to tell what will be the outcome of his choice in the time the decision is taken.

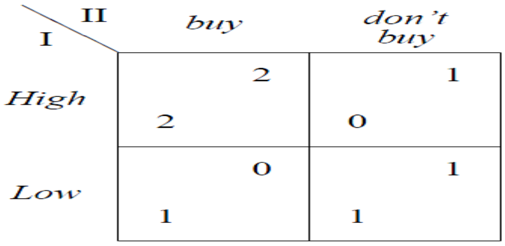
The von Neumann-Morgenstern (VNM) expected utility theory models uncertain prospects as probability distributions over outcomes. The specific set of probabilities, is given as part of the description of the outcome. In this case, each set of available options, is linked with a larger set of probability distributions over these outcomes denoted by P.

Let X be the set of outcomes and P the set of probabilities associated with each possible outcome. All the probabilities in set P must be non negative and not greater than 0<=P(i)<=1). The sum of all the probabilities in the set P should result to one.

2.5 Nash Equilibrium (Best Response)

Games where dominate strategies are available are easy for analysis in order to advice the players on how to play the game and reach the best outcome. On the other hand there are games where there is not any dominating strategy. The considerations made in the existing of a dominating strategy cannot apply in this kind of games. Nash Equilibrium (strategic equilibrium) is a list of strategies (one for each player) which has the function that no player can unilaterally amend his strategy and get a better payoff. Having on mind that all players are rational, a player will not alter his strategy because he expects that the other players will follow their recommended strategy which is the best of their interest. Nash Equilibrium is the situation where a player chooses a strategy and he cannot advantage if he change his specific strategy while the other participant keeps his strategy unchanged [14].

The following figure will show a Nash Equilibrium game. Player I is an internet service provider and player II a potential customer. The problem is the decision whether they will sign a contract of service provision for a period of time. The provider is thinking whether he will provide high or low quality of service because they have different costs and some of the costs of high quality are independent of whether the contract is signed or not. On the other hand, the player has two choices; to buy or not to buy the service.



I \ II	*buy*	*don't buy*
High	2 2	1 0
Low	0 1	1 1

Figure 10: High-Low Quality Game between a Service Provider (Player I) and a Customer (Player II). [3]

The specific game has not any dominated strategies for either player but it has two Nash Equilibrium in which each player chooses his strategy deterministically. The first one is the strategy combination (Low, don't buy) and the second one is the combination (High, Buy). The combination (Low, don't buy), is Nash Equilibrium because Low is the best response to don't buy and vice versa. Best response is the strategy that will maximize the payoff. The same happens in the second combination (High, Buy). A customer prefers to buy when the quality is high and the provider prefers to provide high quality when the client buys.

Both combinations are legitimate recommendations to the two players of how to play the game. When players decide on the strategies that form a Nash Equilibrium stay with their rational choices. Neither player is willing to change his strategy and this result to a consistent solution concept of games.

2.5.1 Calculation of a Nash equilibrium

This section illustrates the procedure that must be followed to find a Nash Equilibrium of a game (if exists). For the illustration purposes a two-player game is used. Each player has two available actions only. In order to find the Nash equilibrium of a game you must follow three basic steps:

Step 1: Find Player's 1 best responses against Player's 2 actions

	Player 2		
Player 1		A	B
	A	20, 30	25, 50
	B	40, 15	35, 60

If player 2 choose action A, then player's 1 best response is to choose action B since 40>20.
If player 2 choose action B, then player's 1 best response is to choose action B since 35>25.

Step 2: Find Player's 2 best responses against Player's 1 actions

	Player 2		
Player 1		A	B
	A	20, 30	25, 50
	B	40, 15	35, 60

If player 1 choose action A, then player's 2 best response is to choose action B since 50>30.
If player 1 choose action B, then player's 2 best response is to choose action B since 60>15.

Step 3: Nash equilibrium exists where Player A's best response is the same as Player B's best response. In the specific game is the pair of actions (B, B).

	Player 2		
Player 1		A	B
	A	20, 30	25, 50
	B	40, 15	35, 60

2.5.2 Best Response Set and Nash Equilibrium [15, 16]

The best response set for player n to s_{-n} is:

$$R_n(s_{-n}) = \arg max_{s_n \in S_n}\ \Pi_n(s_n, s_{-n}),$$

Where arg $max_{x \in X}\ f(x) is\ the\ set\ of\ x\ that\ maximize\ f(x)$

A (pure strategy) Nash equilibrium of an n-player game is a vector $s = (s_1, s_2, \ldots, s_n\ )$ if:

$$S_i \ \in \ R_i(s_{-n}) for\ all\ player\ i$$

The previous equation indicates that each player plays his best response against his opponents.

2.5.3 A Naive Example to Demonstrate Nash Equilibrium in Information Warfare

The main idea of Nash Equilibrium is the fact that the players must take into account their opponents possible actions before they decide with which action they should proceed. For example imagine an insider hacker who aims to disclose some documents of his company he works for. The specific company has two types of documents. The documents of the first category are classified as top secret and the documents of the second category are classified as confidential.

If the company loss any top secret documents, it will suffer a great loss of money despite the loss of any other type of documents which are classified different. Because of this fact, the company allocates its best defence mechanisms which are impenetrable to protect its top secret data. On the other hand, the confidential data are protected by less reliable defence mechanisms.

Both players of the specific game, the attacker and the company are fully informed about their opponents. The attacker knows the defence mechanisms of the company and which data are under the protection of which defence. The company also knows which attacks might encounter and need to defence.

The attacker will get a higher payoff if he manages to obtain any top secret documents than obtaining any confidential documents. On the other hand, he knows that it is almost impossible to gain access to the top secret documents but much easier to access the confidential ones. The company also knows which documents are the most important and that it will suffer a high loss of money in the event of illegal disclose of top secret data. That is the reason it protects them under heavy defence mechanisms.

Having on mind the pre-described scenario, Nash equilibrium for the two players should be:

a. The attacker to try and access the confidential data
b. The company to protect better the top secret data than any other kind of data

It is better for the attacker to gain at least some payoff by trying to access the confidential data than launch an attack aiming the top secret data which has a high probability to not succeed. Also for the company, it is much more preferable to allocate better and more defence mechanisms to data which are most valuable to it and it would not be acceptable any loss this kind.

If any of the two players decide to deviate from his strategy, he will not get any more benefits but he wills only mange to increase his losses. That is the reason that the two strategies described before represent the Nash equilibrium of the specific scenario/game.

2.6 Strategies [16, 17, 18]

2.6.1 Pure Strategy

The available actions of a player are called pure strategies or mixed strategies according to the probability which is assigned to each action. Pure strategy is the action which the player will follow every time his able to make a move. The specific action has a probability of one which indicates that is the only action that might occur. A pure strategy reflects the confidence of the player to play the specific action.

2.6.2 Mixed Strategies

Mixed Strategies consists of a set of possible actions of a player along with a probability distribution (collection of weights) which indicates how frequently each action is possible to be played. Mixed strategies reflect uncertainty about what the other player might play. The utilisation of mixed strategies is desirable when a player is indifferent between several pure strategies. If in a game, the opponent guessing is desirable then the used of mixed strategies is required (randomization over pure strategies). This approach will prevent the opponent to benefit from knowing the next move.

2.6.2.1 Mixed Strategy Notation

Suppose S denotes all the pure strategies available to a player in a game: $s^i \in S, i \in 1, 2, \ldots, n$. A mixed strategy ($\sigma$) of the specific player is a probability distribution over all his pure strategies $s^1, s^2, s^3, \ldots, s^n$. The mixed strategy of this player is denoted as:

$$\sigma = p_1 * s^1, p_2 * s^2, p_3 * s^3, \ldots, p_n * s^n ,$$

Where each $p_1, p_2, p_3, \ldots, p_n$ are all non negative and $\sum_{i=1}^{n} p_i = 1$

Each p_i represents the probability that the player will play the corresponding pure strategy s_i. Pure strategies can also represented as mixed strategies. The case where all but one of the $p_i^{'}s$ are zero in a mixed strategy σ and the one that is non zero has a probability of one indicates that only one pure strategy is played every game. In the specific situation, the mixed strategy is equivalent to the pure strategy.

2.6.2.2 Mixed Strategy Payoffs – Expected Payoffs

The payoffs of mixed strategies changed and are calculated using the expected utility principle. The definition of the expected payoffs will be explained through an example. The specific example, involves a two player simultaneous game. The player A has n pure strategies ($s^1, s^2, s^3, \ldots, s^n$) and player B has m pure strategies ($t^1, t^2, t^3, \ldots, t^n$). The payoff function for player A is $U_A(s^i, t^j)$ and for player B is $U_B(s^i, t^j)$ where $i \in \{1, 2, 3, \ldots, \mathrm{n}\}$ and $\in \{1, 2, 3, \ldots, \mathrm{m}\}$.

The mixed strategy of player A is: $\sigma_1 = p_1 * s^1, p_2 * s^2, p_3 * s^3, \ldots, p_n * s^n$
The mixed strategy of player B is: $\sigma_2 = q_1 * t^1, q_2 * t^2, q_3 * t^3, \ldots, q_n * t^m$

The calculation of the player's A expected payoff $U_A(\sigma_1, \sigma_2)$ is shown below. First, the expected utility principle is applied and decomposes $U_A(\sigma_1, \sigma_2)$ in terms of $\sigma_1$which yield:

$$U_A(\sigma_1, \sigma_2) = \sum_{i=1}^{n} p_i * U_A(s^i, \sigma_2)$$

After that, the expected utility principle is applied again and decomposes each of the $U_A(s^i, \sigma_2)$ in terms of σ_2 and this yield:

$$U_A(s^i, \sigma_2) = \sum_{j=1}^{m} p_i * U_A(s^i, t^j)$$

By putting the above equations together, the result is:

$$U_A(\sigma_1, \sigma_2) = \sum_{i=1}^{n} \sum_{j=1}^{m} p_i * q_j * U_A(s^i, t^j)$$

If the same steps are repeated for player B then the answer is:

$$U_B(\sigma_1, \sigma_2) = \sum_{i=1}^{n} \sum_{j=1}^{m} p_i * q_j * U_B(s^i, t^j)$$

The Nash equilibrium definition for mixed strategies is the same as explained before with the only difference that instead of payoffs the players have expected payoffs. An important theorem related with mixed strategies is the fact that in a k-player game where players have a finite number of pure strategies, then that specific game has a Nash equilibrium (not necessarily unique) if mixed strategies are allowed. In other words, a mixed strategy Nash equilibrium is not guaranteed in a game of mixed strategies except in the case that the specific game has pure strategy equilibrium.

2.7 Solving a Game [15]

As it was showed and discussed on the few examples above each game have many different solutions. How can a player figure out the best possible solution for himself in a game? This can be calculated by utilising different possible solution concepts which are pointed below:

- Elimination of strictly or weakly dominated strategies
- Maxi-Min strategies (for minimizing the loss in zero-sum games)
- Nash equilibrium

2.7.1 Elimination of Dominated Strategies [13, 18, 20]

When a game has a dominated strategy, it means that no matter what your opponent might choose to play, if you choose the dominated strategy you will never benefit or gain a payoff greater than the minimum that you can.

There are two types of dominance strategies:

- Strongly dominated strategy
- Weakly dominated strategy

If someone chooses to play a strongly dominated strategy then he is assigned to gain payoffs that are lower from any other strategies no matter what his opponents will decide to do. If someone chooses to play a weakly dominated strategy, then he assigned to gain payoffs that are generally lower of the most of the rest strategies, no matter what he is opponent decides to play. The next figure will demonstrate an example of strongly and weakly dominated strategies.

	Player 2				
Player 1		Action A	Action B	Action C	Payoff Sum (Player 1)
	Action A	3, 1	0, 0	2, 3	5
	Action B	0, 2	0, 0	0, 0	0
	Action C	0, 3	2, 0	0, 1	2
	Payoff Sum (Player 2)	6	0	4	

Figure 11: A Game with Weakly and Strongly Dominated Strategies.

Action B for player 1 is a strongly dominated strategy for Player 1. No matter what strategies between A, B or C Player 2 might choose, Player 1 will always have a payoff of zero. That's the reason that a rational Player 1 would never accept to proceed with the specific game playing the action B. Similarly, action B is strongly dominated for player 2. Action C for player 2 is weakly dominated. If player 2 decides to play action C, he will get a good payoff if player 1 decides to proceed with action A. On the other hand if player 1 decides to play action B or C, Player 2 will get a much lower payoff than if he chooses to play action A. This is the reason action C for player 2 is said to be weakly dominated. Similarly, action C is weakly dominated for player 1.

If you consider the two previous notions, in a strategic game, all the available actions of the players can be categorised as strictly or weakly dominated except from the one that form the Nash Equilibrium of the game. Nevertheless, finding dominated strategies in a game it is really hard and many times impossible considering games with incomplete information.

A strategy a_i^* strongly dominates a_i if and only if

$$u_i\ (a_i^*, a_{-i}) > \ u_i(a_i, a_{-i}), \forall\ a_{-i}\ \in\ A_{-i}$$

A strategy a_i^* weakly dominates a_i if and only if

$$u_i\ (a_i^*, a_{-i}) \geq \ u_i(a_i, a_{-i}), \forall\ a_{-i}\ \in\ A_{-i}$$

Suppose a game has a strategy space S with n available pure strategies. It is obvious from the above explanation that a rational player will never play a dominated strategy thus any dominated strategies of the game can be removed one by one. Each time a dominated strategy is removed, the player refines his options because a new game is constructed with less available actions. When all the dominated strategies are removed it is possible to result to only one action that yields the maximum payoff according to the actions of the opponent which might also be the Nash equilibrium. The game which is solved using this procedure is called dominance solvable. An example of a game which is solved by eliminating dominated strategies is shown below:

2.7.1.2 An example of Dominance Solvable Game

Player's 2 middle move strongly dominates his right move because 2 > 1 and 1> 0 thus the right move is eliminated.

	Player 2			
Player 1		Left	Middle	Right
	Up	1, 0	1, 2	0,1
	Down	0, 3	0, 1	2, 0

Figure 12: Example of Eliminating Dominated Strategies (step 1/4).

Player's 1 down move strongly dominates his up move because 1>0 and 1>0 thus the down move is eliminated.

	Player 2			
Player 1		Left	Middle	~~Right~~
	Up	1, 0	1, 2	~~0,1~~
	Down	0, 3	0, 1	~~2, 0~~

Figure 13: Example of Eliminating Dominated Strategies (step 2/4).

Player's 2 left move strongly dominated by his middle move because 2>0 thus the left move is eliminated.

	Player 2			
Player 1		Left	Middle	~~Right~~
	Up	1, 0	1, 2	~~0,1~~
	~~Down~~	~~0, 3~~	~~0, 1~~	~~2, 0~~

Figure 14: Example of Eliminating Dominated Strategies (step 3/4).

Finally, the game is solved. The optimal pair of strategy for this game is (Up, Middle) which yields one point for player one and two points for player two.

	Player 2			
Player 1		~~Left~~	Middle	~~Right~~
	Up	~~1, 0~~	1, 2	~~0,1~~
	~~Down~~	~~0, 3~~	~~0, 1~~	~~2, 0~~

Figure 15: Example of Eliminating Dominated Strategies (step 4/4).

2.7.2 Maxi-Min strategies in strictly competitive or zero-sum game

A strictly competitive game is a two-player strategic situation where for each $a \in A$, the following equation is true: u1 (a) + u2 (a) = 0, where u1 and u2 are the payoff function of player 1 and player 2 respectively. This implies that when Player 1 outcome is positive then his opponent outcome will be negative and vice versa.

In zero-sum games, each player should try to minimize his losses by taking into account the worst possible outcomes. Maxi-min is the technique for calculating the best strategy in a zero-sum game.

2.7.2.1 The Maximinimizer Theorem [15, 18, 19]

Let G be a strictly competitive game.

- If the pair (x*, y*) is a Nash Equilibrium of G then it means that x* is a maximinimizer for player 1 and y* is a maximinimizer for player 2.
- If the pair (x*, y*) is a Nash equilibrium of G then it means that $\max_x \min_y u_1 (x, y) = \min_y \max_x u_1(x, y) = u_1 (x^*, y^*)$.
- If $\max_x \min_y u_1 (x, y) = \min_y \max_x u_1(x, y)$ and x* is a maximinimizer for player 1 and y* is a maximinimizer for player 2, then (x*, y*) is a Nash equilibrium.

The following matrix displays a two-player zero-sum game with all the available actions of each player with their associate payoffs.

	Player 2			
Player 1	**ACTIONS**	**D**	**E**	**F**
	A	4, -4	3, -3	-7, 7
	B	2, -2	-1, 1	6,- 6
	C	-5, 5	7, -7	-2, 2

Figure 16: A Zero-Sum Game for the Illustration of the Maxminimizer Theorem.

<u>2.7.2.2 The Maximinimizer Strategy for Player 1:</u>

- Select the minimum over row values: (row 1 → -7, row 2 → -1, row 3 → -5).
- Select the value of the minimums which yields the maximum payoff: row 2 → -1.
- The maximinimizer technique aims to minimize the total loss that a player might suffer. The final outcome of the specific technique might lead to a Nash Equilibrium but this not always the case. On the other hand, if a Nash Equilibrium exists in a game, then the action profile is a pair of maximinimizers.

<u>2.7.2.3 The Maximinimizer Strategy for Player 2:</u>

- The maximum values over columns: column 1 → -5, column 2 → -1, column 3 → -7
- Minimaximizer: Column 2 → -1

An action X is called maximinimizer for Player 1or player 2 if:

$$\min_{y\in A2}\ u1(x^*, y) \geq \min_{y\in A2}\ u1(x, y) \text{ for all } x \in A1$$

In the specific game, the outcome of the Maxminimizer method showed the Nash equilibrium as well.

<u>2.8 Analysis of Games with Imperfect Information [17, 18, 19]</u>

As defined before, this category includes any game where at least one participant of the specific strategic situation is missing some information related to the rest players. Such games consist of much more realistic and important strategic situations. In the same category is the field of information warfare incidents. This section aims for a comprehensive analysis of this kind of games.

<u>2.8.1 Bayesian Games – Strategic games with imperfect information</u>

The kind of strategic games where the participants lack information related with their opponents is called "Bayesian Game". Similarly with the other strategic games, the participants are called players and each of them has a set with his available actions.

One major characteristic in the specification of the imperfect information is the existence of a set of states. A state is denoted by a complete description of the players' relevant characteristics including their available information and their preferences. A state is constructed for each collection of such kind characteristics that a player think that it is possible to occur.

At the beginning of such kind of games, a starting state should be constructed. The first state is not available to the players of the game. On the other hand, each player is possible to receive a signal that might lead some information about the current state of the game.

The signals will be produced by a signal function τ_i. The signals function of the game, are deterministic functions. This means that for each state there exist a specific signal which will be determined by the signal function. For example, the i^{th} player might receive a signal ω by τ_i (ω) in the state ω. Each state which generates any given signal t_i is said to be consistent with t_i. The sets of states consistent with each of the player i's signals, indicate how accurate are the information of player i's. In the case where τ_i (ω) is different for each value of ω, it means that the player which receives the specific signal, gains the knowledge of the current state (after receiving the signal, he is perfectly informed about the characteristics of the rest participants of the game). On the other hand, if τ_i (ω) is the same for all different values of ω, it means that the player who receives the signal will not gain any information about the current state of the game (will not informed about the current characteristics of the rest players of the game). Another possible case for the function τ_i (ω) is where τ_i (ω) is constant for subsets of the whole set of possible states. In the latter case, the player who receives the signal gets partial informed about the current state of the game. If for example there exist three states ω1, ω2 and ω3 where ω1 ≠ ω2 ≠ ω3 and for all these three states the signal which the player receives is always the same, then the player will only have the knowledge that the current state is one of these three sets.

When a player i receives a signal t_i, then he becomes type t_i of player i. The different types of each player hold their beliefs about the likelihood of the states consistent with his signal. Imagine for example $t_i = \tau_i$ (ω1) $= \tau_i$ (ω2), then the type t_i of player i will assign probabilities to the two different types states ω1 and ω2.

The players of Bayesian games want to know the choices made by their participants as well as the current state of the game. Because of the fact that many of the players might be not certain about the state of the game they must specify their preferences regarding probability distributions over pairs (α, ω). The first component of the pair indicates an action profile and the second component shows a state. The preferences of each player in such kind of probability distribution are represented by the expected value of Bernoulli payoff function.

The actions of each player are independent of the state. The set of actions available to each player are always the same in each state.

2.8.1.1 Bayesian Game Components

The components of a Bayesian game are the following:

- A set of players.
- A set of states.
- A set of actions for each player.
- A signal function and a set of signals (each signal is produced by giving the state to the signal function) for each player.
- A belief about the states consistent with the signal (a probability distribution over the set of states with which the signal is associated) for each player.
- A Bernoulli payoff function over pairs (α, ω), where α indicates an action profile and ω indicates a state (this is the expected value of which represents the player's preferences among lotteries over the set of such pairs).

In order to acquire a better understanding of the Bayesian game components a recall to the BoS (Bash Stravinsky)game will be illustrated.

Players: Player 1 and Player 2.
States: Sets of states is: S = {meet, avoid}.
Actions: The set of actions for each player is: A = {Bach, Stravinsky}.
Signals: Player 1 might receive a signal x1 where his signal function τ_1 satisfies the equation: τ_1(meet) = τ_1(avoid) = x1. On the other hand, Player 2 might receive one of the two possible signals: ω1, ω2. Player's 2 signal function τ_2 satisfies τ_2 (meet) = ω1 and τ_2 (avoid) = ω2.
Beliefs: Because of the fact that Player's 1 signal function replies with ω1 for both possible states, he will assign a probability of ½ to each state after he receives the signal x1. Player 2 will assign probability 1 to the state meet after he receives the signal ω1 and probability 1 to the state avoid after he receives the signal ω2.
Payoffs: The payoffs for the specific game are displayed in the following matrices.

For the pair (a, meet) of each player i the payoffs are:

	Player 2		
Player 1		Bach	Stravinsky
	Bach	2, 1	0, 0
	Stravinsky	0, 0	1, 2

Figure 17: The Bach Stravinsky Game – Player 2 prefer to meet Player 1.

For the pair (a, avoid) of each player i the payoffs are:

	Player 2		
Player 1		Bach	Stravinsky
	Bach	2, 0	0, 2
	Stravinsky	0, 1	1, 0

Figure 18: The Bach Stravinsky Game – Player 2 prefer to avoid Player 1.

In a Bayesian game, each player is asked to choose not only one action but an action for each signal he might receive. Thus, each type of each player should choose an action. In such games, a player's choice is optimal if are known to him all the actions that were chosen from all the other players of the game. A type k of player i is not affected from any other choices that have been made by the other types of the specific player i. Consequently, a Nash Equilibrium of a Bayesian game can be defined as a Nash Equilibrium of a strategic game where each player is defined as one of the types of one the players in the Bayesian game.

Let t_i be a type of player i. For each possible state ω, he knows the signal that was received by all the other players of the game (he knows every other player's type). The player i, combines the information which he derived by the known signals of the other players and his beliefs about the states of the game. This fact put him in the position to calculate his expected payoff for each of his choice and each collection of choices for the various types of the other players.

