Modelling Telecommunications Operators and Adversaries using Game Theory

Sakshyam Panda

School of Science

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo April 23, 2018

Supervisor

Prof. Marko Nieminen, Department of Computer Science, Aalto University, Finland

Advisor

Dr Ian Oliver, Nokia Bell Labs, Espoo, Finland

Aalto University
School of Science

Aalto University
School of Science

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the master's thesis

Author Sakshyam Panda

Title Modelling Telecommunications Operators and Adversaries using Game Theory

Degree programme Master's Programme in ICT Innovation

Major Human-Computer Interaction and Design **Code of major** HCID

Supervisor Prof. Marko Nieminen, Department of Computer Science, Aalto University, Finland

Advisor Dr Ian Oliver, Nokia Bell Labs, Espoo, Finland

Date April 23, 2018 **Number of pages** 54+10 **Language** English

Abstract

Telecommunications systems being inherently distributed and collaborative in nature present a plurality of attack surfaces to malicious entities and hence vulnerable to many potential attacks even indirectly demanding a need in prioritising security. The choice of security implementations depends upon the currently understood threats, future possible threat vectors, and the dependencies between systems. Executing these choices while contemplating the financial aspects is exceptionally difficult. It is thus critical to have a perceptible decision support framework for better security decision-making. This thesis studies the strategic nature of the interaction between the Telecoms operators and attackers utilising game theory to understand their strategic decision-making characteristics strengthening security decisions.

To understand the security investment decision-making criteria of operators, this thesis utilises static security investment games. Through these games, we study the effects of security investment decision of an operator on other operators' behaviour. We determine conditions supporting the security investment decisions and propose strategic recommendations supplementing the dependency conditions.

We then study attackers' behaviour considering them with strategic incentives in contrary to their strictly-bounded rationality in traditional game-theoretic modelling approaches. We utilise a behavioural approach and design a decision-flow model capturing the choices of attackers in the attack process. An outcome of this work is a generalised attack framework. Moreover, using this framework, we derive attack strategies optimising attackers' effort. Through this work, we are probing the foundations for drawing inferences about attackers' strategic characteristics from a cybersecurity perspective.

Keywords Telecommunications, Game Theory, Operators, Attackers, Cybersecurity, Security Games, Strategies, Decision-making Behaviour, Economics, Deceit Games, Security Investment Games, Static Games

Acknowledgements

I possibly could not have accomplished the completion of the thesis without the encouragement and support of a number of people. I am grateful to each one of you.

The research for this Master's thesis was done at the Security Research Team of Nokia Bell Labs, Espoo, Finland. I am grateful to the team members of the Security Research Team.

I owe deep gratitude to Dr Ian Oliver - my advisor who motivated me to strategically explore areas of research largely unknown to me. He introduced me to the area of Game Theory and have supported me immensely. He gave me the space to manoeuvre with ideas and insights, and the freedom to conceptualise my content at a steady pace with deep patience and persistence.

I express my deepest gratitude to my academic supervisor, Professor Marko Nieminen, who has been extremely open and supportive of my ideas and concepts during the whole period of research. I thank him for his valuable insights and suggestions.

Both, Ian and Marko, have been very generous in every possible way, providing constructive feedback, inspiring me to put in my best effort, and of course with innumerable hours of mentoring from their stretched schedules. Their insights, attention to detail, vision, openness to using different literature to bring together a cross-disciplinary idea into text has had a profound impact on my overall development. In many ways, they have readied me to take the plunge into the next level of research.

Amongst others who I wish to acknowledge for their support - both academically and morally is my manager, Gabriel Waller. Thank you for giving me a learning opportunity to work with the Security Research Team. I acknowledge and thank members of the team, particularly Dr Yoan Miche, Dr Silke Holtmanns, Leo Hippelainen and Aapo Kalliola for being so supportive and understanding, sharing their experiences and expertise encouraging me to learn and gain new perspectives. Gabriela, Borger and Isha, my charming friends and co-workers whose company I enjoy a lot. I have always found this dynamic team friendly, accepting and inspiring to learn more.

I sincerely thank Professor John Howse and Dr Gem Stapleton from University of Brighton for encouraging me to explore new research disciplines. Many thanks to Ingrid Schembri, EIT Digital Finland and Mika P. Nieminen, Department of Computer Science, Aalto University for their advice and support.

My special thanks to all my friends who I met during my Masters. Thank you, Benjamin and Viet for being my 'go-to friends' over the last year for international travels, hiking trips, sports, movie nights and research discussions. So good to have found you as friends.

Loads of love and gratitude to Mumma for being there for me at all times. Grateful to Bapa, Maa, Disha, Chunu, Arnav and all others for believing in me and in the work that I wish to do.