An illustration of player's 1 expected payoff of the Bash Stravinsky game where its components of the specific game were defined above will take place. Player 1 knows that Player 2 is type ω1 in the state meet and ω2 in the state avoid. He believes that the probability of each state to occur is ½. Subsequently player's 1 expected payoff by choosing B if type ω1 of player 2 chooses B and type ω2 of player 2 choose S is derived by the following equation:

$$\frac{1}{2} * \ u_1 * \big((B,B), meet\big) + \frac{1}{2} * \ u_1 * \big((B,S), avoid\big)$$

A general equation of the expected payoff of a Bayesian game is:

$$\sum_{\omega \in \Omega} \Pr(\omega \mid t_i) * \ u_i * \Big(\big(a_{i,} \, \hat{a}_{-i}(\omega)\big), \omega\Big),$$

Ω is the set of states.
ω is the current state.
a_i is the action which player i chose.
$\hat{a}_{-i}(\omega)$ is the action chosen by every other player j.

2.8.2 Bayesian Equilibrium (Nash Equilibrium of Bayesian Games)

The Bayesian equilibrium is an extension of the Nash equilibrium and handles situation where at least one player in a game does not have complete information about his opponents and he is not able to figure out his opponents strategies with confidence. Games with incomplete information consist one of the categories that use Bayesian equilibrium. The Bayesian Equilibrium consists of mixed strategies. Mixed strategies is a probability distribution over the whole set of action of all the participants of a game. Actions that have the value zero indicate that there is no possibility for a player to proceed with the specific action in the game. On the other hand, if an action has the value 1, it indicates that the player will proceed only using the specific strategy (pure strategy).

The Nash Equilibrium of a Bayesian game is defined as a Nash Equilibrium of the strategic game with the Von Neumann–Morgenstern (vNM) properties:
Players: The set of all pairs (i, t_i). The first component represents the players in the Bayesian game and the second component represents the signals that the players might receive.
Actions: The set of actions of each player (i, t_i). This set represents the available action of player i in the Bayesian game.
Preferences: The Bernoulli payoff functions of each player (i, t_i). The equation of the expected payoff for each player is given in the equation above.

Imagine for example the Rock-paper-scissors game being played by two people. This is a hand-game and each of the two players is asked to choose one of their three available choices randomly. The rock is represented by a clenched fist, the scissors is represented by two fingers extended and separated and finally the paper is represented by an open hand, with the fingers connected horizontal. The objective is to select a gesture which defeats that of the opponent. Rock blunts or breaks scissors so rock defeats scissors, scissors cut paper so scissors defeats paper and paper captures rock so paper defeats rock.

	Player 2			
Player 1		**Rock**	**Paper**	**Scissors**
	Rock	0, 0	-1, 1	1, -1
	Paper	1, -1	0, 0	-1, 1
	Scissors	-1, 1	1, -1	0, 0

Figure 19: The Rock Paper Scissors Game.

The Rock-paper-scissors game has no pure strategy Nash Equilibrium. Because of this fact, each player will assign probabilities to each of the possible actions that his opponent is able to take. For example, player 1 will think that player 2 will play rock with probability m, paper with probability n and scissors with probability 1-(m+n).

The expected payoffs of player 1 for each of his possible actions are:

- Rock: m * (-1) + n * (1) + (1-(m+n)) * (1)
- Paper: m * (1) + n * (-1) + (1-(m+n)) * (1)
- Scissors: m * (1) + n * (1) + (1-(m+n)) * (-1)

When player 1 will solve all these three equations according to the probabilities he assigned to each of the possible actions of player 2, then he will decide with which action to proceed.

2.8.3 The Bach and Stravinsky (Battle of the Sexes)

This is a two-player game where two friends are trying to decide where to go out for the night. There are two concerts available at the specific night: one of music by Stravinsky and one of music by Bach. Player 1 prefers to go to a Bach concert and player 2 prefers to go to a Stravinsky concert.

Player 1 is not sure whether Player 2 really wants to meet him and go out together or avoid him. In such a case, Player 1 will give a 0.5 probability to each of the two possible scenarios he thinks that might occur. On the other hand, Player 2 knows is fully informed about the preferences of Player 1.

The two possible games of the pre-described scenario are the following:

	Player 2		
Player 1		**Bach**	**Stravinsky**
	Bach	2, 1	0, 0
	Stravinsky	0, 0	1, 2

Figure 20: Player 2 wants to go out with Player 1.

The Probability of this scenario to occur is 0.5.

	Player 2		
Player 1		**Bach**	**Stravinsky**
	Bach	2, 0	0, 2
	Stravinsky	0, 1	1, 0

Figure 21: Player 2 does not want to go out with Player 1.

The Probability of this scenario to occur is 0.5.

In a strategic game, Nash equilibrium models a steady state with correct beliefs of each participant about the actions of their opponents. As it was described above, Player 1 is not sure whether Player 2 wants to meet him or not. From Player's 1 side of view, player two has two options. The preferences of the two possible types of player 2 are given on the two tables above. Because of the fact that Player 1 is missing the information of what type player 2 is, and in order for him to make a rational choice, he is obligated to form a belief about the action that each type will take.

Player 1 gives his beliefs about what action might be taken by each type of player 2 together with his beliefs about the likelihood of each type to be real. Now he has all the information needed to calculate his expected payoffs. Imagine for example that player 1 thinks that that the type who wishes to meet him will choose action B and the type who wishes to avoid him will choose action S. In this case, action B will gain her a payoff of 2 with probability ½ and a payoff 0 with probability of ½, so his expected payoff is 2 * ½ + 0 * ½ = 1. When player 2 second type chooses S, player 1 will gain a payoff 0 with probability ½ and a payoff 1 with probability ½, so his expected payoff is 0 * ½ + 1 * ½ = ½. By doing the same calculations for the rest combinations of actions for the two types of player 2, the following table with all the expected payoffs for player 1 will be derived.

		Player 2			
Player 1		**(B, B)**	**(B, S)**	**(S, B)**	**(S, S)**
	B	2*1/2 + 2*1/2 = 2	2*1/2 + 0*1/2 = 1	0*1/2 + 2*1/2 = 1	0*1/2 + 0*1/2 = 0
	S	0*1/2 + 0*1/2 = 0	0*1/2 + 1*1/2 = 1/2	1*1/2 + 0*1/2 = 1/2	1*1/2 + 1*1/2 = 1

Figure 22: The Expected Payoffs of Player 1 for the Four Possible Pairs of Actions of the Two Types of Player 2.

Each row corresponds to an action of player 1and each column corresponds to a pair of actions of the two types of player 2. The first action corresponds to the type of player 2 who wishes to see player 1 and the second action to the player 2 who does not want to go out with player 1.

In this situation, the two different types of player 2, where treated as two different players. This fact transformed the specific situation form a two-player game to a three-player game. Player's 1 payoffs were given as a function of the actions of the two other players. The payoff of each type of player 2, is independent of the action of the other type, and depends solely to the action of player 1.

Although player 2 knows his preferences, an analysis of what the best action for him should be in either case is stated. This analysis is done in order to consider what he would do in both scenarios. Player 1 will have a clear view of what his opponent is most likely to choose to play a rational game which will maximize his payoff. Player 1 must form a correct belief (imposing the equilibrium condition that the player's belief is true) of what player 2 will do in each situation so that for each type of player 2, player's 1 belief will form his best response (Nash equilibrium). Consequently, the Nash equilibrium action for each type of player two may be interpreted as player's 1 correct belief about the action that each type of player 2 is most interested because it will yield him his maximum outcome and not as a plan of action for player 2.

In the specific situation, a pure strategy Nash Equilibrium is a triple of actions (x, (y, z)). The first value(x) indicates the action of player one and the rest two values(y, z) shows the actions of each type of player two. The action of player one(x), is optimal given the actions of the two types of player two and player's one belief about the game state. Furthermore, the action of each type of player two is optimal given the action of player one.

Having on mind that the best action of player 2 when he wants to meet player 1 is choosing the action B and that the best action of player 2 when he wants to avoid player 1 is choosing the action S, the Nash Equilibrium of this specific game is the triple (B, (B,S)). The first component of this triple is the action of player 1 and the rest components form the pair of actions of the two types of player 2. Having in mind the properties of the pure strategy Nash equilibrium, given the triple action above, by giving the action of the two types of player 2 as

(B, S) then player's 1 action B is optimal. Additionally, by saying that player 1 chooses B, if player 2 wishes to meet player 1, then the action B is optimal otherwise, action S is optimal.

The best response for each player in a Bayesian game is to try to maximize his expected payoff. The result of this method will be the Bayesian Nash Equilibrium.

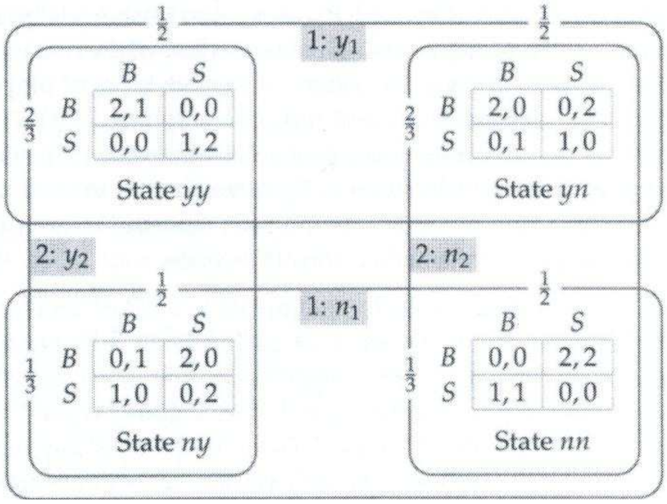
2.8.3.1 A BoS Game with Imperfect Information

In this variant of the BoS game, neither of the players have the information whether the opponent prefers to go out with him or avoid him. More precisely, player 1 thinks that with probability ½ player 2 wants to go out with him and with probability ½ player 2 prefers to avoid him. On the other hand, player 2 thinks that with probability 2/3 player 1 wants to meet him and with probability 1/3 player 1 prefers to avoid him. Each player knows only his own preferences and beliefs.

The specific game has four possible situations. The next figure displays the four possible situations that can be played with the outcome that each player can have:

- In the state yy, each player wants to go out with the other player.
- In the state yn, player 1 wants to meet player 2 but player 2 prefer to avoid player 1.
- In the state ny, Player 2 wants to meet player 1 but player 1 prefers to avoid player 2.
- Finally in the state nn, both players prefer to avoid each other.

Because of the fact that player 1 lack the information related with the preferences of player 2, it is not possible for him to distinguish between states ny and nn or yy and yn. Similarly, player 2 has the same problem. Because player 2 does not know the preferences of player 1, it is not possible for him to distinguish between states yn and nn or between states yy and ny.



	B	S
B	2,1	0,0
S	0,0	1,2

State *yy*

	B	S
B	2,0	0,2
S	0,1	1,0

State *yn*

	B	S
B	0,1	2,0
S	1,0	0,2

State *ny*

	B	S
B	0,0	2,2
S	1,1	0,0

State *nn*

Figure 23: A variant of BoS in which each player is unsure of the other player's preferences. [17]

In the figure above, the frame labelled i:x encloses the states that generate the signal x for player I. Also, the numbers appearing over this frame next to each table are the probabilities assigned by type x of player I to each state he regards to be possible [17].

In order to model the specific situation, the notion of signal is introduced. In this game it is assumed that each player receives a signal before choosing an action. As it was showed in the previous figure, player 1 receives the signal y1 for the states yy and yn and a different signal n1 for the states ny and nn. On the other hand, player 2 receives the signal y2 for the states yy and ny and a different signal n2 for the states yn and nn.

Similarly with the previous example, this game is transformed from a two-player game to a four-player game. There are two different types of player 1 and two different types of player 2. When player 1 receives the signal y1 is referred to as type y1 of player 1 or type n1 of player 1 after he receives the signal n1. Applying the same theory to the other player, player 2 has two types: y2 and n2.

Type y1 of player 1 believes that the states yy and y2 have a probability ½ to happen. Type n1 of player 1 believes that the states ny and nn have also a probability ½ to happen. Type y2 of player 2 believes that the state yy has a probability of 2/3 to happen and the state ny has a probability of 1/3 to happen. Also, type n2 of player 2 believes that the state yn has a probability of 2/3 to happen and the state nn has a probability of 1/3 to happen. The matrices for the expected payoffs for each of the four possible situations are shown below:

y1	**Player 2**				
Player 1		**(B, B)**	**(B, S)**	**(S, B)**	**(S, S)**
	B	2*1/2 + 2*1/2 = 2	2*1/2 + 0*1/2 = 1	0*1/2 + 2*1/2 = 1	0*1/2 + 0*1/2 = 0
	S	0*1/2 + 0*1/2 = 0	0*1/2 + 1*1/2 = 1/2	1*1/2 + 0*1/2 = 1/2	1*1/2 + 1*1/2 = 1

Figure 24: The Expected Payoffs of Player 1 for the Four Possible Pairs of Actions of the Two Types of Player 2 for the State y1.

n1	**Player 2**				
Player1		**(B, B)**	**(B, S)**	**(S, B)**	**(S, S)**
	B	0*1/2 + 0*1/2 = 0	0*1/2 + 2*1/2 = 1	2*1/2 + 0*1/2 = 1	2*1/2 + 2*1/2 = 2
	S	1*1/2 + 1*1/2 = 1	1*1/2 + 0*1/2 = 1/2	0*1/2 + 1*1/2 = 1/2	0*1/2 + 0*1/2 = 0

Figure 25: The Expected Payoffs of Player 1 for the Four Possible Pairs of Actions of the Two Types of Player 2 for the State n1.

y2	**Player 2**				
Player 1		**(B, B)**	**(B, S)**	**(S, B)**	**(S, S)**
	B	1*2/3 + 1*1/3 = 1	1*2/3 + 0*1/3 = 2/3	0*2/3 + 1*1/3 = 1/3	0*2/3 + 0*1/3 = 0
	S	0*2/3 + 0*1/3 = 0	0*2/3 + 2*1/3 = 2/3	2*2/3 + 0*1/3 = 4/3	2*2/3 + 0*1/3 = 4/3

Figure 26: The Expected Payoffs of Player 1 for the Four Possible Pairs of Actions of the Two Types of Player 2 for the State y2.

n2	**Player 2**				
Player1		**(B, B)**	**(B, S)**	**(S, B)**	**(S, S)**
	B	0*2/3 + 0*1/3 = 0	0*2/3 + 1*1/3 = 1/3	1*2/3 + 0*1/3 = 2/3	1*2/3 + 1*1/3 = 1
	S	2*2/3 + 2*1/3 = 2	2*2/3 + 0*1/3 = 4/3	0*2/3 + 2*1/3 = 2/3	0*2/3 + 0*1/3 = 0

Figure 27: The Expected Payoffs of Player 1 for the Four Possible Pairs of Actions of the Two Types of Player 2 for the State n2.

As in the previous example, in order to study the equilibrium for this game, the players' plans before they receive their signals are taken into account. Considering that the game has now four players (two types of player one and two types of player two) instead of two, a Nash Equilibrium should be constructed by four actions (one for each of these players). In this way, the action of each type of the original player is optimal when he gives his belief after he received his signal and the actions of his opponent.

The Nash Equilibrium of the specific game consist the four actions: ((B, B), (B, S), (S, B), (S, S)). The first two pairs represent the actions of the two types of player 1 and the rest two pairs shows the actions of each type of player two. More analytically:

- (B, B) is the pair of best response for player 1 type y1
- (B, S) is the pair of best response for player 1 type n1
- (S, B) is the pair of best response for player 2 type y2
- (S, S) is the pair of best response for player 2 type n2

All these can be checked using the four previous figures that show the expected payoff of each type of player.

3. Game Theory Models of Information Warfare

This section makes an overview of proposed game theoretic-security models for defending cyber incidents. The two most important security mechanisms which are responsible to defend denial of service attacks and malicious system's intrusions are enhanced to utilise game theory principles. Two proposed game theoretic models of DoS/DDoS attacks and one of intrusion detection are analysed. Furthermore, the powerful fictitious strategy of playing a game is described. The last section of this chapter analyse the very interesting Flip It game which is capable for analysing the state of the system within a game and analyse players' performance.

In order to apply the game theory principles to information warfare, a modelling of the components of a game related to an information incident is required. David A. Burke created his information warfare model using the pyramid of data shown below.

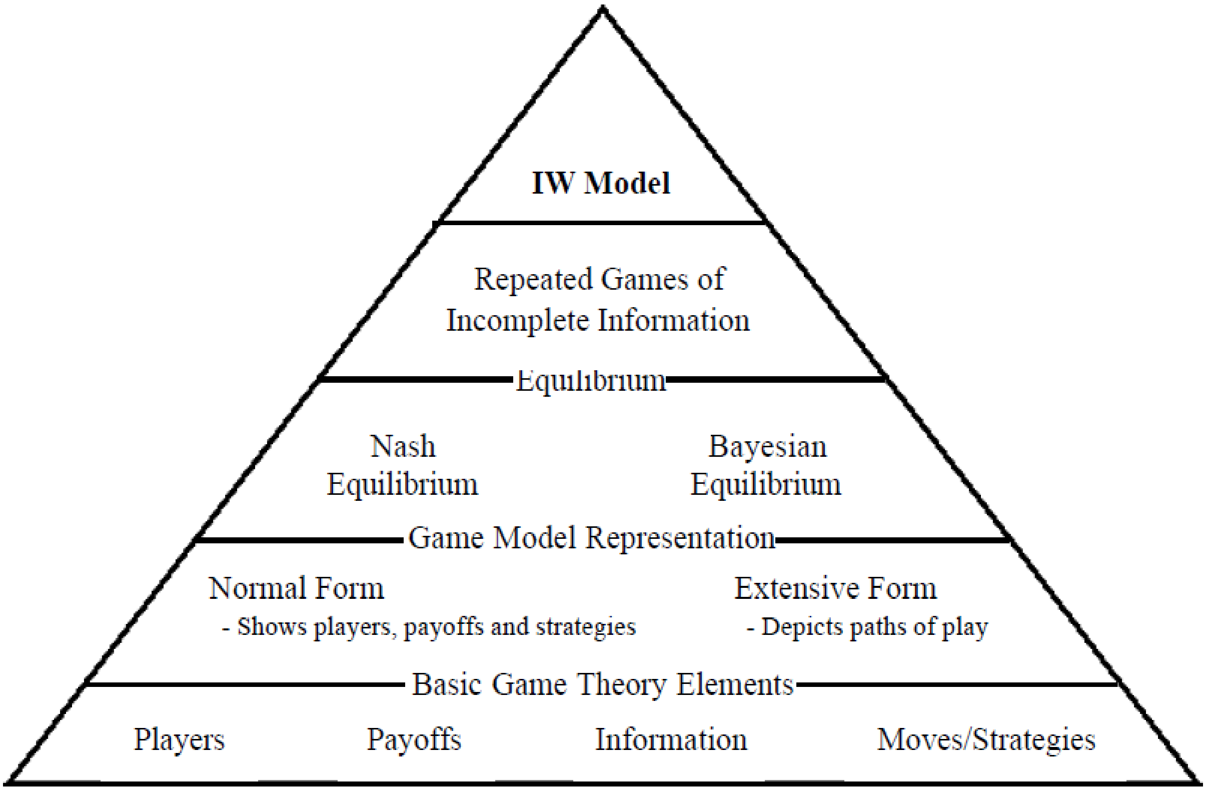


Figure 28: The Construction of an Information Warfare Game Model [20]

3.1 Description of the Game Theory Elements Applied to Cyberwarfare [20]

In order to apply game theory principles to information warfare the modelling of each component should take place. A general game consists of:

- Players
- Information
- Payoffs
- Moves/Strategies

The components of an information warfare incident should customize to suit the components of a game. This is not a very difficult procedure because of the fact that game theory is a methodology which analyse competitive situation like the ones that appear in a cyber warfare incidents.

3.1.1 Players

Most researchers on the specific domain consider the information warfare incidents as two-player games. Generally, the players of such kind of incidents include one attacker and one defender. In all the games, the defender is the same and incarnated by the system administrator of the system that is under attack. Alternatively, the attackers are much more difficult to model because of the fact that there are many different types of cyber adversaries. Usually the attacker is characterized by his objectives and his methodology that follow to accomplish his goal.

A very strong assumption exists in all kind of games. All the participants of a game are rational and therefore they will always choose rational actions. In other words, the players are aiming to maximize their income and minimize their losses. Also, all the players assume that their opponents are also rational.

3.1.2 Information

When a game has complete and perfect information, it means that the payoff function of each player, the moves of each player and the history of the game is common knowledge. This kind of games that do not involve any players' beliefs it is assumed to have perfect rationality. Any other game which is described by incomplete or imperfect information obligate the players to utilise their beliefs in order to make estimations related to their opponents moves, preferences and payoffs. Payoffs and preferences many times are combined. The action that gives the maximum payoff to the player it is assumed that is the preference of the player as well.

The uncertainty of a player about his opponents forms many times the reason that a player cannot play strictly rational. Usually, the beliefs of each player are modelled as a probability distribution function over their opponent's set of actions and payoff structures.

3.1.3 Payoffs

The payoffs that each player receive after an action he chose, is the prime driver of game play. The payoffs of each action should be clear for each player. Most games represent the actions payoffs in purely numeric values or monetary terms. In all games, the players are aiming to choose the action that will earn them the maximum payoff in any possible action that their opponent might choose.

Incomplete or imperfect information games are driven by expected payoffs. Expected payoff of an action is when the player assigns probabilities to the set of possible actions. In this way, the players are estimating the likelihood of each possible game course to happen and they discount their own payoff based on their estimate.
There are two main types of payoff functions:

- Zero-sum Games
- Non-zero sum Games

Zero-sum games involve situations where one player's gain is exactly balanced by the losses of his opponent's. If the total gains of the participants are added up, and the total losses are subtracted, they will sum to zero. Another name of zero-sum games is strictly competitive games. Such games are usually solved by utilising the Minima
x theorem (section 2.7.2).

Non-zero sum games involve situations where the outcome is greater or less than zero. In such games, the gain of one player does not necessarily correspond to an exact loss of another player. This category of payoff functions which include most of the information warfare incidents is non-zero sum games. This is because of the fact that the gains of one player are difficult to be compared to the losses of other players.

3.2 Incomplete Information – Player Types [13, 20]

In the beginning of each game, none of the players is fully informed about the game characteristics. In other words, the players are not certain with who are going to have a battle with. In general terms, if a player has a strong competitor, he knows that it is much more difficult to beat him or have large amounts of positive payoffs. On the other hand, a player who is facing a weak opponent knows that is much easier for him to beat him and maximize his earns.

The inference of the above statement is the fact that different types of players have different moves, payoffs etc. Thus, information about the opponent might derived by classifying the opponent to one possible category.