Contents

List of Original Publications

The listed below original publications, referred as 'paper a' and 'paper b', are the resultant of the research performed during this thesis. The 'paper a' [1] contributes to the essence of Chapter 5, which aims at understanding the factors influencing the strategic behaviour of attackers from a cybersecurity perspective.

The second paper, 'paper b' [2], does not contribute to the core idea of this thesis but is an extension of the intrinsic perception of 'paper a' towards a real application (discussed in Chapter 6).

[paper a] Sakshyam Panda, Ian Oliver, and Silke Holtmanns, "Behavioural modelling of attackers' choices," in The Annual European Safety and Reliability Conference (ESREL 2018), 2018, accepted for publication.

[paper b] Ian Oliver, Sakshyam Panda, Ke Wang, and Aapo Kalliola, "Modelling NFV Concepts with Ontologies," in the 21st International Conference on Innovation in Clouds, Internet and Networks (ICIN 2018), 2018, accepted for publication.

Abbreviations and Acronyms

DNS	Domain Name Services
ETSI	European Telecommunications Standard Institute
FCC	Federal Communications Commission
GSMA	Global System for Mobile Communications
HLR	Home Location Register
MME	Mobility Management Entity
MNO	Mobile Network Operator
NEP	Network Equipment Provider
SSG	Stackelberg Security Game

List of Figures

1 Introduction

Our increasing reliance on computer networks and information systems are making them attractive targets for cybercriminals [7]. The recent activities in cyberspace [8, 9] are evidence that security breaches can cause enormous loss to governments, public and private institutions, and the general public in terms of money, privacy, and reputation.

Even though cybersecurity problems have been paid attention to for over two decades, the problems are far from being resolved. In cybersecurity, quantifying the security risks and determining the effectiveness of one's security investment against perceived threats are major challenges. The ability to prevent a breach is defined by one's security investments as well as on the security standards of other interacting entities. This security interdependencies between entities contribute additional complexities in identifying and quantifying the security risks and crafting suited countermeasures [10].

Besides, cyberattackers are becoming more financially oriented [11, 12] with diverse attack strategies displaying unanticipated behaviour [13]. The malicious activities are due to curiosity, or for peer recognition, and are often undecided in terms of ethical legitimacy [14]. [15] states that the motivations behind attacks are shifting from fame and fun towards profits. Conversely, this shift can be used in arguing that the attackers are becoming more rational (predictable) by being financially oriented as by [16, 17].

This shift in the motives could be a reason behind the increasing frequencies of cybersecurity encounters [18] indicating necessity in investing in security. Results of surveys [19, 20] have stated that users are inclined towards preventing attacks and minimizing the damages from security breaches. However, despite the availability of wide ranges of consumer security technologies, investment in security is elusive [21] providing opportunities for adversaries to exploit.

This uncertain behaviour of users in terms of security and exploitation creates a need for studying and analysing users behaviour to understand their possible interactions, intentions and decision making criteria. Nonetheless, the possibilities of utilising illegitimate methods stimulate advanced strategies and new classes of attacks demanding a comprehensive understanding of attackers' behaviour. This would enable us in anticipating their intentions and priorities.

The telecommunication domain, being the backbone of cyberspace, faces identical challenges with multi-dimensional interactions among multiple stakeholders. These interactions involve diverse motives and intents requiring them to behave strategically to manage demanding situations [22]. This thesis focuses on studying such strategic decision-making behaviour of Telecommunications operators and attackers from a cybersecurity perspective utilising game theory.

Game theory [23] is a mathematical modelling tool for studying multi-person decision-

making scenarios. It has been widely utilised in studying various facets of security [4, 24] and privacy [25]. It provides means to determine and quantify elements influencing decisions and predicting behaviour [26]. It is extremely useful in formulating complex real-life situations into simplified representations and assessing them based on well-defined goals. The expressibility of game theory has encouraged researchers to exercise its concepts in modelling and evaluating a myriad of security-related situations [27, p. 2].

To understand the strategic characteristics of Telecommunications operators we utilise security investment games. The security investment games involve non-malicious strategic players (operators in our study) deciding on whether to invest or not to invest in security [28]. Through these games, we study the interdependency effects of security investment decisions on operators' behaviour.

The next segment of this thesis focuses on studying the attackers' behaviour. Due to lack of conclusive evidence on the forms of motives and intents behind attacks, most studies have assessed security scenarios with strictly bounded attackers displaying prescribed behaviour [29, p. 336] [30]. However, this assumption of attackers displaying confined behaviour is not ideal; particularly in real-world situations which involve human adversaries [27].

To address this, we utilise a behavioural approach to understand the strategic choices of attackers with an intention to better understand their strategic preferences and predict them. Our approach differs from the existing body of research by modelling adversaries rather than defenders.