A naive example of the specific statement could be derived by a tennis game. Imagine that two tennis players will play against each other for the first time during the Olympic Games. Both players do not know anything about the other player. The following game will described by player's A side of view. Player A knows that will have a tennis game with Player B and he is wondering which the strong and weak note of his opponent is in order to maximise his probability to win the game. In order to simplify the game, we assume that there are only to possible types of hitting a tennis ball: forehand and backhand. Player A will have to make a guess of what type his opponent is and try to return the ball to his opponent's weak note. After a few points, player A will acquire a few more information about his opponent and refine his strategy that followed to the previous points. During the progress of the game it might be possible for player A to get fully informed about his opponent and easily manage to solve the complete information game.

		Player B	
		Forehand	Backhand
Player A	Forehand	5, 5	8, 2
	Backhand	9, 1	2, 8

Figure 29: A Tennis Game (Illustration of Different Player Types).

After each player utilise a probability distribution function over the possible opponents' types, the following table is derived:

		Player B	
		Forehand (FH) **Pr(BH) = m**	**Backhand (BH)** **Pr(BH) = 1-m**
Player A	**Forehand (FH)** **Pr(FH) = k**	Game 1 Pr(Game 1) = m*k	Game 2 Pr(Game 2) = (1-m) * k
	Backhand (BH) **Pr(BH) = 1-k**	Game 3 Pr(Game 3) = m*(1-k)	Game 4 Pr(Game 3) = (1-m) *(1-k)

Figure 30: Probability Distribution over the Players' Types.

The next figure displays an extensive form of a static game of the above example. The payoffs were randomly selected.

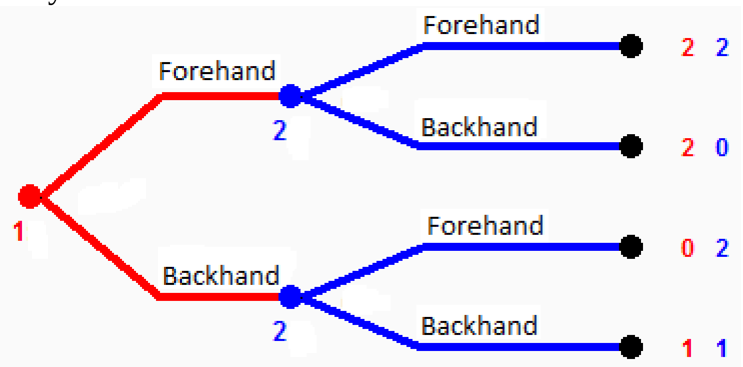


Figure 31: The Extensive Form of the Tennis Game.

3.3 Information Warfare Methodology [20]

In general, information warfare participants employ the following methodology which encompasses the following steps:

- Select and launch a particular strategy.
- Assess the outcomes of the selected strategy when is completed.
- Refine and try to improve the selected strategy based on the outcomes.
- Launch the new refined strategy.

Modelling information warfare incidents as a game is a very difficult and complex procedure. Such scenarios are very rare to be modelled accurately in a one-shot game. Usually, cyber incidents are repeated games and in fact, a more realistic game could be even a correlated series of one shot games. An action of the one player at an earlier stage of the game will consider as bonus information for his opponents. Analysis of previous actions of one player will affect the next move of the other players.

A simple example for illustrating a repeated game is the prisoner's dilemma game. Two criminals are arrested and are the major suspects for a crime. The police do not have enough evidence to convict any of these two prisoners. The suspects are in different cells so they cannot communicate during the process, thus they do not know what the other has chosen to do. If neither confess they will convicted only for a minor crime and sentenced only for five months. If they both testify that they committed the crime then they will both sentenced for five years. Finally, if the one confess and the other stay silent, the confessor one will released and the other will sentenced for ten years.

		Prisoner B	
		Silent	**Testify**
Prisoner A	**Silent**	A: 5 Months B: 5 Months	A: 10 Years B: Free
	Testify	A: Free B: 10 Years	A: 5 Years B: 5 Years

Figure 32: The prisoner's Dilemma Game.

Suppose that prisoner A decides to choose a long-term strategy. Applying his strategy, he chooses testify as long as his opponent choose the same but when his opponent decides to stay silent he also chooses to remain silent. Prisoner B on the other hand, should now analyse how prisoner A response and adjust his choices according to the other player actions. The specific type of game is called repeated games with sequences of history-dependant game strategies. Similarly, the cyber incidents should have a similar template. The defender should wait for the attacker action and response with a proper activity.

3.4 Game theory application in DoS and DDoS attacks [5, 21, 22]

The most important kind of attacks on information systems by cyber criminals is the denial of service (DoS) attack. The adversary aims to collapse the targeted information system and make its resources unavailable to legitimate users. The unavailability of the system resource has as ultimate purpose to prevent an internet site or service from functioning efficiently or at all. DoS attacks targets are most times critical infrastructures like banks, famous websites, governments, embassies et al. where a possible corruption of their services will cause them huge losses in terms of money, reputation and reliability.

Most common method of DoS attacks involves an adversary who is able to send a much larger number of requests that the targeted server can handle in order to make him unavailable to respond to legitimate traffic, or respond very slowly.

The challenge of the defender is to distinguish legitimate users' actions from illegitimate users' actions. The firewall of the system is the primary source of the administrator from where he will acquire the history of the actions that take place within the system. The system administrator must be able to block any detected rogue traffic while in the same time allowing authorised ones.

3.4.1 Network Topology – The Game Board

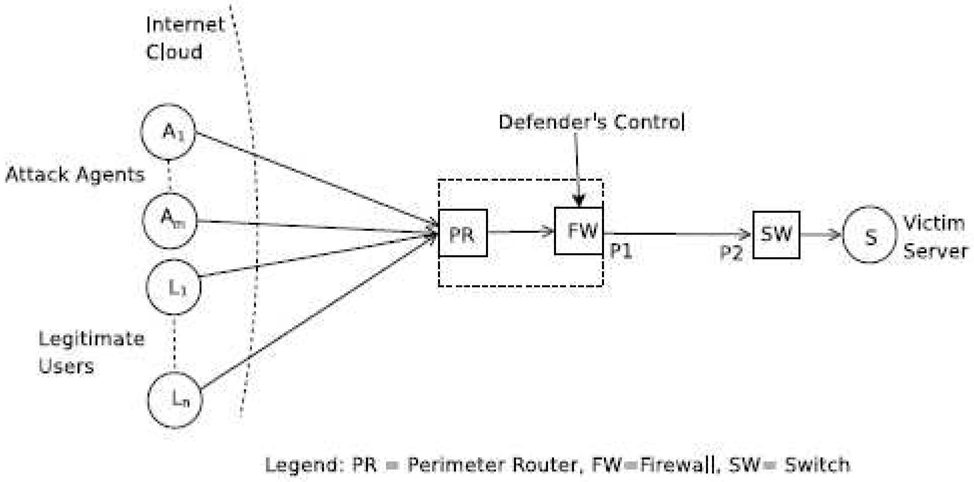


Figure 33: Network Topology for DoS/DDoS Attacks [21]

The figure above, depict a generic network topology for DoS/DDoS attacks. On the left hand side there are the users who are interested to communicate with the server S. There are n legitimate users and m adversarial users who aim to launch a DoS/DDoS attack. The difference of DoS attack from DDoS attack is the fact the m is equal to one. The internet is connected to the server through the perimeter router, the firewall and the switch. The bandwidth between the perimeter router and the firewall is unlimited. On the other hand, the bandwidth between the firewall and the switch is limited and is subject to DoS and DDoS attack.

For the specific scenario, a single attacker is the one that controls all the adversarial nodes. The defender is not able to know if a packet is legitimate or malicious. The administrator's belief about the legitimacy of the packet's flow decreases when the number of packets which pass through the firewall increases. Packets of the flow are possible to drop in two places: the firewall and the pipe p1. The latter, it is possible to happen when the flow rate is more than the available bandwidth.

3.4.2 Game Model

The DoS/DDoS attack is modelled as a two-player non-zero sum game. The two players are on the one side the adversary (attacker) and on the other side the system administrator (defender). The attacker is the person who will try to find some zombies (adversarial nodes) and exploit them to increase the server's traffic and the defender is the one who is responsible to prevent the illegitimate requests to make his server not functional.

The attacker's goal is to find the most effective packet sending rate which will not sound the alarm that the system is under attack. The defender will try to find the best firewall settings to block malicious traffics while allowing authorised ones.

3.4.3 Defender's Information – Legitimate User Profile

The system administrator considers the presence of n legitimate users interested to use the services provided by the server S. In order to model the sending rate of a legitimate user, the administrator will pick a random number. More specifically, the administrator must pick n samples from a Normal Distribution:

$$X_i \sim N\ (r_l, \sigma_l^2)$$

i = 1, 2, 3...,n where X_i represents the sending rate of the ith user, r_l is the mean value of a legitimate user's sending rate and σ_l is the standard deviation.

Consequently, the total incoming flow rate with no attacks is

$$\vartheta = X_1 + X_2 + X_3 + \ldots + X_n$$

By basic laws of probability the following equation is constructed:

$$\vartheta \sim N\ (n * r_l, n * \sigma_l^2)$$

Having this on mind, the bandwidth β between the firewall and the switch is chosen such that the total incoming legitimate flow is less than β with high probability:

$$\vartheta < \beta$$

3.4.4 The moves

There are two available actions to the attacker:

- Choose the number of the adversarial nodes: value m.
- Set the sending rate: value r_A.

It is assumed that the sending rate for each node is the same for all of the attacking flows. Thus, the total flow rate during an adversarial situation is calculated by:

$$T = (X_1 + X_2 + X_3 + \ldots + X_n) + m * r_A$$

In the situation where the bandwidth β between the firewall and the switch is less than T ($\beta < T$) it means that the denial of service is successful because of the congestion condition that will occur between the pipes p1 and p2.

3.4.5 Attack with the absent of defence

In the case where the defence mechanisms are not activated, all the packets of each flow will be able to pass the firewall. Nevertheless, when the total flow rate (T) is greater than the bandwidth β, only a portion of the packets which are contained in the specific flow will manage to pass through the pipe p1 and reach the pipe p2. This portion of packets is defined by a fraction α. The fraction α which indicates the number of the packets that can pass p1 is the same for all the flows. This means that (1 – α) fractions of each flow will dropped at point p1. When the bit rate of a flow is r, only $\alpha * \mathrm{r}$ bit rate will reach the server. Also, assuming that the bandwidth resource is shared equally: $\alpha = \frac{\beta}{T}$.

If γ indicates the minimum bit rate of a flow to be considered as a flow and n_g is the average number of legitimate flows able to reach the server it means that:

$$n_g = n * P\left[X_i > \frac{\gamma}{\alpha}\right],$$

where n is the total number of legitimate flows and P[X>x] is the probability that the value of the random variable X is higher than x.

In the same sense, a portion of packets of an attacking flow will also be dropped at p1 point. The attacker's average bandwidth consumption ratio is calculated by:

$$v_b^{no\_defence} = \frac{m * \alpha * r_A}{\beta} = \frac{m * r_A}{(n * r_l) + (m * r_A)}$$

The average ratio of lost users to the total number of users is calculated by:

$$v_n^{no\_defence} = \frac{n - n_g}{n} = P\left[X_i < \frac{\gamma}{\alpha}\right] = P[X_i < \frac{\gamma\,(n * r_l + m * r_A)}{\beta}]$$

The main goal of the attacker is to increase $v_b^{no\_defence}$ and $v_n^{no\_defence}$ and these are consider as his payoffs as well. The cost that the attacker has is the procedure to take the control of a legitimate node and transform it to an adversarial node. The attacker's total cost is proportional to the number of nodes that he has under his control and is indicated by:

$$v_c = \mathrm{m}$$

The attacker's net payoff of the above three quantities can be modelled as a weighted payoff by:

$$V^a = w_b^a * v_b^{no\_defence} + w_n^a * v_n^{no\_defence} - w_c^a * v_c,$$

where w_b^a, w_n^a and w_c^a are the attacker's corresponding weighted coefficients.

The defender's net payoff can be modelled as a weighted payoff by:

$$V^d = -w_b^d * v_b^{no\_defence} - w_n^d * v_n^{no\_defence} + w_c^d * v_c,$$

where w_b^d, w_n^d and w_c^d are the defender's weighted coefficients.

3.4.6 Attacks with the Firewall Activated

The firewall represents the shield of the network administrator. It is capable to drop a portion of packets of an incoming flow with a probability which depends on the flow rate. The dropping rate is modelled by the following function:

$$F(x) = \frac{1}{\left(1 + e^{-\delta * \frac{(x-m)}{\beta}}\right)},$$

where parameter M represents the flow rate for which the drop rate is 0.5 and δ is a scaling parameter.

The role of the firewall is to drop the portion of packets of a flow of rate r according to the probability F(r). It is obvious that in such situations, some of the packets that are dropped by the firewall belong to legitimate users. The only defence action of the defender is the assigning of the value M. The following graph depicts several dropping rates of sample functions where β = 1000 units and $\delta = 20$. The dropping rate of the firewall is modelled by the S curves.

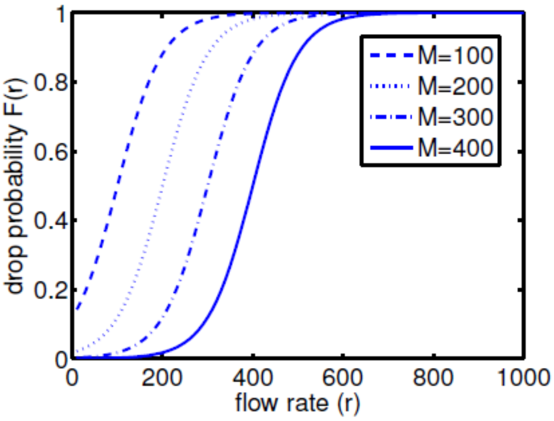


Figure 34: Samples of Dropping Rates of the Firewall. [21]

Having on mind that r_l is the expected rate of a legitimate user then $r_l^{'}$ represents the average rate of legitimate flows passing through the firewall. This means that $r_l^{'} = (1 - F(r_l))$. In the same sense, r_A is the bit rate of an attack flow so $r_A^{'}$ represents the average of attacking flows passing through the firewall. This means that $r_A^{'} = r_A * (1 - F(r_A))$.

The ratio of average bandwidth consumption by the attacker is calculated by:

$$v_b = \frac{m * r_A^{'}}{\left(n * r_l^{'}\right) + \left(m * r_A^{'}\right)}$$

The average ratio of lost users to the total number of users is calculated by (the right hand side of the equation, considers both the losses depending on the firewall and the congestion):

$$v_n = P[X_i < \frac{\gamma\,(n * r_l' + m * r_A')}{\beta}]$$

The attacker's payoff is calculated by:

$$V^a = w_b^a * v_b + w_n^a * v_n - w_c^a * v_c,$$

The defender's payoff is calculated by:

$$V^d = -w_b^d * v_b - w_n^d * v_n + w_c^d * v_c$$

3.4.7 Nash Equilibrium

The objective of both players is to maximize their payoff. From the attacker's side of view, he must choose optimal values for m and r_A. From the defender's side of view, he must choose optimal value for M which is being used by the firewall. The Nash Equilibrium of the specific game is a pair of strategies $\{(r_A^*, m^*)\ ,\ M^*\}$. A Nash equilibrium should also satisfy the following two relations:

$$V^a_{(r_A^*,\, m^*,\, M^*)} \geq V^a_{(r_A, m,\, M^*)}\ \forall\, r_A, m$$

$$V^d_{(r_A^*,\, m^*,\, M^*)} \geq V^d_{(r_A^*,\, m^*, M)}\ \forall\, M$$

3.5 Game Inspired Defence Architecture (GIDA) [5, 23]

GIDA is another model which utilise game theoretic principles in order to counteract any potential DoS/DDoS attacks. Adversarial nodes attempt to break down network links by exhausting limited bandwidth. The interaction between the attacker and the network administrator is considered as a two-player non-zero game. The attacker's optimal strategy is once more the choice of the appropriate effective sending rate and the number of botnets (adversarial nodes). On the other hand, the defender must define the optimal firewall settings which will allow the flow of legitimate packets and in the same time to block any adversarial packets. The network topology of the GIDA model is displayed in the next figure.

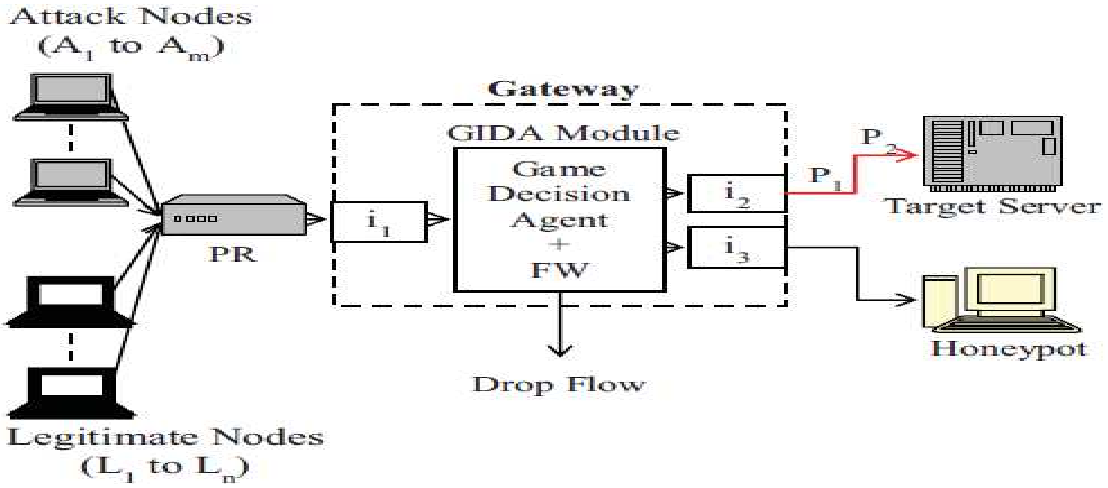


Figure 35: GIDA Network Topology [22].

As shown in the above figure, the target server is accessible to the internet via a Gateway (GW) machine. On the left hand side there are n legitimate nodes which are interested to communicate with the server and m adversarial nodes which are controlled by the attacker in order to launch a DDoS attack. The traffic flow first pass through the perimeter router (PR) of the network and then enters the GW. The GW is an isolated machine which runs the GIDA module and it has three interfaces. The interface i_1 is connected with the internet via the PR, i_2 is connected with the Target server and i_3 is connected with the Honey-pot (HP). The GIDA monitors and analyse the flow which pass from i_1 interface and according to the decision of the GIDA module the traffic might dropped entirely or allowed to reach the server via interface i_2 or reach the HP via interface i_3. The scope of redirecting the traffic to HP is in order to make a more comprehensive analysis so that the defender might acquire more information from the attacker.

The network pipe p1 and p2 which connect the GW to the server has limited bandwidth. The objective of the attacker is to use the specific limited network bandwidth in order to prevent the legitimate users from using the server properly. High usage of the specific bandwidth will cause denial of service situation for the legitimate users of the server.

The GIDA module consists of two major components, the firewall and the game decision agent. The game decision agent is responsible for the analysis of the flow and the extraction of a decision which will be executed from the firewall.

3.5.1 Actions of the players:

The GIDA module has the following three classifications and actions available over the incoming traffic:

- Normal traffic: allow the traffic to reach the server
- Rogue traffic: prevent the traffic to reach the server and drop it using the firewall
- Redirect traffic: sent the rogue traffic to the HP for more comprehensive analysis in order to acquire more information about the attacker.

The available actions of the attacker are the following:

- Find vulnerable nodes and exploit them in order to make them in order to take them under his control.
- Adjust the rate of the packets that each malicious node will sent to the target server.

The attacker’s cost is proportional to the attacking nodes that has under his control. In the case where he use a small number of nodes but with high request frequency his cost will decrease but the specific flows have highest probability to dropped by the system. On the other hand, if the attacker utilise a larger number of nodes, his cost will increase. Nevertheless, because of the fact that the attacker will adjust the sending frequency of the nodes much lower, his benefits will increase since the attack becomes less obvious.

3.5.2 Legitimate user profile:

The profile of a legitimate user is modelled the same way as in the previous model which used a normal distribution: $s_i\colon N(s_l, \sigma_1^2), i = 1, 2, \dots, n$ where s_i represents the number of flows of the i^{th}user, s_l is the mean value of the legitimate user and σ_1 is the standard deviation.

If B is the available bandwidth between pipe p1 and p2, and S = $s_1 + s_2 + s_3 + \ldots + s_n$ then in a situation where there is no attack, the available bandwidth for each user is: $r^{no\_attack} = \frac{B}{S}$ (each flow gets an equal share of the bandwidth of the pipe p1 and p2). One countermeasure is the threshold bandwidth associated with each flow. If at any point, the bandwidth available to a flow is less than its threshold, then the specific flow is considered as dead. The threshold bandwidth of a legitimate flow is considered as a random variable and modelled using a normal distribution: $\Gamma_i: N(\gamma_{l,}\sigma_2^2), i = 1, 2, \ldots, S$ where Γ_i represents the threshold bandwidth of the i^{th} flow, $\gamma_{l,}$ is the mean value of a legitimate flow's threshold and σ_2 is the standard deviation.

A legitimate flow is possible to terminate in the absence of an attack with probability: $P[r^{no_{attack}} < \gamma_i]$ where γ_i represents the instantaneous value of Γ_i and P[x < X] represents the probability that the value of the random variable X is greater than x. The pipe bandwidth B is chosen such that P[$r^{no\_attack} < \gamma_i$].

Each flow has a pair of IP addresses. The first one indicates the source and the second one the destination. The modelling of each user flow is done using the amount of bandwidth used between one IP source/destination address pair.

3.5.3 Attacks with firewall disable

The bit rate r is the same for all the flows and the number of attack flows u is the same for all adversarial nodes. Thus, considering an attack situation, each flow rate is: $r = \frac{B}{S+m*u}$. The denial of service attack will occur when r is small.

If S_g is the average number of legitimate flows able to reach the server and they have rate greater than γ_l then:

$$S_g = S * P[\gamma_l < r]$$

The attacker's average bandwidth consumption ratio can be calculated by:

$$v_b^{no\_defence} = \frac{m * u}{S + m * u},$$

where S= legitimate flows, m * u = attack flows

The average ratio of lost legitimate flows against the total number of legitimate flows can be calculated by:

$$v_n^{no\_defence} = \frac{S - S_g}{S} = 1 - P\ [\gamma_l < r] = P[\gamma_l > r]$$

The attacker's cost is proportional to the number of the adversarial nodes that are under his control:

$$v_c = m$$

Considering the above three equations, the attacker's net payoff is modelled as a weighted sum of:

$$V^a = w_b^a * v_b^{no\_defence} + w_n^a * v_n^{no\_defence} - w_c^a * v_c,$$

where w_b^a, w_n^a and w_c^a are the attacker's corresponding weighted coefficients.

The defender's net payoff can be modelled as a weighted payoff by:

$$V^d = -w_b^d * v_b^{no\_defence} - w_n^d * v_n^{no\_defence} + w_c^d * v_c,$$

where w_b^d, w_n^d and w_c^d are the defender's weighted coefficients.

3.5.4 Attacks Vs GIDA Module

Previously, it was said that the defender has three available actions: allow traffic to reach the server, dropped the traffic and redirect traffic to the HP. In order for the defender to be possible to make his choices, he must choose two thresholds: E_1 and E_2.