More precisely, this thesis bases itself on the hypothesis that attackers behave as rational entities and could have various underlying determinants for an attack. It, therefore, seeks to explore different possible implications behind attackers' displayed behaviour. In simple terms, understand different considerations and reasons behind actions. This reflection logically brings us to the second level of strategising that is expected of the defenders. If attackers could have multiple reasons and motives behind attacks, are defenders equipped with multiple countermeasures - strategies or even a strategic modality to address the multiplicity of determinants moderating attackers' behaviour?

1.1 Problem Statement

Although the research community has extensively focused on studying the importance of security, existing practices lack decent security measures implementation [10]. The major reasons supporting the inefficacy in security adaptation are the lack of adequate incentives for investing in security [31], and the available security information being highly asymmetric - favouring the attackers [28, p. 5]. The attackers need to exploit one vulnerability of a target, whereas the operators have to defend against all possible threat vectors. Furthermore, the possibility of using illegitimate practices

provide attackers with a broader range of breaching options than the operators could determine and prevent a breach.

The key limitations in current research practices are that the approaches are considerably restricted through biases and heuristics and are struggling to incorporate rapidly emerging new classes of attacks [32]. The critical difficulties in modelling adversaries are due to lack of decisive information regarding potential adversaries and the interactions being highly complex and extensive [33]. Furthermore, lack of conclusive data and evidence generation on the forms of motivation and intention behind attacks makes it immensely challenging in understanding and modelling attackers' behaviour.

The security modelling approaches normally operate under the presumption that attackers are strategy-less or strictly bounded displaying restrained behaviour [34]; inconsistent with reality which involves human attackers [27]. A prescribed set of actions for attackers consistent with the threat models confines the applicability of the proposed security solutions.

Besides, taking rationality of attackers into account expands the possibilities where actions could bear latent motives raising concern on the admissibility of existing cybersecurity defence tactics. Above all, admitting that attackers have strategies, which they do [35, 13, 36], implies that defenders need to reassess their investment in security and change how they perceive, defend and react to attackers. The ability to assess with such details would require a perceptible decision support framework with capabilities to decisively predict attackers' behaviour which further depends on the extent of our understanding of intents, incentives and strategic preferences of attackers.

In addition, securing systems and networks with confined resources is a well-known challenge and decision-makers need to follow effective decision-making strategies[37]. Hence, it is a necessity to investigate effective ways and strategies to be able to successfully defend our systems and networks from malicious entities.

1.2 Research Objectives and Questions

The principal objective of this study is to enhance cybersecurity by understanding attackers' behaviour. More specifically, the focus is on understanding the economics behind strategic interactions between Telecoms operators and attackers from a cybersecurity perspective. In particular, this research advocate in exploring the following questions:

Q1. What are the core parameters and how do they influence the security investment decisions of Telecoms operators?

Q2. What factors moderate the strategic priorities of attackers?

This research inquires the stated topics by:

1. applying a game-theoretic approach to understand conditions influencing the security investment decisions of Telecoms operators.
2. applying a behavioural game-theoretic approach to understand the choices of attackers and their strategic decision-making behaviour.
3. representing the abstract behavioural parameters as quantifiable and modellable units.

1.3 Contributions

Contributions from this research are as follows:

1. Investigated conditions influencing security investment decisions of operators in a cooperative and competitive environment, and extended the security dependency model presented by Kunreuther and Heal [38].
2. Proposed financially beneficial strategies for operators in choosing collaborators or partners. Further, discussed the strategic moves for operators in dependency relations against attackers utilising the results of [39].
3. Extended the investigation of security interactions by acknowledging attackers with strategic incentives, contrary to the traditional game-theoretic security modelling approach, and designed a decision model capturing the choices of attackers during the attack process.
4. Introduced a reusable attack framework decomposing the attack process into effort requiring in a successful attack and determined attack strategies optimising the overall effort. This attack framework could be used in categorising attacks as [6] and can be used in extending the model proposed by [40].

1.4 Significance of Research

Even though this study utilises game theory and concentrates on understanding interactions between Telecoms operators and attackers, the ultimate goal of this research is to better understand the preferences and behaviour of attackers. Understanding these would enable us in decisively anticipating their behaviour and fabricating suitable countermeasures strengthening cybersecurity. The attack framework, after being evaluated, could be employed in categorising security encounters and determining the intentions behind attacks.

Additionally, a refined attack model could rightly predict attackers' behaviour with the adequate reasoning for such behaviour. This model could be practised supporting the strategic decision-making against the perceived threat. We believe it is no more confined to the boundaries of cybersecurity and can be applied to the whole class of security scenarios. However, this study is in its preparatory stage and is a step

towards comprehensively understanding the motivation, intention and behavioural characteristics of attackers from a cybersecurity perspective.