For each source node, the defender must calculate its total flow rate which is r * u (r is the bit rate per flow and u is the number of flows for the specific node). The decision of GIDA is based on the following statements:

1. If $r * u < E_2$: The firewall allows to the set of flows from the specific source node K to reach the target server.
2. If $E_1 > r * u > E_2$: All the flows from the specific source node K are redirected to the HP.
3. If $r * u > E_1$: The firewall drops all the flows from the specific source node K.

Because of the fact that the specified decision statements are probabilistic in nature, there is a minute likelihood that even if $r * u < E_2$ the flows from the specific source node might drop.

The modelling of the allowing, dropping and redirecting probabilities of flows per source node is shown below by the utilization of the two thresholds E_1 and E_2.

$$F_1(x) = (1 + e^{-\beta * (\frac{x - E_1}{d})})^{-1}$$

$$F_2(x) = (1 + e^{-\beta * (\frac{x - E_2}{d})})^{-1}$$

Where E_1 and E_2 represent the flow rate for which the probability of dropping and redirecting a flow is 0.5, β is a scaling parameter, d is the bandwidth consumed per node (B/t). E_1 and E_2 are the only control parameters of the specific filters.

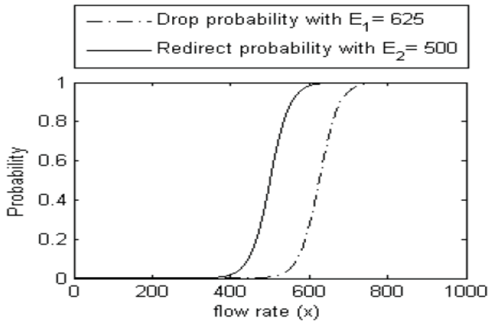


Figure 35: Plot of sample S curves – drop and redirect rate of a flow at the firewall [22]

The above figure, depicts a situation where B = 1000 units, t=2 and $\beta = 20$. With probability $F_1(x)$ and $F_2(x)$ the firewall drops and redirects a flow of rate x respectively.

The defender designs three probabilistic functions in order to make a decision:

- $F_a(E_1, E_2, x)$: The probability that a flow will be allowed to reach the server.
- $F_d(E_1, E_2, x)$: The probability that a flow will be dropped.
- $F_r(E_1, E_2, x)$: The probability that a flow will redirected to the HP.

The third argument of each function indicates the bandwidth consumed by a specific node (x = r * u, where r is a bit rate of each flow and u is the number of flows). The sum of the three probabilistic functions is one. The next figure shows how the two filters F_1 and F_2 work together in order to construct the three probabilistic functions F_a, F_d and F_r. The value x (total bit-rate for each source) is the input of filter F_1 which is responsible to create the probability whether the flow of the specific source should be dropped or not (F_d). The probabilities of redirecting a flow (F_r) and allowing the flow to reach the server (F_a) are constructed using the filters together. The probabilities are defined as follows:

- Dropping: $F_d = F_1$.
- Redirecting: $F_r = F_2 * (1 - F_1)$.
- Allowing: $F_a = (1 - F_1) * (1 - F_2)$.

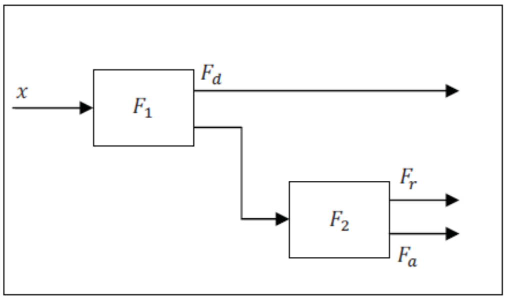


Figure 36: Filters F_1 and F_2 Arrangements for Computing the Probabilities of Allowing (F_a), Dropping (F_d) or Redirecting (F_r) Incoming Flows. [22]

Considering the fact that the attacker sends u flows from each attack node the following equations are derived:

Attacker's average bandwidth consumption ratio is calculated by:

$$v_b^d = \frac{m * u * F_a\,(E_1, E_2, r_a * u)}{S * \ F_a * (E_1, E_2, r_l * s_l) + \ m * u * \ F_a\,(E_1, E_2, r_a * u)}$$

The average ratio of lost legitimate flows over the total number of legitimate flows is calculated by:

$$v_n^d = \gamma_l > \frac{B}{S * \ F_a * (E_1, E_2, r_l * s_l) + \ m * u * \ F_a\,(E_1, E_2, r_a * u)}$$

where S = s_l * n; s_l is the mean value of the total number of flows for one legitimate node and n is the total number of legitimate users.

The defender makes usage of the HP when the attacker's total bit rate exceeds the threshold E_2. The defender's cost for using the HP is the same with the amount of information gained from the attacker by using the same. Each attacker requires an instantiation of a new HP and the cost of this procedure is a weight factor w_h^d. On the other hand, the attacker also has a cost if his flow is redirected because the specific flow does not assist him in accomplishing his goal thus a weight factor for the attacker is denoted as w_h^a.

The defender's benefit from the amount of flows redirected to the HP is calculated by:

$$v_h^d = m * u * F_r\ (E_1, E_2, r * u)$$

The new payoff functions of the attacker and the defender including the v_h^d are calculated by:

$$V^a = w_b^a * v_b^d + w_n^a * v_n^d - w_c^a * v_c - w_h^a * v_h^d,$$

where w_b^a, w_n^a, w_c^a and w_h^d are the attacker's corresponding weighted coefficients.

$$V^d = -w_b^d * v_b^d - w_n^d * v_n^d + w_c^d * v_c + w_h^d * v_h^d,$$

where $w_b^d, w_n^d\ w_c^d$ and w_h^d are the defender's weighted coefficients.

3.5.5 Nash Equilibrium

Both players ultimate goal is to maximize their payoffs. The attacker must choose values for variables m and u and the defender must choose values for E_1 and E_2. The Nash equilibrium of the specific game is a pair of strategies $\{(m^*, u^*), (E_1^*, E_2^*)\}$ which also satisfy the following two conditions:

$$V^{\alpha}_{(m^*,u^*,E_1^*,E_2^*)} \geq V^{\alpha}_{(m^*,u^*,E_1,E_2)}\ \forall\, E_1, E_2$$

$$V^{d}_{(m^*,u^*,E_1^*,E_2^*)} \geq V^{d}_{(m,u,E_1^*,E_2^*)}\ \forall\, m, u$$

3.6 Game Theory application in Intrusion Detection of Access Control Systems [24, 25, 26]

Intruders in an information system can cause lot of damage in terms of confidentiality integrity and availability. Top secret documents on the hands of adversary can make the owners of the specific system to lose great amount of moneys and possible advantages they might have. This section describes an intrusion detection system (IDS) in access control based on game theory principles.

Access control systems are useful in order to enable authorised users to access only the allowed data and services using an identification technique. The system prevents any users to access data or services that are not entitled to do so. IDS can help to increase the security of a system by monitoring and analysing the traffic in the network. Current IDS are lacking a quantitative decision and control framework that can analyse and model attacks or threats and decide on the best response action. Such tools can be provided by using game theory.

3.6.1 The model infrastructure

The IDS is distributed in the network and has the virtual sensors S = $\{s_1, s_2, s_3, \dots, s_{max}\}$. Each sensor is an autonomous software agent able to monitor the system and collect information for detection purposes. Using different kinds of techniques, like pattern detection or signature comparison, the sensors report possible anomalies or intrusions that might occur in a subsystem of the network. The whole system which is monitored by the sensors is represented as a set of subsystems T = $\{t_1, t, t_3, \dots, t_{max}\}$. The set of possible threats or detectable anomalies which might indicate an intrusion is the set I = $\{i_1, i_2, i_3, \dots, i_{max}\}$. The set of attacks A = $\{a_1, a_2, a_3, \dots, a_{max}\}$ is a cross product of the sets I and T, A = T * I.

3.6.2 The Game

This is a non-cooperative two-player non-zero sum game between the attacker and the IDS. The sensor network is modelled as “fictitious player”. The role of the specific player is the distribution of a fixed probability given a specific attack. It also represents the output of the sensor network during an attack.

The game will be illustrated through the following simple example. The network of the specific game consists of a single sub-system and a single detectable threat (A = {a}).

The available actions of the IDS are two:

- Set an alert
- Do nothing

Thus, the strategy spaces of the IDS the attacker and the sensor network are:

- $U^{IDS} = \{u_1^{IDS}, u_2^{IDS}\}$
- $U^{Attacker} = \{u_1^{Attacker}, u_2^{Attacker}\}$, $u_1^{Attacker} = attack, u_2^{Attacker} = no\ attack$
- $U^{Sensor} = \{p1, p2\}$, given $u^{Attacker} \in U^{Attacker}$,
  $p = [p1, p2] \in \mathbb{R}^2, p \geq 0, p1 + p2 = 1$, where p1 and p2 give the likeliness of an attack and no attack respectively.

The payoff values of the attacker and the IDS are chosen randomly for illustrative purposes:

- $[(R_1^A, R_1^I), \dots, (R_8^A, R_8^I)]$

The following figure depicts a possible game of the above inputs in extensive form. According to the player’s actions a game is illustrated by following a path from left to right. The upper left branch in the figure indicates the event of no attack and the lower branch indicates the event of an attack. The nodes labelled chance, models sensor network where Sensor_NA indicates no attack detection and Sensor_A1 indicates detection of an attack. The nodes U decides to take a predefined action according to the information gathered by from the sensor network.

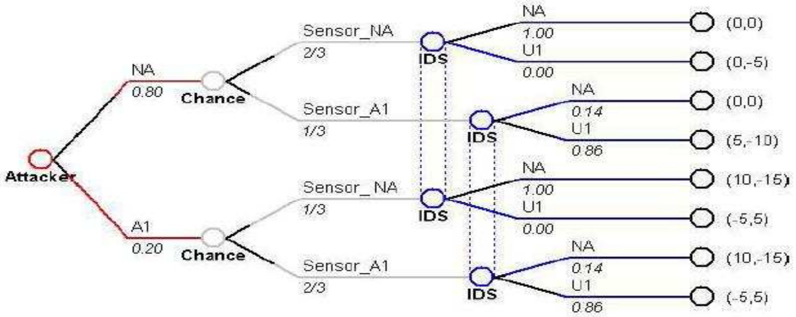


Figure 1000: A security Game shown in Extensive Form. [25]

3.6.3 Nash Equilibrium

The Nash equilibrium of the specific game is defined as a pair of strategies. The specific game does not have any Nash equilibrium solution in pure strategies thus the analysis of finding a solution should extend to mixed strategies. Recalling mixed strategy is a probability distribution over the space of all available pure strategies. On the figure above, the probability values are displayed under each branch. It should be noted that the sensor network- chance player has its own predefined fix probability distribution. The latter, is used to model the imperfect flow of information from the attacker to the IDS.

Analysing the Nash equilibrium of the specific game, the attacker does not want to attack the system with probability 0.80. This is because of the high probability of the sensor network to predict an intrusion with 2/3. The Nash equilibrium strategy of the IDS given this information is no response (NA) with probability 1 if there is no alarm and response (U1) with probability 0.86 if an alarm is set.

3.7 Fictitious Play [25, 27, 28]

Fictitious play is a learning rule strategy that a player might follow during a game. One player assumes that his opponent is playing a mixed strategy with some unknown stationary distribution. If this is the case, then the player's action will be chosen according to the historical frequency of actions of his opponents.

At the beginning of the game the defender makes some assumptions about his opponent's intentions in order to form a behaviour rules. The defender's beliefs about his opponents will be the guide rule which will help him to choose his actions. While the game is in progress, the defender is able to obtain more information about the strategy followed by the attacker. The acquire information of each course of play is analysed by the defender. Aim of this analysis is the construction of the attacking methodology of the adversary. During the game, the defender is refining his strategy if the information that have been analysed derived new indications about how the opponent is acting. It is possible after a number of courses to create the exact pattern of moves that the attacker is following.

For example imagine that two players are involved in the following game:

u_i = utility function of player i		Attacker		
		Attack 1	Attack 2	Attack 3
Defender	Defence 1	$u_1\ (d1), u_2\ (a1)$	$u_1\ (d1), u_2\ (a2)$	$u_1\ (d1), u_2\ (a3)$
	Defence 2	$u_1\ (d2), u_2\ (a1)$	$u_1\ (d2), u_2\ (a2)$	$u_1(d2), u_2\ (a3)$
	Defence 3	$u_1\ (d3), u_2\ (a1)$	$u_1\ (d3), u_2\ (a2)$	$u_1\ (d3), u_2\ (a3)$
	Defence 4	$u_1\ (d4), u_2\ (a1)$	$u_1\ (d4), u_2\ (a2)$	$u_1\ (d4), u_2\ (a3)$

Figure 35: The Pairs of Utility Functions for Each Possible Course of Play.

The defender has a set of four possible moves (pure strategies): $A_d = \{d1, d2, d3, d4\}$
The attacker has a set of 3 possible moves (pure strategies): $A_a = \{a1, a2, a3\}$

Applying a probability distribution function to the set of possible action of each player the following mixed strategies are created. The p_i value next to each possible action of the defender or the attacker indicates the probability that the specific action might occur.

Defender's pure strategy

$$A_d = \{d1 * p_1, d2 * p_2, d3 * p_3, d4 * p_4\}$$

m= total number of defender’s pure strategies, p_i = probability of action i

$$\sum_{i=1}^{m} p_i = 1$$

Attacker’s pure strategy:

$$A_a = \{a1 * \ p_1 \ , a2 * p_2 , a3 * p_3\}$$

The sum of the probabilities of all available actions of each player must be equal to 1:

$$\sum_{i=1}^{n} p_i = 1,$$

where n= total number of attacker’s pure strategies, p_i = probability of action i.

The payoffs for the pair of mixed strategies are: $(d_i * \ p_i , a_i * \ p_i)$

In this point, each of the players will calculate his expected payoff. As shown in a previous section, the expected payoff of one player, is the sum total of multiplying the selected pure strategy actual payoff with the probability that the action of his opponent might happen. An example is illustrated below. The last column of the table shows the probabilities that each of the defender’s action might occur. The last row of the table shows the probability that each of the attacker’s action might occur. The sum of all the probabilities of the defender’s or the attacker’s action are equal to one.

u_i = utility function of player i		Attacker			
		Attack 1	Attack 2	Attack 3	Defender Pr:
Defender	Defence 1	$u_1\ (d1), u_2\ (a1)$	$u_1\ (d1), u_2\ (a2)$	$u_1\ (d1), u_2\ (a3)$	p_1
	Defence 2	$u_1\ (d2), u_2\ (a1)$	$u_1\ (d2), u_2\ (a2)$	$u_1(d2), u_2\ (a3)$	p_2
	Defence 3	$u_1\ (d3), u_2\ (a1)$	$u_1\ (d3), u_2\ (a2)$	$u_1\ (d3), u_2\ (a3)$	p_3
	Defence 4	$u_1\ (d4), u_2\ (a1)$	$u_1\ (d4), u_2\ (a2)$	$u_1\ (d4), u_2\ (a3)$	p_4
Attacker Pr:		p_{11}	p_{22}	p_{33}	

Figure 36: Defender’s and Attacker’s Payoffs with Probabilities.

<u>Expected Payoff for Defender’s Action:</u> Defence 1

$$Expected_{payoff}(Defence\ 1) = \ u_1\ (d1) * \ p_{11} + \ u_1\ (d1) * \ p_{22} + \ u_1\ (d1) * \ p_{33}$$

<u>Expected Payoff for Attacker’s Action:</u> Attack 3

$$Expected_{payoff}(Attack\ 3) = u_2\ (a3) * \ p_1 + \ u_2\ (a3) * \ p_2 + \ u_2\ (a3) * \ p_3 + \ u_2\ (a3) * \ p_4$$

The mixed strategies of each player are defines as:

$$\Delta_{(m)} = mixed\ strategies\ of\ the\ defender$$
$$\Delta_{(n)} = mixed\ strategies\ of\ the\ attacker$$

In order to find the best response of each player, a function must select the action with the maximum expected payoff:

$$\text{MAX}\,\{\, U_i(\delta_i, \delta_{-i}\,)\,\},$$

where $\mathrm{U_i}$ = the utility function of action i,
$\delta_i \in \Delta_{(m)}, \Delta_{(n)}$,
-i = in game theory literature, this symbol is used to indicate those of other players, or the opponent's in this case (i.e. if in an example about the defender's actions the specific notation is included it indicates the attacker's actions)

If there is more than one action that yield the maximum expected payoff then the player will randomize his choice over the set of the actions with the maximum earnings:

In the end, a mixed strategy Nash Equilibrium is defined as a pair $(\delta_1^*, \delta_2^*) \in \Delta_{(m)} * \Delta_{(n)}$ such that for all $\delta_1 \in \Delta_{(m)}$ and $\delta_2 \in \Delta_{(n)}$:

$$U_i(\delta_i, \delta_{-i}^*\,) \ \leq \ U_i(\delta_i^*, \delta_{-i}^*)$$

Because of the fact that the game is repeated, it is obvious that the same process it will continue during the progress of the game. Imagine that the game is now repeated at times $\tau \in \{0, 1, 2, 3, ...\}$. The empirical frequency $f_i(\tau)$ of player P_i is given by:

$$f_i(\tau + 1) = \frac{1}{\tau + 1} \sum_{h=1}^{t} \delta_i(j)$$

By using the induction method, the following recursive relation is proved:

$$f_i(\tau + 1) = \frac{\tau}{\tau + 1} * f(\tau) + \frac{1}{\tau + 1}\,\delta_i(\tau)$$

Summing up, the following four steps will be followed in the specific Fictitious Strategy:

1. Calculate the payoff matrix of the game
2. Find the empirical frequency of the opponent according to the times played
3. Select the optimal pure strategy (best response)
4. In the case where more than one pure strategies yield the same maximum payoff, randomly choose one of these strategies

By using the pre-described fictitious strategy, it is possible for a player to play very well in any kind of the information incidents that his system might come against with. In the specific games, it is obvious that the player can play well with incomplete information about his opponents. The player must observe the game (all the actions of his opponent's up to present) and then he will be able to estimate the mixed strategy that is being used by his opponents. After the player is done with his estimation about the other player's strategy, he will continue by finding the optimal pure strategy that which will form his next move. After a new round of a game, the player playing the fictitious game, should update his previous estimation by analyzing once more his opponent's moves which might result to a new optimal strategy. It is obvious that if his opponent plays either a pure or mixed strategy, the fictitious play procedure will end up with the best response for the specific strategy. A game where all the participants are engaged to a fictitious play strategy it is feasible, that most of the times the players will be playing a Nash Equilibrium. Nevertheless, this is not always the case.

3.8 The Game of "FlipIt" [29]

FlipIt is a very interesting game which was introduced during the latest Crypto Conference on the 15th of August 2011 by Ronald L. Rivest. It is a very interesting game which concerns with the application of game theory principles to cryptography security. The specific game can be easily adjusted for the security needs of a more general security mechanism of an information system. The rest of this section describes some general characteristics of this methodology. Some adjustments have been made to the game in order to confront the question of this thesis.

Similarly with previous games, FlipIt is a two-player game which includes a defender and an attacker. In the specific game, the defender (the administrator of the system) is trying to keep his system in a secure state. On the other hand, the attacker tries to move the system from a secure state to an adversarial state. A few examples of possible secure and non-secure states of the system are defined in the following two paragraphs.

Here the system is viewed as a combination of many other subsystems. Each state corresponds to at least one subsystem. A secure state might me defined as one of the following different situations:

- All services provided by the system run smoothly and as they are intended to do so.
- Any secure data of the system are kept secure.
- Any secure data of the system are disclosed only to legitimate users.
- Access of the system is allowed only to legitimate users.
- System is under the control of the system's administrator

A non secure state might me defined as one of the following different situations:

- The services of the specific system are not available to the users (DoS attack).
- Secure data of the system are stolen (or guessed).
- Secure data of the system are disclosed to not legitimate users.
- Illegal users managed to access the system.
- System is under the control of the adversary.

The players of the specific game are able to make their move any time and it is possible to make move at the same time. This characteristic transforms this situation to a dynamic simultaneous move game. A defender's move aims to put the system into a good state (i.e. initialize, reset, recover, dis-infect). The attacker's move aims to put the system into a bad state (i.e. compromise, corrupt, steal, infect). The moves of the players might not always succeed thus they will not make any change to the current state of the system.

Some examples of the players' moves-responses are the following:

- Attacker: Steal critical sign-in data.
  Defender: Deactivate specific data and create new ones.

- Attacker: Install a background script which creates a back door for illegitimate users.
  Defender: Restore system to initial settings/ Re-install system software.

- Attacker: Disclose critical documents to public.
  Defender: Recover the specific documents and secure them.

As it has been shown from the examples above, the specific game might never have an end. This game should be considered as an infinite game. It is a continual game where at one point of the time the defender controls the system and at another point of the time the attacker will manage to gain control; then the defender might be able to regain the control of his system in a later point in the time line.

In the specific game, one player cannot be sure or is not possible for him to immediately know when his opponent has made his move. While the time passes by from a player's last move, the specific player's uncertainty related with the current state of the system increases. For example, player A might made a move in time t_1 and have on mind that the current state of the system is s_1 but player's B undetectable move in time t_2 transformed the system to state s_2. Having on mind the pre-described scenario, the participants of the specific game should never take a given state of the system as real and always assume for a probability of mistaken state.

The available moves of each player are not guaranteed that they will succeed. For all the moves of all the participants of the game it is possible to fail. A succeed move on the specific game is called "flip" because of the fact that the control of the system flip from one player to another (i.e. the control of the system flip from the defender to the attacker after the attacker made a succeed move). A player's move which has no effect (no change on the system state) is called "flop". Flops are the major reason that causes the uncertainty to the players of the game.

The exact state of the system it is known to the player the time he takes a move. The players have fully recovery which means that the history of the game becomes available to them before they move. Each move has a cost assign to it. The cost is not general and depends to the type of the move. An action that is designed to steal some passwords will cause less than an action that is designed to take the control of the whole system. Player i pays $k_i(action\ x)$ for the move labelled as action x. When a player has the control it means that has some gain. In other words, if the system is on a secure state it means that the defender of the system has the control and that is the player which currently earns positive gains. On the other hand, if the state is in a non-secure state (adversarial situation) then the adversary is the one who gains positive payoff and the defender is the one who is experiencing some kind of losses (depending on the kind of the attack the system was hit). The player who has the control of the system earns one point for each second he is in the specific situation.

In order to compute how well a players has played the following calculations take place:
The total moves of player i up to time t is determined by: $N_i(t)$
The average rate of play for player i is determined by: $\alpha_i(t) = \frac{N_i(t)}{t}$

The number of second that player i is in control up to time t is determined by: $G_i(t)$
The rate of gain up to time t for player i is determined by: $\gamma_i(t) = \frac{G_i(t)}{t}$
The score of player i up to time t is determined by: Time_In_Control – Cost_Of_Moves = $B_i(t)$ = $G_i(t)$ - $k_i * N_i(t)$
The benefit rate for player i is: $\beta_i(t)$ = $\frac{B_i(t)}{t}$ = $\gamma_i(t)$ - $k_i * \alpha_i(t)$
The goal of each player is to maximize the β_i = $\lim_{t\to\infty}\beta_i(t)$

An example of a game is shown in the figure below:

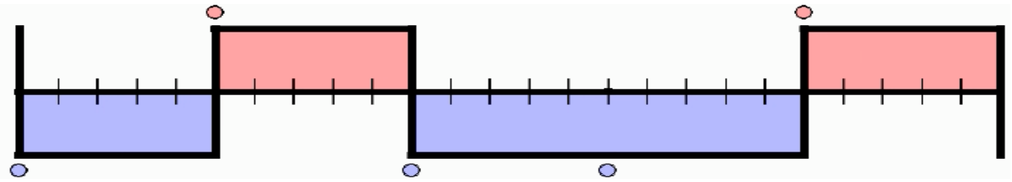


Figure 37: Moves of an Attacker and a Defender in a Random Period of Time [29].

The blue colour is for the defender and the red colour is for the attacker. The blue dots indicate the start of defender's move and the red dots indicate the start of the attacker's move. The rectangles which are fill of the colour of each player shows the period of time where each of the players has the control of the system. The time line of the specific game is divided in seconds.

From the above figure the following information is extracted:
The defender made three moves.
The moves of the defender yielded him 15 seconds of control.
The score of the defender is: Control ($G_i(t)$) – Cost (k_i)$*$ Moves ($N_i(t)$)
Control (15) – Cost (1) $*$ Moves (3) = 12
The attacker made two moves.
The moves of the attacker yielded him 10 seconds of control.
The score of the attacker is: Control ($G_i(t)$) – Cost (k_i)$*$ Moves ($N_i(t)$)
Control (10) – Cost (2) $*$ Moves (2) = 6

As stated above, each player's main objective is to maximize his total payoff (score). The player should decide a strategy that will help him to gain as much possible gains as possible. There are two possible types of strategies concerning this type of game:

1. Non – adaptive play
2. Adaptive play

3.8.1 Non - Adaptive Play

In a non-adaptive play, each player chooses his actions without concerning about his opponent's moves. It is said that the player who plays a non-adaptive strategy plays on blindly because of the fact that he does not care what his opponent might choose. A non-adaptive player is able to pre-compute his entire list of moves even before the game starts. This is very similar to the fictitious type of games of game theory.

The most important non-adaptive strategies are the following:

- Periodic Play
- Exponential (memory-less) play and
- Renewal strategies: iid intermove times

3.8.2 Periodic Play

If player i chose to play a periodic strategy, he must choose a rate which indicates the periods of time that player i will proceeds to a move. The rate of each player is determined by α_i and the period of time is $\frac{1}{\alpha_1}$. In other words, if player 1 decides to play with rate $\alpha_1 = 3$ and period = $\frac{1}{\alpha_1} = \frac{1}{3}$ this means that player 1 will proceed to a new move for each 3 values of time. The following figure indicates the moves of player 1 in a random period of time playing a periodic strategy.

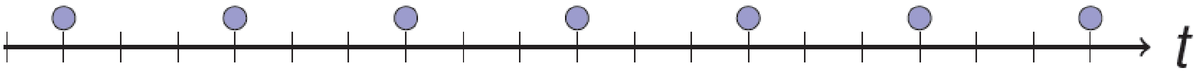


Figure 38: Moves of player i playing a periodic strategy with rate $\alpha_1 = 3$. [29]

The disadvantage of periodic strategy is the fact that an adaptive attacker can easily find out the period rate and win the game unless it is very fast.

The following graphs illustrate a game of a periodic attacker and defender. The final analysis of the graph will result to the Nash Equilibrium of the specific game. In the specific game it is assumed that the attacker moves periodically at rate $\alpha_1$and period $\frac{1}{\alpha_1}$ with unknown phase. The cost of each move for the defender is $k_1 = 1$and the cost for each move of the attacker is $k_2 = 1.5$. The optimum non-adaptive strategy for the defender should be the following:

- If α_1 > ½ k_0, do not play (Each move will yield only losses),
- If α_1 = ½ k_0, play periodically at any rate If α_0, 0≤ α_0 ≤ If α_1 > ½ k_0
- If α_1 < ½ k_0, play periodically at rate α_1 = $\sqrt{\frac{\alpha_1}{2k_1}} > \alpha_1$

If the defender applies the following rules to his game he will be able to reach the Nash equilibrium of the specific game.

The following graphs show the possible rates that each player might choose to move and play his periodic game. The x axis shows the defender's rate and the y axis shows the attacker's rate.

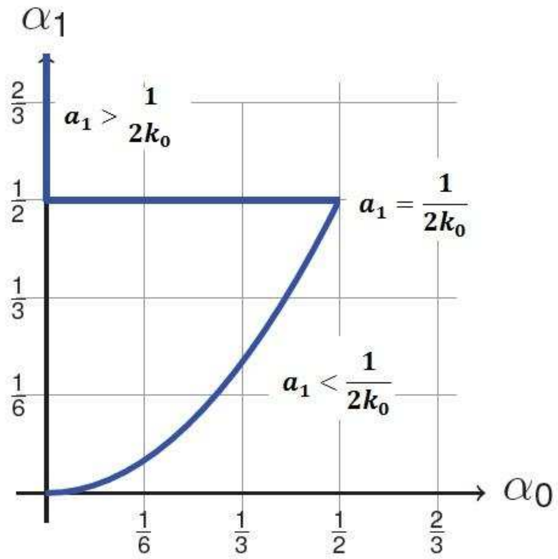


Figure 39: The Defender's Moves (Periodic Play). [29]

The figure above depicts the defender's moves. If the attacker chooses to play with rate $^1/_2$ to $^2/_3$, it means that the attacker is too fast for the defender (α_1 > ½ k_1) and he will not make any move because of the fact that he will not earn any benefits. If the attacker chooses to play with rate $^1/_2$, it means that the defender is able to play but with zero benefit (α_1 = ½ k_1). If the attacker chooses to play with rate $< {}^1/_2$, it means that the defender is able to play and maximize his benefit with playing his moves with rate $\alpha_0 = \sqrt{\frac{\alpha_1}{2k_0}}$.

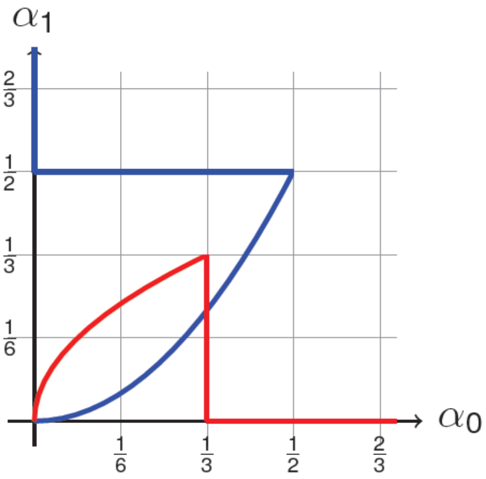


Figure 40: The Attacker's Moves (Periodic Play). [29]

In the same way, the attacker's moves were analysed. The optimal strategy for the attacker was computed in the figure above. If the defender chooses to play with rate 1/3 to 2/3, it means that the defender is too fast for the attacker (α_0 > ½ k_1) and he will not make any move because of the fact that he will not earn any benefits. If the defender chooses to play with rate 1/3, it means that the attacker is able to play but with zero benefit (α_0 = ½ k_1). If the defender chooses to play with rate < 1/3, it means that the attacker is able to play and maximize his benefit with playing his moves with rate $\alpha_1 = \sqrt{\frac{\alpha_0}{2k_1}}$.

After analysing what would be the best move according to the opponent's rate for each of the two players in a periodic game, the Nash Equilibrium of the game is displayed below:

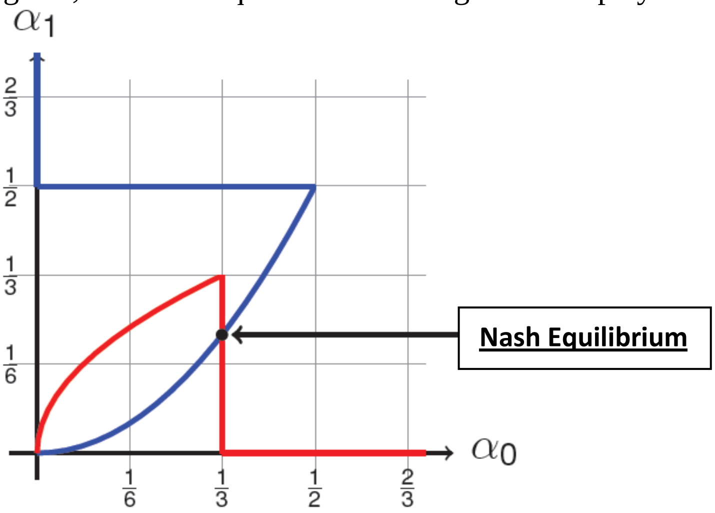


Figure 41: The Nash Equilibrium of the Periodic Game. [29]

The Nash Equilibrium of the specific game is on the set of rates (α_0, α_1) and particularly (1/3, 2/9).

$(\gamma_0, \gamma_1) = (\frac{2}{3}, \frac{1}{3})$

$(\beta_0, \beta_1) = (\frac{1}{3}, 0)$

3.8.3 Exponential Attacker

The second non-adaptive strategy is the exponential type of play. When a player plays exponential with rate α_1, in each interval of time dt he plays independently with probability α_1* dt. The next figure shows a possible sequence of moves of a player with $\alpha_1 = 0.5$.

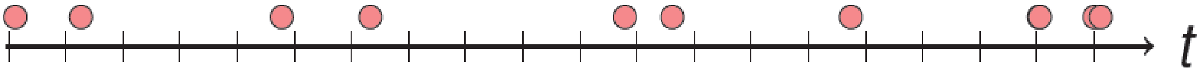


Figure 42: The Possible Moves of an Exponential Player with Rate $\alpha_1 = 0.5$. [29]

The following graphs will indicate the optimal moves of the attacker and the defender in an exponential game. The cost for the defender moves is 1 and the cost for the attacker moves is 1.5.

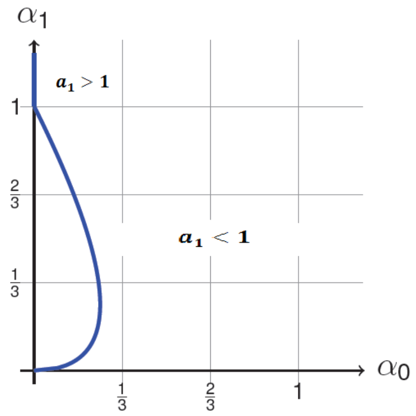


Figure 43: The Defender's Moves (Exponential). [29]

If the attacker's rate is greater than 1, it means that the defender is not able to make any move because it will have only losses. If the attacker's rate is less than 1, then the defender's optimal play is $\alpha_0 = \sqrt{\frac{\alpha_1}{k_0}} - \alpha_1$.

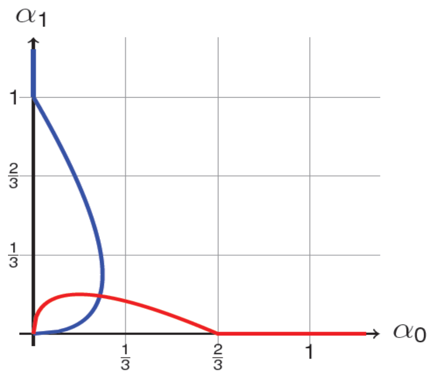


Figure 44: The Attacker's Moves (Exponential). [29]

From the attacker's point of view, if the defender's chosen rate is greater than 2/3 the defender is too fast for the attacker but when the attacker's rate is less than 2/3, the attacker's optimal play is $\alpha_1 = \sqrt{\frac{\alpha_0}{k_1}} - \alpha_0$.

After finish analyzing the strategies of the defender and the attacker, the Nash Equilibrium is shown in the figure below:

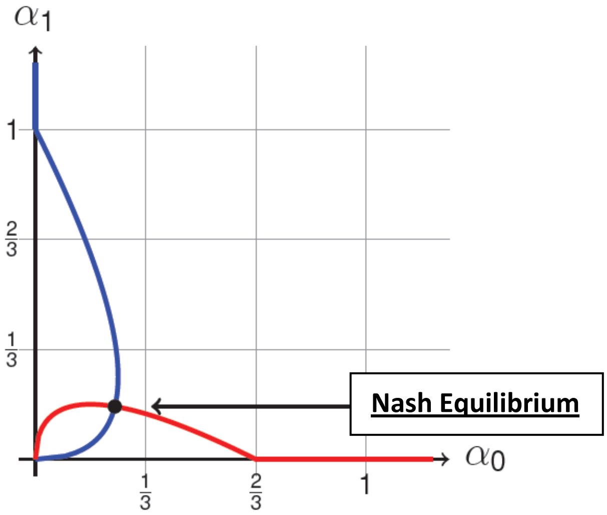


Figure 45: The Nash Equilibrium of the Exponential Game. [29]

The Nash Equilibrium of the specific game is on the set of rates (α_0, α_1) and particularly (6/25, 4/25).

$(\gamma_0, \gamma_1) = (\frac{3}{5}, \frac{2}{5})$

$(\beta_0, \beta_1) = (\frac{9}{25}, \frac{6}{25})$

3.8.4 Renewal Strategies

The third class of non-adaptive strategies concerns with the renewal strategies. The characteristic of this strategy is the iid inter-move delays for player *i's* move.

Pr (delay $\leq$ x) = F_i (x) , for some distribution F_i.

3.8.5 Adaptive Strategies

A player would never prefer to play a periodic strategy against an adaptive player. The adaptive player is able to figure out the rate of moves of the periodic player and respond to him with a new move right after his opponent's move completed.

On the other hand, an exponential strategy is a good defence against a player that chooses an adaptive strategy. If a defender plays exponentially, the attacker has only two options. The first one is to try to play periodically and the second one is to not play at all.

The next figure illustrates the defenders benefit β_0 against the attacker. The blue line describes the benefit of periodic defender against a periodic attacker. The green line, described the benefits of an exponential defender against an adaptive attacker.

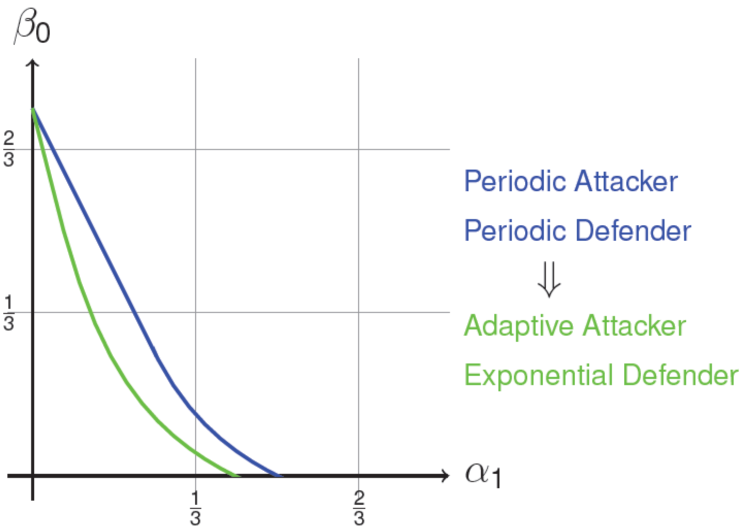


Figure 46: Defender's net benefit $\boldsymbol{\beta_0}$ against optimal (periodic - adaptive) Attacker ($\boldsymbol{a_0 = 0.25}$). [29]

From FlipIt game, a few very important rules have derived that if they followed by the players will be able to play the best strategy for their self which will maximize their payoffs and minimize their losses.

- A player must always have on mind the he might loss the control repeatedly and his actions might not be able to re-gain the control of the system for a long period of time.
- A good player, except from trying to find out the possible action for him, he should also be fast with his responses in order to make his opponent to give up.
- The player should always try not only to maximize his payoff but to maximize the cost of his opponents as well.

4. A Game Theoretic System of Flipping States [21, 29, 30, 31]

The previous chapter presented a review of some papers which applied game theory in information security. This part combines the previous sections and proposes a new model which seems more capable and powerful against different kind of cyber incidents.

The main idea behind the specific model is the methodology followed by the Flip-It game. Generally, all the systems which are connected on the internet are under the control of their authorised system administrator until an attack is launched against them. In the case where the attack is successful, the control of the system flips from the system administrator's hands to the attacker's hands.

The following game has two participants, the defender of the system and the attacker of the system. The specific stochastic game can be described by the tuple:

$$(S, s_i, I^1, I^2, E^1, E^2, A^1, A_i^1, A^2, A_i^2, \mathrm{U}_1, \mathrm{U}_2, \mathrm{T}).$$

S: Is the set of the possible states.
I^1: The information that player 1 has related to the game.
I^2: The information that player 2 has related to the game.
s_i: Is the state of the system that is calculated by player i according to his information.
E^1: The error probability of player's 1 sensor about the state s_i over his information I^1.
E^2: The error probability of player's 2 sensor about the state s_i over his information I^2.
A^1: Is the set of all available actions for the defender.
A_i^1: The actions available to player 1 at state s_i.
A^2: Is the set of the available actions for the attacker.
A_i^2: The actions available to player 2 at state S_i.
U_1: Is the function that calculates the reward of defender's action (i.e. $\mathrm{k}_1(\text{action x} = 2)$).
U_2: Is the function that calculates the reward of attacker's action (i.e. $\mathrm{k}_2(\text{action y} = 1)$).
T: is the state transition function. After the completion of each action, the state of the system might transform or if the action did not have any effects the state will remain the same as previous. The equation to calculate the new state is: T = $(\mathrm{S} * \mathrm{A}_1) * (\mathrm{S} * \mathrm{A}_2)$.

The game has the following structure: At a particular time t, the system is in state $s_i \in S$. The defender chooses an action a_i^1 from A_i^1 and the attacker chooses an action a_i^2 from A_i^2. Subsequently, the defender will receive a payoff r_i^1 = $\mathrm{U}_1(s_i, a_i^1, a_i^2)$ and the attacker will receive a payoff r_i^2 = $\mathrm{U}_2(s_i, a_i^1, a_i^2)$. Finally, the game will move to a new state s_{i+1}.

One very important factor of game theory models of information warfare is the set of states. The larger the state set is, the most accurate and complete the analysis of the specific problem could be. A game which has many different states it means that each minor possible change that might occur in the system will yield a new state. On the other hand, the game becomes more complex and difficult.

The error probability indicates how certain a player is that the game is actually at a specific state. The smaller the probability is the more confident the specific player is about the game state. Each state has several defined characteristics. The error probability is proportional to the characteristics of a state that are not detected from the system's sensors. If the sensors have met all the defined characteristics of a specific state it means that the error probability is zero.

The next figure depicts a fictitious two-player game of a strategic situation. Each player has six available actions. The matrix shows the utility functions of each possible course of play in detail.

		Attacker					
		$\boldsymbol{a_2^1}$	$\boldsymbol{a_2^2}$	$\boldsymbol{a_2^3}$	$\boldsymbol{a_2^4}$	$\boldsymbol{a_2^5}$	$\boldsymbol{a_2^6}$
Defender	$\boldsymbol{a_1^1}$	$\mathrm{U}_1(a_1^1), \mathrm{U}_2(a_2^1)$	$\mathrm{U}_1(a_1^1), \mathrm{U}_2(a_2^2)$	$\mathrm{U}_1(a_1^1), \mathrm{U}_2(a_2^3)$	$\mathrm{U}_1(a_1^1), \mathrm{U}_2(a_2^4)$	$\mathrm{U}_1(a_1^1), \mathrm{U}_2(a_2^5)$	$\mathrm{U}_1(a_1^1), \mathrm{U}_2(a_2^6)$
	$\boldsymbol{a_1^2}$	$\mathrm{U}_1(a_1^2), \mathrm{U}_2(a_2^1)$	$\mathrm{U}_1(a_1^2), \mathrm{U}_2(a_2^2)$	$\mathrm{U}_1(a_1^2), \mathrm{U}_2(a_2^3)$	$\mathrm{U}_1(a_1^2), \mathrm{U}_2(a_2^4)$	$\mathrm{U}_1(a_1^2), \mathrm{U}_2(a_2^5)$	$\mathrm{U}_1(a_1^2), \mathrm{U}_2(a_2^6)$
	$\boldsymbol{a_1^3}$	$\mathrm{U}_1(a_1^3), \mathrm{U}_2(a_2^1)$	$\mathrm{U}_1(a_1^3), \mathrm{U}_2(a_2^2)$	$\mathrm{U}_1(a_1^3), \mathrm{U}_2(a_2^3)$	$\mathrm{U}_1(a_1^3), \mathrm{U}_2(a_2^4)$	$\mathrm{U}_1(a_1^3), \mathrm{U}_2(a_2^5)$	$\mathrm{U}_1(a_1^3), \mathrm{U}_2(a_2^6)$
	$\boldsymbol{a_1^4}$	$\mathrm{U}_1(a_1^4), \mathrm{U}_2(a_2^1)$	$\mathrm{U}_1(a_1^4), \mathrm{U}_2(a_2^2)$	$\mathrm{U}_1(a_1^4), \mathrm{U}_2(a_2^3)$	$\mathrm{U}_1(a_1^4), \mathrm{U}_2(a_2^4)$	$\mathrm{U}_1(a_1^4), \mathrm{U}_2(a_2^5)$	$\mathrm{U}_1(a_1^4), \mathrm{U}_2(a_2^6)$
	$\boldsymbol{a_1^5}$	$\mathrm{U}_1(a_1^5), \mathrm{U}_2(a_2^1)$	$\mathrm{U}_1(a_1^5), \mathrm{U}_2(a_2^2)$	$\mathrm{U}_1(a_1^5), \mathrm{U}_2(a_2^3)$	$\mathrm{U}_1(a_1^5), \mathrm{U}_2(a_2^4)$	$\mathrm{U}_1(a_1^5), \mathrm{U}_2(a_2^5)$	$\mathrm{U}_1(a_1^5), \mathrm{U}_2(a_2^6)$
	$\boldsymbol{a_1^6}$	$\mathrm{U}_1(a_1^6), \mathrm{U}_2(a_2^1)$	$\mathrm{U}_1(a_1^6), \mathrm{U}_2(a_2^2)$	$\mathrm{U}_1(a_1^6), \mathrm{U}_2(a_2^3)$	$\mathrm{U}_1(a_1^6), \mathrm{U}_2(a_2^4)$	$\mathrm{U}_1(a_1^6), \mathrm{U}_2(a_2^5)$	$\mathrm{U}_1(a_1^6), \mathrm{U}_2(a_2^6)$

Figure 46: The Payoff Matrix of the Defender and the Attacker

Each player of the game must compute his opponent mixed strategy. The mixed strategy will assign a probability value to each available action of his opponent. The defender will assign a probability to each action of the attacker and the attacker will assign a probability to each action of the defender. The following figure shows the defender's and attacker's assign probabilities over their available actions. The probabilities shown on the figure were chosen in random for illustration purposes. As described in previous sections, some kind of signs might help the players in the probability distribution process by extracting some extra information about their opponent's preferences. During the game, is possible for a player to refine his beliefs and assign new values to his opponent's actions according to the observations he made.

Attacker Actions	Action Probability	Defender Action	Action Probability
a_1^1	0	a_2^1	3/8
a_1^2	2/8	a_2^2	1/8
a_1^3	1/8	a_2^3	0
a_1^4	2/8	a_2^4	1/8
a_1^5	3/8	a_2^5	1/8
a_1^6	0	a_2^6	2/8

Figure 47: Probabilities Distribution over the Player's Actions

The actions with probability zero indicate the belief of the player that his opponent will not choose the specific action at any time during the game. Subsequently, with the use of the reward functions, each player will compute his expected payoff. The expected payoff is calculated using the following equation:

k_1 (Defender_action) * Pr (Defender_action) + k_2 (Attacker_action) * Pr (Attacker _action)

Each player has his own sensor which outputs a prediction about the system state according to the input information that the player gives to the sensor. The output of the sensor is $s_i \in S$ and has an error probability E. Each sensor system has his error probability which can be decreased with different kinds of techniques which can train the sensor to have more reliable and accurate outputs. The sensors part is not within the scope of the system thus for simplicity it will assumed that none of the sensors are perfect.

4.1 Types of Attacks

There are two kinds of attacks available to the adversary. The first category consists of the attacks where the adversary must find and exploit potential vulnerabilities of the system. In the unlikely situation where an information system lacks of any vulnerability, the specific attacks are not feasible to occur. The second category includes the attacks where the adversary is running external legal or illegal processes in order to achieve his goal. These two general categories have the following most important types of attacks:

Attacks launched without the need of system vulnerabilities:

- Denial of Service (DoS) Attacks
- Distributed Denial of Service (DDoS) Attacks

Attacks launched exploiting system vulnerabilities (Intruders)

- Web-site Defacement
- Stealing of important-private data
- Disclosure of important-private data

4.1.1 Analysis of the attacks

The first category has two major attacks, the DoS and the DDoS attack. The only difference of the specific two categories is the fact that the first one has only one node (system) that launch the attack but on a DDoS attack there are n number of nodes that launch the attack. For both scenarios, it is assumed that the leader behind each attack is only one person. In a DDoS attack it is assumed that there is one master computer which controls all the other nodes (zombies) that are included in the attack.

The attacker needs to find a way to intrude into the system in the attacks included in the second category. The actions of this category need the adversary to control the system or sub-systems in order to be accomplished. Once the intruder gain the control of the system, the state flips from a good state to a bad state but it does not guarantee that the final objective of the attack will succeed because of the fact that the defender might gain control much earlier. Generally, none of the actions of each player are guaranteed to succeed.

4.1.2 Two-player Game

These attacks are modelled as repeated two-player non-zero games. The participants of the game are the defender (system administrator) and the attacker. The game-board of the game is the system network. The players are represented as shown below:

- Defender = Blue = Player 1
- Attacker = Red = Player 2

The specific games are characterised as infinite games which means games without an end state. Although the attack might fail or the defender might manage to regain the control of his system, such kinds of games in the cyber world are not likely to terminate. The defender of the system is always the same and his objective is to protect the functionality of the system at all times. On the other hand, the attacker has the tendency to change. For example, critical systems are facing frequent DoS/DDoS attacks by different adversarial teams. Once the A team failed to launch a successful attack, a new different adversarial team will show up and launch a new attack on the specific system. This is the nature of critical information systems that are involved in the cyberwarfare field.

In the first category, the system administrator aims to preserve the normal and smooth functionality of his system. His main objectives are to maintain a reliable and standard providence of his system services and any other kind of electronic data that authorised users are entitled to have access. In contrast, the adversary aims to corrupt the system's services providence to their legitimate users or at least to decrease the number of users that will manage to have access to the system's services. They also might try to increase in a large scale the time needed for the system to provide the specific services or to make any other type of data unavailable to the authorised users.

In the second category, the defender aims to prevent any intrusions to his system. Monitoring and analysis of the system's network extract information about possible intrusions and sound the alarm when a network traffic anomaly is detected. Access control mechanisms are responsible for the type of data and services that each user is entitled to have access to. In the specific category of attacks the defender does not only cope with external adversarial nodes that are trying to access the system but he has to counteract another adversarial category, the insiders.

The critical resources that need a protection shield in information warfare games in general are:

- System's services
- System's data

When the system is under the defender's control is said to be in a good state. If the system is in a bad state it means that the control has been gained by the attacker. If the action of a player was successful then it is said that the game flip control indicating the change of a state and the gaining of the control by the opponent. In the case where an action was not completed successfully then the game flops indicating that the state did not change and the control remains to the player that already had it before the last move. Some of the most important good and bad possible states that the system might be are displayed below:

Good States:

1. System's services provided smoothly and as intended to do to authorised and legitimate users only.
2. Data can be accessed by legitimate and authorised users only.
3. Data are displayed as they intended to do so by the system's administrator.
4. System under the control of the defender

Bad States:

1. System's services are not available to the legitimate users.
2. System's services are available to not authorised users.
3. System's services are available but with many problems (i.e. a small number of people can use the services or the services need a long period of time to complete).
4. System's data are not available to the users who are entitled to access the specific data.
5. Data can be access from unauthorised users
6. Data are not displayed as intended to do so by the system's administrator.

7. System under the control of the attacker

The system's network is the battle field of the defender and the attacker. Any of the two players can choose an action at any time. The actions are not guaranteed that they will be successful. A successful action is the one that will flip a good state to a bad state and vice versa. The aim of the defender's actions is to put the resource into a good state and the basic target of the attacker's actions is to put the resource into a bad state.

The defender's security mechanism is the firewall and the sensors of the system. The adversary's attack mechanism constitute by the nodes that exploit and has under his control and the sensors of his system.

The challenge of the system's administrator for the first category of attacks is to distinguish a legitimate flow of packets from illegitimate ones. The legitimate flows are most likely to have their origin from an authorised user and should be allowed to reach their destination which is the system server. Illegitimate flows of packets have their origin from adversarial nodes and should be blocked by the firewall and not allowed to reach the system's server or redirect to another system which will try to extract information about the attacker. The attacker must choose the number of the nodes that will exploit to launch his attack and the frequency and sending rate of the specific nodes.

For the attacks of the second category, the defender must find any kind of intrusions that his system might suffer from and block them. He should also strictly maintain the permissions of each legitimate user. The attacker on the other hand, must find his way to intrude in the targeted system and gain control of the specific mechanisms of the systems that will allow him to accomplish his goal.

Some available actions of the players are shown below:

Defender:

- Check system state
- Choose the error probability of his sensors (in what degree should this value influence the decision mechanism)
- Choose the drop rate of the firewall
- Choose the bandwidth available to each user
- Re-install software

Attacker

- Check system state
- Choose the error probability of his sensors (in what degree should this value influence the decision mechanism)
- Choose the number of nodes that will launch the attack
- Choose the sending request frequency for each node
- Choose the sending rate for each node
- Install malicious software
- Steal data
- Disclose data

4.2 Strategy

This section shows the strategy of the defender player. The following steps are executed each time the defender wants to make a move. The steps of the proposed strategy are shown below:

1. Information Gathering

The system administrator must gather any available information related with his system functionality and the adversary that launched the attack. This information is the input of the system's programs which are responsible to estimate the system's state and the type of the attacker that the system's administrator is facing. In nowadays, system's sensors related with security have an unwanted ratio of false positive and false negative alarms which play a major role to the functionality of the proposed system.

One example of the specific task could be the observation of the network traffic. The system might analyse the frequency and the number of requests that received during regularly periods of time. Additionally it might try to classify the nodes according to their sending rate. On the one hand there will be the nodes with low sending rate and on the other hand the nodes with higher sending rate.

2. Estimate the system state

The defender must then consult his system's classifier to verify the current state of his system. This is a vital step due to the fact that an accurate description of the system state can eliminate the player's actions associated to the given state to the minimum. Thus, the complexity for calculating the Nash equilibrium of the game will decrease rapidly.

One example of this task could be the following: The system examines the data gathered from the previous task and tries to classify the system in a state. Continuing from the previous scenario, high sending rates of a portion of some nodes might indicate that the system is under a DoS/DDoS attack and appropriate actions should be taken immediately. The classification of the system in an adversarial situation is an attempt to eliminate the available defence actions of the system administrator to the actions that are proper only to the specific situation.

3. Estimate the attacker's type

Afterwards, the defender inputs the possible state of the system that was calculated from the previous step to a new classifier which is responsible to categorise the attacker into a group. Researchers have shown that modelling of the attackers is possible and can also reveal much information about them related to their attacks, objectives, intents etc [44]. This procedure might give a better idea to the security specialist of the system on how to distribute his different available security mechanisms through his system.

In the example scenario the previous tasks find out that the system might be threaten by a DoS/DDoS attack. A prediction of the type of the attacker is possible to indicate to the defender which part of the system the attacker is aiming to transform to not functional. This task is aiming to make the defender to focus on a particular part of the system that is primary targeted by the attacker and defence it as much as possible.

4. Fictitious Play

The defender should now have his available options and possible actions available to his opponent. A fictitious play as described in section 3.7 will give the best response to the attacker’s actions. The defender will be able to choose the action that will maximize his payoffs by defending his system with the best possible way.

The defender should now have all the available and most appropriate actions for the specific attack on his hands. A fictitious methodology will predict which of the available options will yield the maximum payoff (or the minimum loss) for the defender.

5. Re-estimate of the system state

The final step is to verify whether the response was successful or not by checking the system state. The system administrator’s desire is the flip of the system’s control to his hands by moving the system to a good state. If the system remained to a bad state the defender should start again from the first step by gathering new information and try to model a new game with new options. It is possible that the system will return to the defender the same options as before but the steps should start from the beginning because if the attacker made another move the information and the state of the system is possible to transform again.

6. Check how did you play

In the case where the defender managed to regain the control of his system he must not complacent. He must analyse the way he played, his payoffs and his losses in order to find out how he can improve his game. Most important for him is the total time that his system was under the control of the attacker. He must analyse his actions taken during the specific period and figure out what was the problem that gave the attacker the control of the game. Another important factor is the time needed for him to make his move. He should always try to respond to any potential adversarial actions as soon as possible.

4.3 Nash Equilibrium

Assuming that both players are rational, their main goal is to maximize their payoff and decrease their losses. Regardless of the fact that a move of a player might not transform the system state, each player incurs some cost for each move he makes. The final payoff of a player is the payoff he receives by subtracting the cost of the move.

The Nash Equilibrium of the game is defined as a pair of strategies:

$$(a_1^*, a_2^*)$$

The specific pair should also satisfy the following two statements:

$$U^1(a_1^*, a_2^*) \geq U^1(a_1, a_2^*) \,\forall\, a_1 \in A^1$$

$$U^2(a_1^*, a_2^*) \geq U^1(a_1^*, a_2) \,\forall\, a_2 \in A^2$$

4.4 Game Illustration with Figures

This section depicts a system which transforms from a good state to a bad state and vice versa according to the actions taken by the players of the game. Each figure has only one axis and it represents the time line. The blue colour represents the defender and the red colour represents the attacker. The rectangles which are above the x axis indicate that the system is in good state which means is under the control of the system administrator. The rectangles which are below the x axis indicate that the system is in a bad state which means that it is under the control of the attacker. The small circles indicate that a player made a move. If a player makes a move and then the rectangle appears on his side, it means that the action was completed successfully and the control of the system flipped to his hands.

The first picture displays a system in a normal/good state under the control of its system administrator.

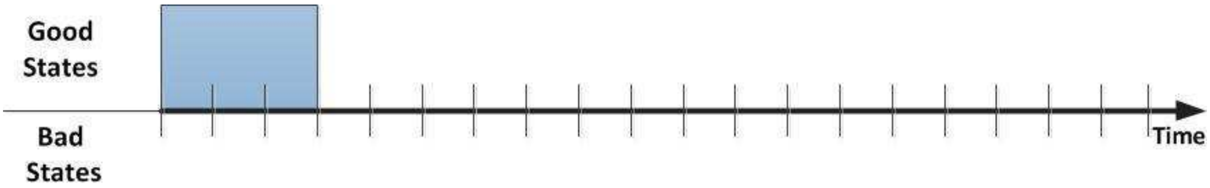


Figure 48: State 1 – Good State – The System's Administrator has the Control.

The next figure shows that the attacker has made a move and manages to gain the control of the system from the system administrator.

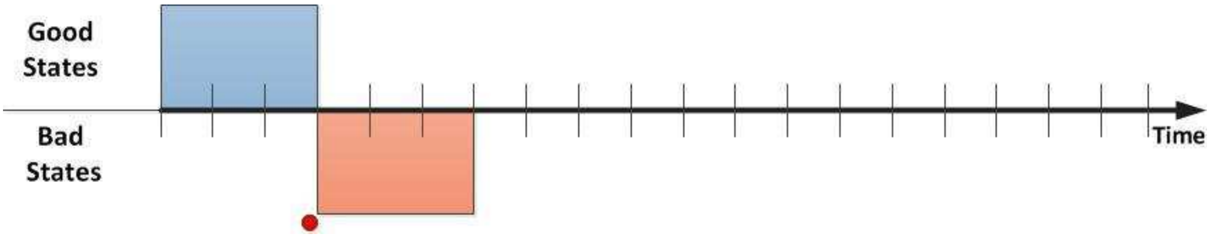


Figure 49: The control flip from the defender to the attacker after the successful move of the attacker.

The next figure shows the move of the defender who is trying to regain the control of his system but his action did not succeed. This is a flop situation and the control of the system does not change hands. The attacker is the one that continues to have the system's control.

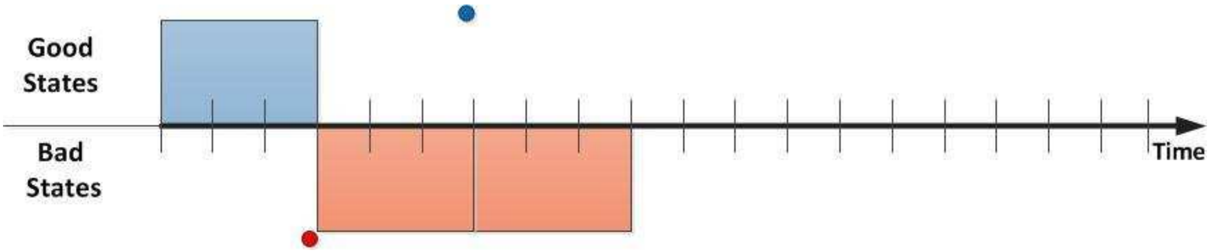


Figure 50: An unsuccessful move of the defender leaves the system's control to the attacker.

The next figure displays another move of the defender. This time it seems that the defender have chosen a better action, more suitable to the specific situation and achieved to get successful results. The control flips from the defender's hands to the attacker's hands.

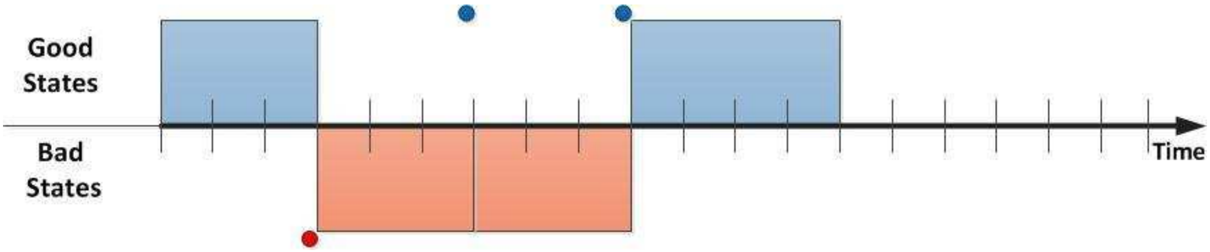


Figure 51: A second continues move of the defender results to the flip of the system's control.

The last figure shows one last move that is made by the attacker and regains him the control of the system.

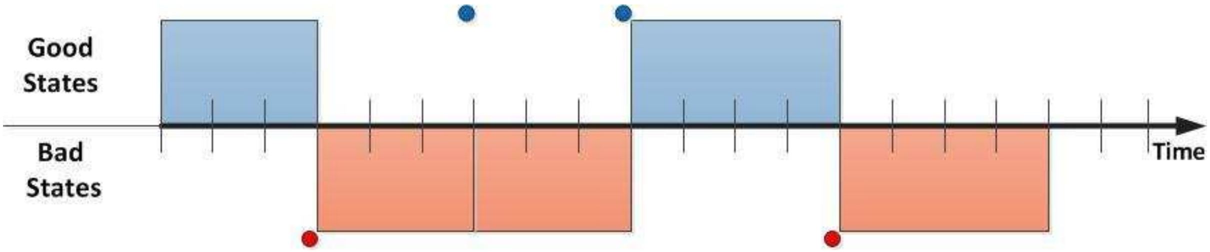


Figure 52: The attacker moves again and regain the control of the system.

From the figures above the following information is extracted:

The defender made two moves.
The moves of the defender yielded him 4 seconds of control.
The score of the defender is: Control ($G_i(t)$) – Cost (k_i)$*$ Moves ($N_i(t)$)
Control (4) – Cost (1) $*$ Moves (2) = 2
The attacker made two moves.
The moves of the attacker yielded him 10 seconds of control.
The score of the attacker is: Control ($G_i(t)$) – Cost (k_i)$*$ Moves ($N_i(t)$)
Control (10) – Cost (1) $*$ Moves (2) = 8

4.5 Discussion

This chapter has described a conceptual model of a defence mechanism which utilise game theory principles. The specific model would be ideal to be implemented using a simulator and tested over empirical data in order to validate its performance over real attacks. The combination of the FlipIt game with the fictitious strategy of play looks promising and very powerful in order for the defender to analyse his game, model the attacker methodology and choose his best available move.

5. Cyber Warfare Components

The aim of this chapter is to describe some basic components of Cyber Warfare. A key task before trying to solve any kind of problems is the comprehensive analysis of the problem domain. The two major parts of information incidents are the people who are involved and the weapons available to these people. A modelling and categorisation of the possible types of attackers that any computer security agent might face and a description of their arsenal will take place. It is significant to be well informed about your enemy in order to become capable to defend your system to the maximum of your potentials. The last subsection illustrates a conceptual model of a defence system which involves the attacker's modelling.

Modelling of the adversarial nodes is very helpful for the security agent of the system because he might be able to identify the goal and the intent of the attacker [44, 45]. It might also be able to figure out the weapons used by the adversary and what might be his next move.

5.1 Attacker taxonomy [32, 33, 34]

The taxonomy of the attacker is not an easy and straightforward task. For many years, security specialists are trying to find the patterns that match any possible cyber incident with a category of an attacker. The difficulty of this procedure is the fact that people who tend to produce adversarial situations are not rational and are always unpredictable in terms of skills, aims etc. Many researchers have drawn their own categories of hackers and some of them are displayed below:

5.1.1 Taxonomy 1

In 1985, Bill Landreth wrote the book "Out of the inner circle: a hacker's guide to computer security" where he proposed the following five categories of a hacker:

- Novices: This category consists of young hackers of the ages 12-14 who engaged in petty mischief making.
- Students: This category involves people who have the same characteristics as the first hacker's who were products of the MIT in 1970. The people of this category have a minimal criminal motivation and they are interested mostly in hacking for intellectual challenges.
- Tourists: These people have more criminal motivations than the students category and are enjoying being in adversarial situations.
- Crashers: This category involves people whose primary goal is to damage information and systems.
- Thieves: Finally the fifth category involves real dangerous and sophisticated criminals who get paid for the attacks they produce.

5.1.2 Taxonomy 2

In 1988, Richard C. Hollinger categorised the hackers in three groups:

- Pirates: This category concerns with not advanced hackers with activities limited to copyright infringements and distribution of illegally copied software.
- Browsers: Here are the hackers who aim to gain unauthorised access to information systems and browse through private and important data.
- Crackers: This is the most dangerous category of the specific researcher which involves sophisticated hackers aiming for sabotage and modification of files and programs.

5.1.3 Taxonomy 3

In 1996, Chantler N. proposed three categories of attackers:

- Losers and Lamers: This category concern with hackers of low intellectual ability who are motivated by greed and vengeance.
- Neophytes: Hackers with much more sophisticated skills of the previous category.
- Elites: The most dangerous hackers characterised by high level of technical skills who are motivated by challenge, excitement and achievement.

5.1.4 Taxonomy 4

The final taxonomy is the one made in 2009 by Meyers et al. The specific taxonomy is heavily based on the work made by Rogers during the years 2000-2006. Roger has made a comprehensive analysis of the attackers' motivations and extracted some important characteristics from a sample of sixty six cyber hackers. The proposed classification consists of eight categories of hackers.

- Script kiddies, newbies and novices: This category includes people with limited programming skills who mostly use toolkits (pre-written scripts freely available on the internet) for their actions thus their maliciousness level is low. Most of the hackers are young in age and motivated by thrill-seeking and boredom.
- Hacktivists, Political activists: The main characteristic of the people of the specific category is their political motivation. Their malicious actions consist of defacement and denial of service attacks against the sites of rival organizations.
- Cyber punks, crashers and thugs: This category is similar with the first category. The main difference is the fact that hackers have more advanced skills and are able to write their own toolkits. They are after high-profile targets seeking for attention and recognition. Their basic actions are identity theft, spamming and defacing.
- Insiders, user malcontents: This group form the greatest risk of companies. They are motivated by revenge and the damage that they can cause is extremely large due to the fact that they know very well the system functionality and have authorised privileges.
- Coders, writers: This category concerns with the adversaries who are responsible for writing the toolkits and exploits that are used by other categories (especially the first group). They are motivated by prestige and power and their level of dangerous is corresponding to the distribution level of their code.
- White hat hackers, old guard and sneakers: This group consists of hackers motivated by intellectual challenge and penetration testing. They are not malicious although sometimes they breach the law in terms of personal privacy. These people are not consider adversaries but are included in the specific taxonomy for the sake of completeness.
- Black hat hackers, professionals, elite: This category concerns with professional criminals who use their skills for launching criminal activities. They are motivated by greed and money and they are very dangerous. They are often employed by organized crime.
- Cyber terrorists: The last category represents the most dangerous hackers in terms of maliciousness and power. They engage in state-sponsored information technology warfare and their main goal is to destroy and disrupt the cyber assets and data of a foreign nation. The attacks are well-funded, highly sophisticated and motivated by ideology.

The next figure depicts the skills and mallicuouness of the attackers' categories derived by the last taxonomy. The blue columns indicate the skills level and the red columns indicate the maliciousness of each adversarial category. The scale of this graph ranges from 10 points (stands for very low) to 80 points (stands for very high).

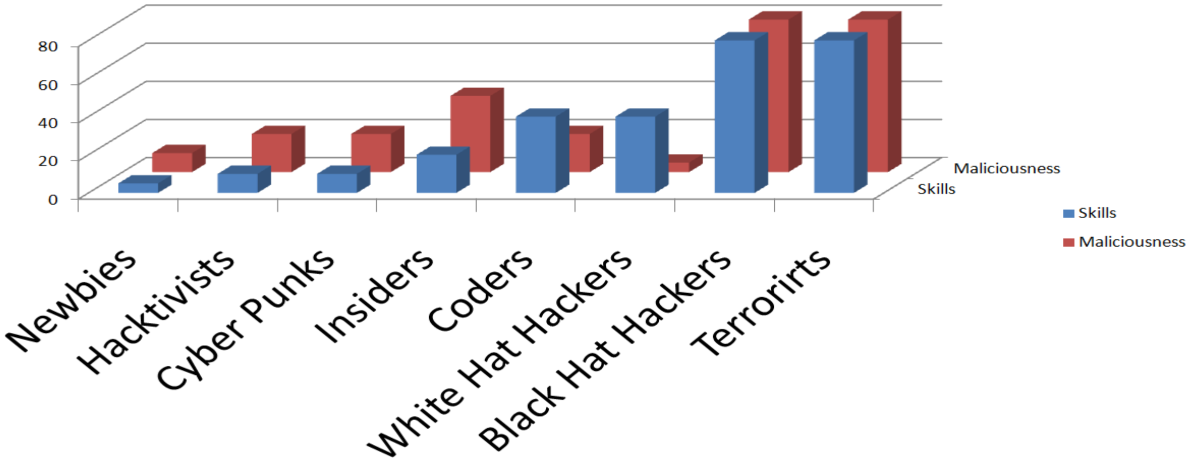


Figure 53: Skills and Maliciousness of Cyber Adversaries [32]

The next graph indicates the sophistication and motivation of the last taxonomy of cyber adversaries. The circle is divided in four quarters and each quarter has a different type of motivations. Additionally, the position that each category appears in the circle indicates the degree of the sophistication that the specific category is capable for launching an attack.

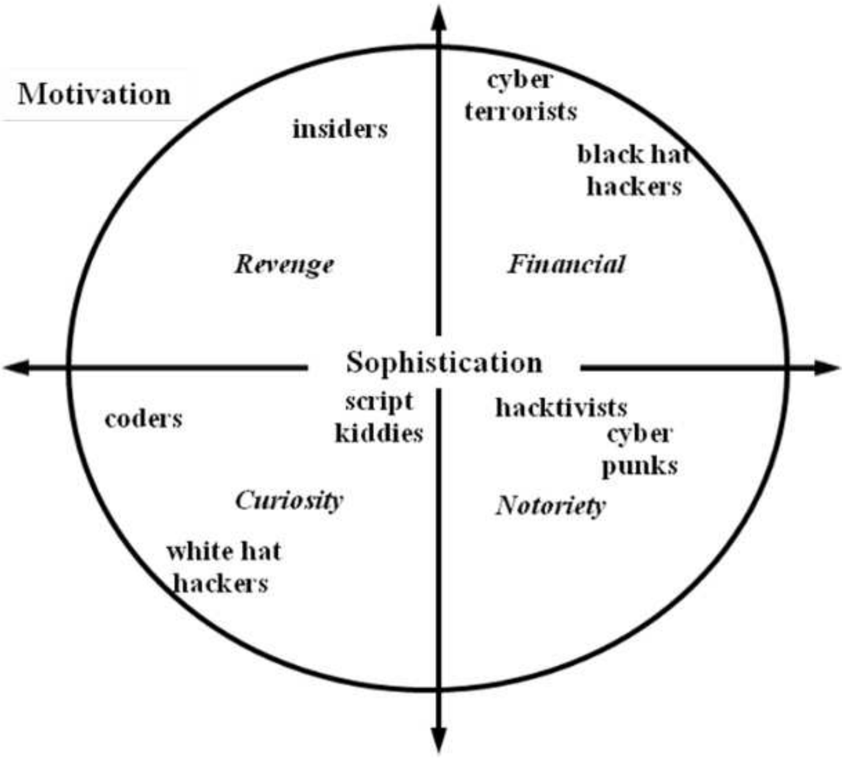


Figure 54: Motivation of Cyber adversaries [32]

5.2 Cyber Adversaries Arsenal [35]

This section will briefly cover some of the most important “digital weapons” used by the attackers for launching their attacks. Unlikely with conventional weapons, cyber weapons have two key characteristics; versatility and propagation. Versatility is the ability to generate attack on a wide variety of applications. Many times, such type of attacks are accomplished without any knowledge of the infrastructure of the target. The aptitude of a weapon to use infected programs to spread the virus to other programs as well is called propagation. The most important and known weapons that held in a cyber warfare arsenal are the following [35, 36, 37]:

- Computer worms: malicious computer programs which are designed to spread using computer networks. Self-executable scripts hidden in messages or e-mail attachments can be used to install the worms. They are spread using system’s vulnerabilities and they usually cost some damage to the network (bandwidth consumption).
- Botnets: Involves compromised computers that are control and exploit from a head computer for malicious activities on the network.
- Trojan horses: Applications that seem to perform desirable functions for the user but they steal information or harm the specific system that activated them.
- Viruses: A malicious computer program similar to worms but with differences in the technique they use to reproduce and spread. It is able to corrupt or delete data on a computer.
- Software vulnerability exploitation: Software with bugs which are exploited by the adversary to proceed with actions that will cause the information system to behave unintended or unanticipated. Exploiting of vulnerabilities help the attacker to intrude to the system, escalate privileges and launch DoS/DDoS attacks.
- Denial of service attacks: actions that tend to make a computer resource unavailable to its authorised users. The most important attacks of this category involves: consumption of computational resources (bandwidth, processor time and disk space), disruption of state information, disruption of physical network components and disruption of configuration information (i.e. routing information).
- Root kits: Hidden software that enables continues privileged access to a computer.
- Keystroke logging: Hidden software that monitors the keyboard activity of a user.
- IP spoofing: Altering or hiding the real IP address of a computer system in order to conceal the identity of the sender.
- Logic bombs: Malicious software installed on an information system which will deactivate when several criteria are met.
- Spamming: The exploiting of e-mail servers for sending randomly and unauthorised bulk of messages.

5.3 Types of Defence [38, 39]

There are six main categories of defences: prevention, deterrence, indications and warnings, detection, emergency preparedness and response.

Prevention is the operation which prevents the attack from occurring in the first place. This is usually achieved by denying access to the target information resource to the offensive player. Some other defences’ procedures of this category include: authentication, information hiding, access controls and vulnerability assessment and avoidance. Authentication concerns with mechanisms for confirming the identity of people and the authenticity and integrity of information (passwords, access tokens, biometrics, watermarks and digital signatures).

Information hiding concerns with the prevention of unauthorised disclosure of information (locks and keys, encryption and paper shredders). Access controls consist of computer control mechanisms such as guards, gates, login programs, firewalls and other. Finally, vulnerability assessment and avoidance concerns with finding and eliminating security holes or back-doors in information resources and human practises (personnel screening, security training and awareness, network scanning, penetration testing, product and system certification and backups).

Deterrence involves the procedures taken to prevent an offensive player to proceed with an attack. This category is constituted by laws and the threat of criminal penalties or civil action and the potential for retaliatory action. Security controls of a preventative nature have a deterrence role as well [40].

Indications and warnings are the procedures taken in order to recognize a potential attack before it becomes real or during the early stages. This can be very helpful for future measures to avert the attack or diminish its consequences. This category involves collection and analysis of information about attacks of similar threats which have been already occurred. It would be very useful for a defender to know the methods and aims of the attacks which used by the offensive player in order to prevent any attacks against his own information resources.

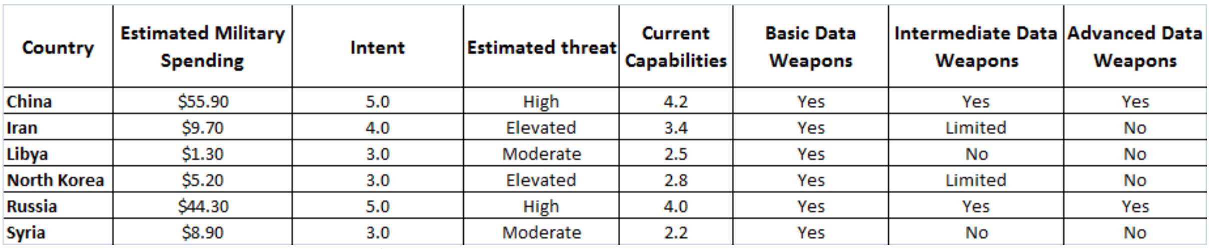
Detection is constituted by similar procedures like the previous category but it generally refers to the use of surveillance techniques (i.e. monitors) in order to recognize an attack after it has started. The procedures of this category include the scan of open media for false and damaging information, filter incoming messages, audit system’s operations and detect attacks in operations. Tools for performing these procedures include security guards, surveillance cameras, computer intrusion and detection systems and virus scanners. The ideal detection model would tackle the attack to its early stages but this situation is really difficult because most offensive operations use deceptive techniques to avoid detection.

Emergency preparedness concerns with the responses of the system to an attack when it occurs and the capability to recover to a normal condition. The tools which are being used in this category include backups and establishment of an incident response capability. In many situations it is known that it is not possible to anticipate or prevent all attacks.

Finally, response or incident handling concerns with actions that are taken after an attack occurs. Operations include recovering from damages and hardening defences. The attacks are investigated and the appropriate actions are taken against the attack. Such actions include notification, prosecution, sue, passing of new laws and other. The defence might response with a similar attack against the offensive player. An example of a national level might lead a government to respond with economic threats, military action or in extreme cases with a declaration of war. An estimation of some cost might be possible in this category. For example, in the situation where documents of outside sources get destroyed, the defence will suffer the purchasing cost. In other situations, where a company losses its competitive position it would be much difficult to estimate the cost of regaining its previous position.

5.4 Theoretical models of a Nation-State Level Offensive Player [41]

There are three main approaches for a nation to conduct cyber warfare. The first approach is by using the forces own by the nation. Many countries have stated that are capable for conducting cyber warfare. This approach is the most expensive one due to the fact that a construction of a cyber military needs a lot of resources. The benefits of this approach are that the nation will have full control and coordinate the attacks precisely to its major goals.



Country	Estimated Military Spending	Intent	Estimated threat	Current Capabilities	Basic Data Weapons	Intermediate Data Weapons	Advanced Data Weapons
China	$55.90	5.0	High	4.2	Yes	Yes	Yes
Iran	$9.70	4.0	Elevated	3.4	Yes	Limited	No
Libya	$1.30	3.0	Moderate	2.5	Yes	No	No
North Korea	$5.20	3.0	Elevated	2.8	Yes	Limited	No
Russia	$44.30	5.0	High	4.0	Yes	Yes	Yes
Syria	$8.90	3.0	Moderate	2.2	Yes	No	No

Estimated Military Spending is in Billions of U.S. Dollars
Rating Scale: 1 = Low 2 = Limited 3 = Moderate 4 = High 5 = Significant

Figure 55: Analysis of the Cyber Threat of Six Nations [35].

The second approach for conducting cyber warfare is by using volunteers. The positives of this approach are the facts that an attack will cost nothing to the nation and an attack cannot be linked direct to the state. The disadvantage of this approach is the unpredictability altitude of volunteers who might go beyond the aims of the state or more badly to involve other countries in the conflict.

Finally the last approach is using outsourcing. It is possible for a nation to employ mercenaries to launch its cyber attack. The real attacker can hide behind a third country which does not have any official policy or organizational structure. In such situations it is really hard to prove that a specific state is behind an attack. The weakness of this approach is the concern that the outsourcing party might change sides and start to blackmail the government. Moreover, if the outsourcing party is constituted by criminals, the employer state might exploit by the outsourcing party to pursue their criminal activities.

5.5 A Conceptual Model using the classification of the Adversary

A reliable and accurate modelling of the cyber warfare attacker is a very useful tool for every information security agent. This modelling can be used from the systems' administrators in order to figure out the type of the attacker that they are facing and be prepared of what they might encounter. The proposed system should have the following six steps:

1. Gathering attack's information: After an information system has been attacked, various kinds of sensors must start gathering any kind of information related with the specific attack. Such information might consists of: the specific domain of the system that the attack took place, the type of damage and the level of damage that caused, possible malicious software that the sensors discovered within the system and other.
2. Analysis of the attack's characteristics: All the information that have been gathered in the previous task must be analysed and run on a trained classifier that will try to match the specific attack with patterns of known attacks.
3. Adversary Categorisation: The previous section will enhance the categorisation of the attack to a group of attackers. This categorisation should give to the security specialist the possible electronic weapons that the specific category of attackers might have available. This fact will increase the awareness of the defender of what might be the next step of the attacker. The categorisation it should also give the intents and objectives of the specific group of attackers. The security agent should try for a better distribution of any available defensive mechanisms. The intents of the attacker should show with a probability distribution over all the parts of the information system, which part is targeted by the attacker.

4. Utility of Game Theory principles in order to have the best reactions: Finally, the system should have the proposed game theoretic defence mechanism in order for the attacker to be able to choose the best possible action he has available.

6. Analysis and Evaluation of Game Theory in Information Warfare

Cyberwarfare is a complex and extremely difficult area of research which tends to evolve daily. Although security specialists are fighting for more than twenty years trying to find the appropriate defence mechanism for exterminating the information warfare threats the problem remains unsolved. On the other hand, the game theory principles have shed a light to this black Pandora box giving a hope for more reliable and accurate defence mechanisms. The results of game theory application in other disciplines are extremely surprising [3, 45] and it is also possible to find answers in the field of cyberwarfare.

Many ad-hoc security mechanisms are active in various systems and effectively can solve the particular problems they are designed for. Nevertheless, are not capable to respond appropriately under dynamically changing real world scenarios. Game theory is a mature and effective methodology for analysing competitive situations in many different disciplines like economics, political sciences, management and others. Similar to those strategic situations is the information warfare field.

A game theoretic application for countering possible cyber warfare incidents might be possible to achieve the following [5, 21, 24, 42]:

- Game theory could provide a better understanding of cyber warfare tactic and implications.
- Game theory principles can model the information warfare domain and develop a formal decision and control framework.
- Automation of human irreplaceable decision making mechanism.
- Possible to model attacker's behaviour, intent and target.
- Provide the ability to analyze million of possibilities, model opponent characteristics, and self-generate what-if scenarios. Computers are capable to analyse huge numbers of possibilities in order to find exceptions to general rules that can be exploit cruelly. In some cases, whole new theories on how to play are constructed because of this fact (probabilistic outcomes could have a strong impact on game play).
- Game theoretic techniques have proven successful at analysing what-if scenarios, allowing comprehensive analysis of significant chains of events, and utilizing that analysis at a later date.
- Game theory provides the capability of examining hundreds of thousands of possible scenarios.
- Game theory can provide techniques for suggesting a number of potentials courses of action with associated predicted payoffs.
- Game theory provides the technique to illustrate complex, competitive games into mathematical models that allow a more precise study of the situation at hand.
- Game theory can be used to better understand behaviour in competitive social situations. It can provide a means to define and specify elements influencing decisions and to make behavioural guesses.
- Game theory models can predict actual game play (i.e. those that yield the highest payoff).
- After the validation of a game model, game theory could predict behaviour and provide the means to study why people act as they do in information warfare situations.
- Game theory gives the opportunity for a formal modelling and analysis of complex social situations. Constructing a mathematical model that represents

> selected features of a complex social situation can allow a player to better understand some of the elements influencing the specific situation. Moreover, if the underlying game model is adequately robust, it can form the foundation for: policy development guidelines and decision support tools.

On the other hand, information warfare incidents are not like conventional crime and are much more difficult to create defence mechanism against them. Some of the features and challenges that a security specialist must bear in mind are the following [43]:

- The actions will not always complete successfully (regardless of the opponent's actions).
- Difficult to gather evidence's of an attack
- Players' risk aversion has a strong impact on his chosen strategy
- Payoffs are difficult to predict. The impact of an attack in terms of losses is not easy to calculate in the virtual world. The Nash Equilibrium of a game has a great dependant on the outcome payoffs of the game. This is a crucial and important finding that all the players of the game should bear on mind. The probability distribution on the sensor networks has also a large fraction of contribution for deciding the next move. The correct analysis highly depends on the payoff functions thus, they should reflect the trade-offs of the system at hand. The researchers are imposed to make a comprehensive analysis for finding the most accurate payoffs of each player and the capabilities of any kind of sensors they might use. A promising technique is the use of supervised learning schemes in order to approximate the actual player payoffs and detection capabilities of the different kinds of sensors.
- The strong assumption that all the players participating in a game are rational is not real in warfare situations. It is known that humans tend to act irrational during adversarial events.
- Limited examples: The application of game theory to information warfare has limited examples yet and this is the fact that makes it difficult for providing a critical and comprehensive evaluation.
- Multiple simultaneous moves: Most of the games in game theory have players who tend to alternate moves. In the domain of cyberwarfare this assumption is not true and in most situations, the defender and the attacker of the system move simultaneous transforming the game to a very complex event. Additionally, the attackers are likely to launch multiple simultaneous moves.
- Opponent under no time constraint: The attacker might come back in a later period of time with a stronger attacking technique after he analyse the game of the defender. The game of information warfare does not have an end state and this can be widely exploited by the attacker.
- Opponent may have different goals from the defender: In information warfare there is no symmetry between the evaluation functions of each player. This might give great probabilities for either player to win or it might show that one asset is very important for the attacker but for the defender is not so vital for his system.
- Set of known legal moves may change: Most of the games that have been analysed using game theory have standard rules which are known to all the participants of the game. In the field of information warfare the specific assumption is extremely wrong. In cyber warfare everything goes and there are not any strict regulations. On a regular basis, the attackers construct new and more sophisticated techniques for accomplishing their illegal actions. Security agents are always facing unknown attacks and are lacking of appropriate response.

- Opponent end goals may change: Despite the conventional games which are analysed in game theory, an information system is usually under the attack of different opponents which can be considered equivalent to an opponent changing goals. The alteration of objectives of an attacker during the game results to the adoption of a new evaluation function. The defender is challenged to find if his opponent has changed his goals and transform his defensive techniques to suit the new game which have been created.
- Time of moves and state updates are not well defined: In game theory literature, when a player moves then the effect of the move is instantaneously. In information warfare games, the action of one player usually needs a variable amount of time in order to complete and in many cases an action is semi-completed or fails. This is the big difference between an intended move and a complete move.

6.1 Future Work

The proposed models could extend and modified for analysis of the specific attacks in low levels. Simulations of the specific models can give more clear results of the capabilities of applying game theory in information warfare. The simulations could give a better evaluation of what the proposed systems can achieve. Furthermore, the models should be tested using a large number of available options for each player in order to assess the time needed for response and whether the proposed system are appropriated in the dynamic field of cyberwarfare. Finally, categorisation of the attackers' objectives and skills should be done by analysing and simulating the specific attacks.

7. Conclusion

This thesis has managed to investigate in deep the principles of game theory and some of their application to information warfare. Past results of game theory application in strategic situations of different disciplines have shown remarkable solutions. The application of game theory in information warfare is extremely promising and seems to be able to shed a light in this enormous problem of the twenty first century [45].

The great difference of the information warfare domain related with the other disciplines where game theory has been applied successfully is the unexpected nature of the specific field and its tend to dynamically and frequently change. This is the greatest disadvantage that has the application of game theory in cyberwarfare. On the other hand, the powerful principles of this mathematical framework for analysing any kind of strategic situations can dramatically enhance the performance of any defence mechanism considering the results of such analysis.

A perfect defence to any kind of adversaries' attacks does not exist. The only available options to the security agents of an information system is to response to the attackers' moves and try to gain back the control of their system [29]. Although the silver bullet of the specific problem domain has not been founded yet, game theory seems to be the most promising methodology that each defence mechanism should utilise to encounter any kind of information attacks.

How much Security is enough?

"You still don't know if you're dealing with a kid, organized crime, an intelligence service or an economic competitor. [Frank Cilluffo]"

Lincoln's Riddle: "If I call the dog's tail a leg, how many legs does it have? Four! It doesn't matter what you call the tail; it is still a tail." [29]
Corollary to Lincoln's Riddle: "Calling a system secure, does not actually make it secure. Rather it just identifies it as an interesting target for the adversary." [29]

8. References

1. Libicki, M. C. (1995) What is information warfare? Washington, DC: National Defence University, Institute for National Strategic Studies.

2. Ramsaroop, P. (2003) Cybercrime, cyberterrorism, and cyberwarfare: critical issues in data protection for health services information systems. Washington, DC, Technology and Health Services Delivery, Health Services Organization Unit, Pan American Health Organization.

3. Turocy T.L., and Stengel von B. (2001) Game Theory http://www.cdam.lse.ac.uk/Reports/Files/cdam-2001-09.pdf [Accessed 15 September 2011]

4. Cabinet Office (CSIA). (2007) A National Information Assurance Strategy http://www.culture.gov.uk/images/working_with_us/nia_strategy.pdf [Accessed 31st August 2011]

5. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q. (2010) A survey of game theory as applied to network security. The 43rd Hawaii International Conference on System Sciences.

6. Stytz, M., and Banks S. (2010) Addressing Simulation Issues Posed by Cyber Warfare Technologies http://www.scs.org/magazines/2010-7/index_file/Files/Article_Stytz.pdf [Accessed 15 September 2011]

7. Davis, J. (2007) Hackers Take Down the Most Wired Country in Europe http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all [Accessed 31st August 2011]

8. Potter C., and Beardcite A. (2010) Information Security Breaches, PricewaterhouseCoopers www.pwc.com [Accessed 31st August 2011]

9. Verton, D. (2002) FBI chief: Lack of incident reporting slows cybercrime fight http://www.computerworld.com/s/article/75532/FBI_chief_Lack_of_incident_reporting_slows_cybercrime_fight?taxonomyId=082 [Accessed 31st August 2011]

10. Carr, J. (2009) Inside Cyber Warfare. Sebastopol: O'Reilly Media.

11. Richardson, R. (2008) 2003 CSI/FBI Computer Crime and Security Survey http://www.gocsi.com, [Accessed 31st August 2011].

12. Wihl, L., Kong, J., and Varshney, M. (2010) Introducing a Cyber Warfare Communications Effect Model to Synthetic Environment. Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), No. 10313, pp. 1-9.

13. Polak, B. (2007) Game Theory. YALE ECON 159, University of Yale, 15 November 2010 [Lecture Notes Taken by Benjamin Polak].

14. Matusitz, J. (2009) A Postmodern Theory of Cyberterrorism: Game Theory. Information Security Journal: A Global Perspective, Vol 18, pp.273-281.

15. Nebel, B. (2009) Game Theory. University of Freiburg [Lecture Notes taken by Bernhard Nebel].

16. Osborne, J. M., and Rubinstei, A. (1994) A Course in Game Theory. Cambridge: MIT Press.

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

18. Rasmusen, E. (2006) Games and Information: An Introduction to Game Theory. 4th Ed. Wiley-Blackwell.

19. Slantchev, L. B. (2010) Game Theory. POLI 204C, Department of political Science, University of California.

20. Burke, D., (1999) Towards a game theory model of information warfare. MSc in Software Systems Management , Graduate School of Engineering and Management, Airforce Institute of Technology, Air University.

21. Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V. (2010) On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks, SpringSim.

22. Agah, A., and Das, S. K. (2007) Preventing DoS attacks in wireless sensor networks: A repeated game theory approach. International Journal of Network Security, Vol 5, No 2, pp. 145-153.

23. Bedi, H.S., Roy, S., and Shiva, S. (2011) Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. Computational Intelligence in Cyber Security (CICS), IEEE.

24. Alpcan, T., and Basar, T. (2003) A game theoretic approach to decision and analysis in network intrusion detection. In Proceeding of the 42nd IEEE Conference on Decision and Control (CDC).

25. Alpcan, T., and Basar, T. (2004) A game theoretic analysis of intrusion detection in access control systems. In Proceeding of the 43rd IEEE Conference on Decision and Control (CDC).

26. Liu, Y., Comaniciu, C., Man. H. (2006) A bayesian game approach for intrusion detection in wireless ad hoc networks. In Proceedings of the Workshop on Game Theory for Communications and Networks, page Article No.4.

27. Nguyen, K. C., Alpcan, T., and Basar, T. (2009) Security games with incomplete information. Proc. of IEEE Intl. Conf. on Communications (ICC).

28. Khirwadkar, T.S., (2011) Defense Against Network Attacks Using Game Theory. MSc in Computer Science, University of Illinois at Urbana-Champaign

29. Rivest, L.R. (2011).Illegitimi non carborundum. Invited keynote talk given August 15, 2011 at the CRYPTO 2011 conference (Santa Barbara).

30. Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu, Q. (2010) An Imperfect Information Stochastic Game Model for Cyber Security, The 5th Intnl Conference on i-Warfare and Security.

31. Lye, K., and Wing, J. M. (2005) Game strategies in network security. In Proceedings of the 2002 IEEE Computer Security Foundations Workshop.

32. Meyers, C., Powers, S., and Faissol, D. (2009) Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. Technical Report, Lawrence Livermore National Laboratory.

33. Meyers, C., Powers, S., and Faissol, D. (2009) Probabilistic Characterization of Adversary Behavior in Cyber Security. FY2009 SMS Project, Final Report, Lawrence Livermore National Laboratory.

34. Kjaerland, M. (2005) A Classification of Computer Security Incidents Based on Reported Attack Data. Journal of Investigative Psychology and Offender Profiling, Vol 2, pp.105-120.

35. Coleman G. K., (2007). World War III: A Cyber War has begun www.technolytics.com [Accessed 31st August 2011].

36. Coleman G. K., (2007). *Department of Cyber Defence: An Organisation who's time* has come! www.technolytics.com [Accessed 31st August 2011].

37. Denning, P. J., and Denning, D. E. (2010) Discussing Cyber Attack. Communication of the ACM, Vol 53, No 9, pp. 29-31.

38. Denning, D. (1999) Information Warfare and Security. Wesley: ACM Press.

39. B. Panda and J. Giordano, (1999) Defensive Information Warfare. Communications of the ACM, Vol. 42, No. 7, p. 31-32.

40. Hayes, Richard E. and Gary Wheatley. (1996) Information Warfare and Deterrence. Strategic Forum 87, Institute for National Strategic Studies.

41. Ottis, R. (2009) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon, Reading: Academic Publishing Limited, pp 177-182

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

43. Hamilton, S. N., Miller, W. L., Ott, A., and Saydjari, O. S. (2002) Challenges in applying game theory to the domain of information warfare. Proceedings of the 4th Information survivability workshop (ISW-2001/2002).

44. Liu, P., Zang, W., and Yu, M. (2005) Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies. ACM Transactions on Information and System Security , Vol 8, No 1, pp. 1-41

45. The Economist. (2011) Game theory in practice http://www.economist.com/node/21527025 [Accessed 15 September 2011]

9. Appendices

9.1 Appendix A: Information Warfare Incidents

Estonia Vs Russia [1] [2] [3]

On the 27th of April 2007, a huge wave of cyber attacks “swamped” websites of Estonian organizations including Estonian parliament, banks, ministries, newspapers and broadcasters. Russia was the country which blamed for this heavy attack. According to Estonia (the most wired country in Europe), the motive for these attacks was the move of a Soviet war memorial in Tallinn (the statue which was symbolizing the winning of Russia in the War World Two). Estonia’s action was condemned by the Kremlin. The defence ministry of Estonia said that the cyber attacks came from all over the world but some have been hosted by Russian state servers. On the other hand, Moscow denied any involvement in the internet attacks and said that the allegations were completely untrue. The attacks had a really bad impact in the country of the so-called “Paperless Government”. Estonia depends largely on the internet considering that its government run online, all the bank services are on the internet et al. Even their election for parliament has been done via the internet. The attacks were of the form of Denial-of-Service attacks and for three weeks they had as outcome the paralysation of key organisations of the country. Jaak Aaviksoo, Estonian Minister of Defence, stated that "The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia and this affected the majority of the Estonian population". This was the first time in history that a cyber-warfare threatened the national security of an entire nation and that is the reason many people called it “Web War One”. The attacks were orchestrated by individual hackers mainly from Russia, and there were coordinated through public and private chat rooms.

China Vs Google [4] [5] [6]

In mid-December 2009, a highly sophisticated and targeted attack on Google’s corporate infrastructure originating from China was detected. The goal of the specific attack was the theft of intellectual property from Google. The Google Company stated that a minimal amount of user information was compromised, and that the attackers’ primary goal was to access information of Chinese human rights activists. According to Google this was not achievable and they only mange to access only two Gmail accounts with limited activity related to account information. Also, they mentioned that the specific attacks were intended to at least twenty other major companies spanning sectors including Internet, finance, chemicals, and more. Phishing attacks aiming the compromise of the Gmail accounts of Chinese human rights activists around the world were reported as well. These attacks were achieved by phishing scams or malware placed on the users’ computers. An investigation

[1] BBC News. (2007) The cyber raiders hitting Estonia, bbc.co.uk [Internet] 17 May 2007. Available at http://news.bbc.co.uk/1/hi/world/europe/6665195.stm [Accessed 15 September 2011]

[2] BBC News. (2007) Estonia hit by ‘Moscow cyber war’, bbc.co.uk [Internet] 17 May 2007. Available at http://news.bbc.co.uk/1/hi/world/europe/6665145.stm [Accessed 15 September 2011]

[3] Davis, J. (2007) Hackers Take Down the Most Wired Country in Europe http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all [Accessed 15 September 2011]

[4] BBC News. (2010) China leadership ‘orchestrated Google hacking’, bbc.co.uk [Internet] 4 December 2010. Available at http://www.bbc.co.uk/news/world-asia-pacific-11920616 [Accessed 15 September 2011]

[5] Quain, J.R. (2010) Google vs. China: The Tip of the Cyberwar, foxnews.com [Internet] 22 January 2010. Available at http://www.foxnews.com/scitech/2010/01/22/google-vs-china-tip-cyberwar/ [Accessed 15 September 2011]

[6] Haddad, M. (2011) Google Points the Finger at the Chinese Government In Latest Cyber Attack http://business2press.com/2011/03/20/google-blames-chinese-government-second-gmail-cyber-attack/ [Accessed 15 September 2011]

showed that dozens of Americans, Chinese and European Gmail users who are advocates of human rights in China appear to have been regularly accessed by third parties. It is said that the motivation of these attacks has political content and are included in the attempts of Chinese Government to limit free speech on the web. Google threaten that it would stop cooperating with Chinese Internet censorship and consider shutting down all of its operations in the country. Further investigations showed evidence of unknown vulnerabilities of Microsoft's Internet Explorer web browser. The specific vulnerability has been used by the hackers in order to gain access on individuals' computers at different companies and download intellectual property data, computer code and other secrets that were stored in the servers they controlled. Most of the companies involved did not disclose any information because of the fear that such publication would ruin their reputation and encourage more related to the specific cyber crime. According to the experts, the attacks were highly organised and the hackers were well trained, knowing who to attack, who the key people were in the organisation and how to attack them.

China Vs India [7] [8]

According to Indian officials, for more than a year and a half, India was suffering from daily cyber attacks (since 2006). When the, senior government officials was asked publicly, he stated that India is on the target of daily cyber-warfare but according to the researchers, the detected cyber-attack wave origin in China is much more real and severe. The incidents were classified as well organised and sophisticated aiming sensitive information from both government and private computers of India. Three main techniques were used against Indian networks: Bots, key loggers and mapping of networks.

Russia Vs Georgian [9] [10] [11]

On August of 2008 Russia and Georgian had an armed conflict. A week after the initiation of the war between the two countries, Georgian faced a well structured coordinated attack. Cyber attacks were detected weeks before the warfare but without such a big impact on the on-line services of Georgian. Main targets were government websites, Georgian news sites and other popular information forums. The attacks comprised of defacement of the websites, web-based Psychological Operations (Psyc-Ops), a fierce propaganda campaign (PC) and Distributed Denial of Service attacks. The attacks managed to "hijack" many of the key websites of Georgian even before Russia's armed intervention into Georgian. In this example of Cyber-attack it is high noticeable that such kind of warfare can be a very powerful weapon in hostile situations like a war. The Georgian Ministry of Foreign Affairs said: "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs".

Russia Vs Kyrgyzstan [12] [13] [14]

[7] Hoffman, S. (2010) China Hackers Launch Cyber Attack On India, Dalai Lama, crn.com [Internet] 6 April 2010. Available at http://www.crn.com/news/security/224201581/china-hackers-launch-cyber-attack-on-india-dalai-lama.htm;jsessionid=SBtsDiacTxcpgfWzToywhw**.ecappj01 [Accessed 15 September2011]

[8] Branigan, T. (2010) Cyber-spies based in China target Indian government and Dalai Lama, guardian.co.uk [Internet] 6 April 2010. Available at http://www.guardian.co.uk/technology/2010/apr/06/cyber-spies-china-target-india?INTCMP=SRCH [Accessed 15 September 2011]

[9] Hoffman, S. (2008) Russian Cyber Attacks Shut Down Georgian Websites, crn.com [Internet] 12 August 2008. Available at http://www.crn.com/news/security/210003057/russian-cyber-attacks-shut-down-georgian-websites.htm [Accessed 15 September 2011]

[10] Arun, N. (2008) Caucasus foes fight cyber war, bbc.co.uk [Internet] 14 August 2008. Available at http://news.bbc.co.uk/1/hi/world/europe/7559850.stm [Accessed 15 September 2011]

[11] Defensetech. (2008) Cyber War 2.0- Russia v. Georgia http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/ [Accessed 15 September 2011]

On January 2009, in the small country of Kyrgyzstan, three out of the four main internet service providers were under a massive online assault. The evidences showed that Russian cyber militia was guilty for the specific attack. A successfully distributed denial of service attack managed to take Kyrgyzstan “offline”. The cyber-security expert Don Jackson of Internet security firm Secure-Works stated that the attack shut down more than eighty percent of Kyrgyzstan’s bandwidth. Once more, the motivation of the attack seems to be of political content. A number of analysts have considered that the attack is intended to prevent Kyrgyzstan’s embattled political opposition or to pressure Kyrgyzstan’s government, which hosts a U.S. airbase outside of the capital, Bishkek.

Turkey Vs Cyprus [15] [16]

On the 27th of December 2010, twenty Cypriot Companies websites were invaded by Turkish hackers. The attacks comprised of defacement of the websites and on each site they put an image of Cypriot democracy under a crescent with the slogan: No terrorism in sports. This cyber-attack is considered to be retaliation for the episodes during the match between APOEL and Pınar Karşıyaka for the final phase of Euro-challenge 2010.

LizaMoon SQL Injection Attack [17] [18] [19]

Unidentified cyber criminals used a well-known attack vector that utilizes security vulnerabilities on other sites to insert a link to their website. Unsuspecting users who visited the sites that were compromised by the attackers confront a message saying that their computer was infected by various types of viruses offering them to download fake virus protection. The victims of this well structured attack were basically paying the hi-tech criminals for protection over their computer but indeed they were only giving them money. A security firm call Websense has been tracking the attack since it started on 29 March and count over 28,000 sites that were compromised to the specific attack. Patrik Runald, senior manager for security research at Websense told the BBC's Katty Kay that the scale of the attack was "worrying". It is a very good orchestrated attack if you consider that the Google search finds hundreds of thousands URLs with the nasty script around the world. Also, it is said that the criminals do have the bank details of the victims and they might try to get some more money. The specific attack was called LizaMoon after the first domain Websense discovered with the malicious script on March 29. It is believed that it was an SQL injection. SQL injection is when hackers get their script into a Microsoft SQL Server database which

[12] Hodge, N. (2009) Russina ‘Cyber Militia’ Takes Kyrgyzstan Offline? http://www.wired.com/dangerroom/2009/01/cyber-militia-t/ [Accessed 15 September 2011]

[13] Keizer, G. (2009) Russian ‘cybermilitia’ knocks Kyrgyzstan offline http://www.computerworld.com/s/article/9126947/Russian_cybermilitia_knocks_Kyrgyzstan_offline [Accessed 15 September 2011]

[14] Defensetech. (2009) Russia Now 3 and 0 in Cyber Warfare http://defensetech.org/2009/01/30/russia-now-3-and-0-in-cyber-warfare/ [Accessed 15 September 2011]

[15] Aftzigianni, V. (2010) Turkish Hackers Launch Massive Cyber-Attack on Cypriot Companies, greekreporter.com [Internet] 27 December 2010. Available at http://eu.greekreporter.com/2010/12/27/turkish-hackers-launch-massive-cyber-attack-on-cypriot-companies/ [Accessed 15 September 2010]

[16] Computer Service Now. (2010) Cypriot Companies Attacked by Turkish Hackers http://blog.computerservicenow.com/posts/2010/12/28/cypriot-companies-attacked-by-turkish-hackers/ [Accessed 15 September 2011]

[17] Gonsalves, A. (2011) LizaMoon SQL Injection Attack Hits Websites, informationweek.com [Internet] 1 April 2011. Available at http://www.informationweek.com/news/security/attacks/229400764 [Accessed 15 September 2011]

[18] BBC News Technology. (2011) Sites hit in massive web attack, bbc.co.uk [Internet] 1 April 2011. Available at http://www.bbc.co.uk/news/technology-12933053 [Accessed 15 September 2011]

[19] Allan, D. (2011) LizaMoon SQL Injection attack not as widespread as thought http://www.techwatch.co.uk/2011/04/04/lizamoon-sql-injection-attack-not-as-widespread-as-thought/ [Accessed 15 September 2011]

then adds it to a site's URL. SQL injections are one of the most common forms of attacking web sites and back end databases.

Night Dragon Attacks [20] [21]

In November 2009, at least a dozen multinational oil, gas and energy companies targeted from cyber-criminals. According to the security firm McAfee the hackers took advantage of various computer vulnerabilities and weak security controls to gain access to their computers and steal their secrets. Five of the energy firms have confirmed the attacks. Top confidential documents of these firms concerning with oil exploration and bidding contracts were the major targets of the attackers. Such documents are tremendously sensitive and worth huge amounts to competitors. According to Greg Day, director of security strategy at McAfee, the attacks were based on code and tools widely available on the net's underground. This fact shows minimal level of proficiency and structured attack but on the other hand the attacks were successfully. Rik Ferguson, director of security research at Trend Micro said that "The intrusions were multi-staged, multi-vector, pervasive and sustained". Analysts suspect China for the specific attack with a common motive as the attack behind the Operation Aurora attacks on Google in China which targeted industrial plant and machinery. It is thought that the specific attack has been designed to attack Iran's nuclear programme.

Customer e-mail security breach on Play.com [22] [23]

On March 2011, many customers of Play.com, one of the most popular online shops in the UK for DVDs, CDS, games and movies might were victims of cyber attacks. Play.com blamed another company that it employs to do marketing for the specific situation and asked from its customers to be aware of spam-emails. Such kind of e-mails are aiming to trick users into believing they are sharing data with a company that they trust, and giving out personal information such as a credit card details. Silverpop, a US-based firm which was employed by the site in 2008 to manage e-mail marketing and communications stated that nothing goes wrong with the services they provide and there is not such a breach on any of its email servers. They stated that the only incident of security breach was last year where they were hit by ordering glitch. Customers of play.com received e-mails reporting the despatch of an order they did not place but it was placed by another customers. These e-mails did not contain any sensitive data but according to some customers all the messages had scrambled text at the bottom that could hide some information.

Cyber attack on France targeted Paris G20 files [24] [25]

This is the biggest and more dangerous cyber attack against France considering the top secret data that have been compromised. According to France, the attacks started on December 2010 and after France took over the presidency of the G20. The summit agreed a list of targets for reducing imbalances in the global economy in order to head off future financial

[20] McAfee. (2011) Global Energy Cyberattacks: "Night Dragon" http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf [Accessed 15 September 2011]

[21] BBC News Technology. (2011) Hackers hit 'at least five oil and gas firms http://www.bbc.co.uk/news/technology-12416580 [Accessed 15 September 2011]

[22] BBC News. (2009) Play.com hit by ordering glitch, bbc.co.uk [Internet] 6 November 2009. Available at http://news.bbc.co.uk/1/hi/technology/8346833.stm [Accessed 15 September 2011]

[23] BBC News Technology. (2011) Play.com warns of customer e-mail security breach, bbc.co.uk [Internet] 22 March 2011. Available at http://www.bbc.co.uk/news/technology-12819330 [Accessed 15 September 2011]

[24] BBC News Business. (2011) Cyber attack on France targeted Paris G20 files, bbc.co.uk [Internet] 7 March 2011. Available at http://www.bbc.co.uk/news/business-12662596 [Accessed 15 September 2011]

[25] Hall, K. (2011) France's G20 files target of cyber attack http://www.computerweekly.com/Articles/2011/03/07/245737/France39s-G20-files-target-of-cyber-attack.htm [Accessed 15 September 2011]

crises. The French finance ministry has confirmed the attacks and stated that the attackers were after documents related to the G20 and international economic affairs. More than 150 of the ministries computers were infected. It is not yet clear who is behind these attacks but according to some unconfirmed reports in the French press, they found that some information was redirected to Chinese sites. Analysts said that the topic of G20 was particularly contentious for the Chinese Government. According to Patrick Pailloux, general director of the French National Agency for IT Security, the attacks were orchestrated by “a number of professional, determined and persistent hackers".

North Korea Vs South Korea & US [26] [27]

On July 8th of 2009, North Korea was suspected for launching a cyber-attack on some of the most important government offices in the US and South Korea including the White House, the Pentagon, the New York Stock Exchange and the presidential Blue House in Seoul. US government managed to defeat the specific attacks successfully but not the same for South Korea. According to, Ahn Jeong-eun, a spokeswoman for Korea Information Security Agency, eleven organisations had either gone down or had access problems. It is believed that the attack was thoroughly prepared and committed "at the level of a certain organisation or state". Specialists on web security are concerning whether North Korea was capable of such attacks and if someone else is behind of this incident like sympathisers of North Korea or China. In 2011, South Korea faced another wave of Cyber attacks. Denial-Of-Service attacks were used by hackers in about 40 South Korean government and private websites. According to a South Korean cyber security company, AhnLab, targets included websites belonging to South Korea's presidential office, the foreign ministry, the national intelligence service, US Forces Korea and major financial institutions. AhnLab spokesman Park Kun-woo stated that the attacks were similar of others in the past and were having the same targets.

Secret US military computers “cyber attacked” in 2008 [28] [29]

Deputy Defence Secretary William Lynn, said that the specific attack by a foreign spy service was the most significant breach ever for US military networks. The attack began when an infected flash drive was inserted into a US military laptop at a base. The computer code then spread silently through US military computer networks and readied itself to transfer military data to the hackers. Further details about the attack are not available and it remained unclear whether the hackers accomplish their attack gaining access to secrets of the US military. After the 2008 assault, the Pentagon banned its work force from using flash drives but later they eased the prohibition. Since the specific attack, the military has developed methods to uncover intruders inside its network, or so-called “active defence systems”.

Asprox Virus [30] [31]

[26] Weaver, M. (2009) Cyber attackers target South Korea and US, guardian.co.uk [Internet] 8 July 2009. Available at http://www.guardian.co.uk/world/2009/jul/08/south-korea-cyber-attack [Accessed 15 September 2011]

[27] BBC News Technology. (2011) South Korea hit by cyber attacks, bbc.co.uk [Internet] 4 March 2011. Available at http://www.bbc.co.uk/news/technology-12646052 [Accessed 15 September 2011]

[28] BBC News US & CANADA. (2010) Secret US military computers ‘cyber attacked’ in 2008, bbc.co.uk [Internet] 25 August 2010. Available at http://www.bbc.co.uk/news/world-us-canada-11088658 [Accessed 15 September 2011]

[29] Physorg. (2010) Worst cyber attack on US military came via flash drive, physorg.com [Internet] 25 August 2010. Available at http://www.physorg.com/news201978152.html [Accessed 15 September 2011]

On July 2008, Eastern European cyber-criminals are suspected of placing the Asprox virus on more than a thousand key British government and consumer websites. The specific virus seems much more powerful than any other virus and it is undetected on mainstream sites and any visitor was facing the risk of being infected. In the US, the virus has gone through Sony's Playstation, the city of San Francisco and Snapple sites. The virus automatically installs itself on a visitor's computer and enables hackers to steal files, e-mails, passwords and more important to access financial information. It could also be used to infect other computers and even make attacks against companies and foreign governments. Security experts stated that at least two million computers worldwide were infected. Any computer without up-to-date anti-virus software was vulnerable. Only half of current anti-virus programmes can detect Asprox. According to Fijan, "the attack toolkit that has been used (which is aliased as "Asprox") has been around for few years; however, during the last year we have noticed a rise in the number of attacks using it". The attack toolkits is designed to first search Google for web-pages with the file extension .asp and then launch SQL injection attacks to append a reference to the malware file using the SCRIPT tag.

Activist Group Vs Australia [32] [33] [34]

On February 2010, an activist group known as Anonymous spread a cyber-attack to key Australian government websites. A man saying that he is the representative of the specific group stated that more than five hundred people are involved in the specific attack. The attacks were comprised by DDoS attacks. The reason for the attack was Australia's plan to apply a country-wide filter to block certain content in 2011 in order to make the internet a safer place for Australian children. On the other hand, the activists stated that they do not support the creation of illegal content but that banning it would not tackle the issue.

[30] Schofield, J. (2008) 'Asprox computer virus' runs riot, hits the NHS, claims The Times, guardian.co.uk [Internet] 23 July 2008. Available at http://www.guardian.co.uk/technology/blog/2008/jul/23/asproxcomputervirusrunsrio [Accessed 15 September 2011]

[31] Mostrous, A. (2008) Asprox computer virus infects key government and consumer websites, timesonline.co.uk [Internet] 23 July 2008. Available at http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4381034.ece [Accessed 15 September 2011]

[32] Kleinman, Z. (2010) Cyber attacks against Australia 'will continue', bbc.co.uk [Internet] 12 February 2010. Available at http://news.bbc.co.uk/1/hi/technology/8513073.stm [Accessed 15 September 2011]

[33] Wilkes, J. (2010) Activist group warns that cyber attacks will continue in Australia http://www.broadbandexpert.com.au/broadband-news/broadband-news/activist-group-warns-that-cyber-attacks-will-continue-in-australia_77880 [Accessed 15 September 2011]

[34] Google. (2010) Australia cyber attacks could last 'months': hackers, google.com/news [Internet] 11 February 2010. Available at http://www.google.com/hostednews/afp/article/ALeqM5jnujRPFE6kMQ8Ns22WpjgTun-PHQ [Accessed 15 September 2011]