1.5 Structure of the Thesis

After this introduction chapter, the next chapter provides a literature review on areas related to this work, followed by a chapter describing the cybersecurity environments analysed in this work. The next two chapter models the behavioural characteristics of Telecommunications operators and attackers utilising the described environments, and then the conclusion chapter. The chart in the figure 1.1 summarises the flow of this thesis.

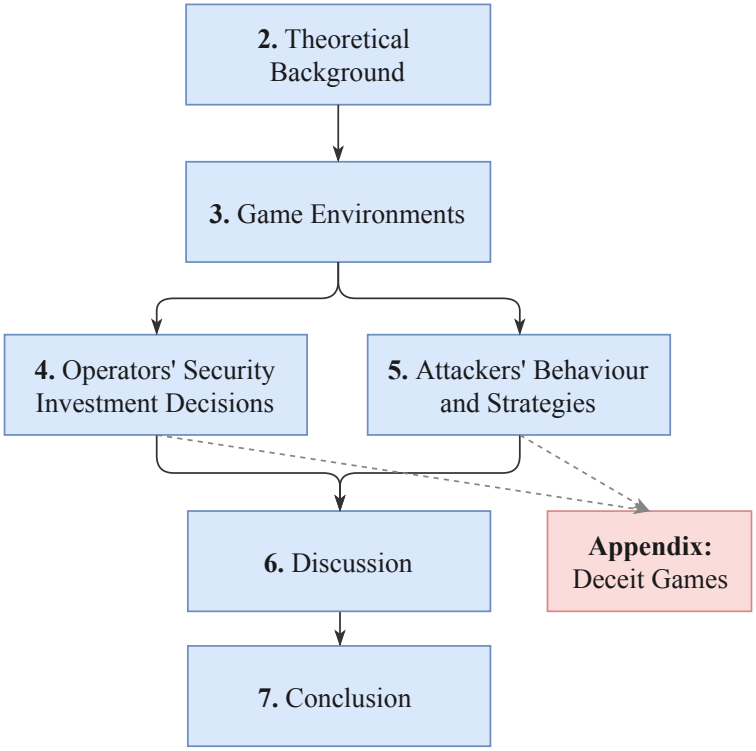

Figure 1.1: Illustrates the structure of this thesis. The boxes represent the chapters appearing in the thesis. A solid arrow connecting two boxes indicates one chapter depends on the other. The dotted arrow indicates the additional work not included as a core idea of the thesis.

Chapter 2
Presents an overview of game theory and relevant game-theoretic concepts, cybersecurity, and a literature review on the application of game theory to cybersecurity.

Chapter 3
Formulates the game environments to study the strategic behaviour of the Telecommunications operators and attackers, classifies the operators and discusses existing

game theory supported practices enhancing operators' security levels, and the research methodology utilised in this work.

Chapter 4
Discusses the first research question, that is to determine the critical parameters influencing the security investment decisions of Telecoms operators. A model capturing the conditions influencing the decisions is discussed, together with our evaluation and strategic recommendations.

Chapter 5
Discusses the second research question, that is understand factors moderating attackers' strategic preferences. A decision-flow model capturing the strategic choices of attackers is illustrated, together with an attack framework. Utilising the framework attack strategies against the operators are proposed.

Chapter 6
Presents the application of the core concepts of this thesis in real life and highlights important future work.

Chapter7
Summarises and concludes this thesis.

2 Conceptual and Theoretical Background

This chapter presents an overview of game theory, cybersecurity and the application of game theory in cybersecurity. We also discuss the significance of game theory in investigating security interactions.

2.1 Basic Game Theory

Game theory, conceptualised by von Neumann and Morgenstern in 1944 [41], is a mathematical modelling tool to analyse multi-person decision-making interaction scenarios. The fundamental assumptions that define the underline theory are that the decision-makers are rational entities (exogenous) seeking well-defined objectives and behave anticipating the rational choices of other decision-makers. The expectations of others' behaviour are based on strategical reasoning [23, p. 1].

The following sections discuss the basics of game theory to aid the understanding of games and game-theoretic concepts. Further specific and formal explanations of these concepts can be found in [42, 23].

2.1.1 Games

A game is a staged environment representing an instance of a strictly bounded interaction between a set of players (participants). The environments are studied to understand the strategic behaviour of the players.

A game includes a set of players, a set of actions available to each player, and resultant payoffs (outcomes) for each action for each player. Moreover, a game could include additional rules affecting the payoffs (eg. order of the play, frequency of the play), and the information available to players.

A number of classifications of games exist, and a game can satisfy characteristics of more than one category. The classification of games relevant to this thesis are listed below

a) *Cooperative Games*
   In cooperative games, players are enforced to cooperate with other players. The cooperative behaviour of players could be the result of agreements imposed by an external entity (e.g. through contract law, standardised policy). These games are often analysed through cooperative game theory with an objective to anticipate decisions forging alliances.

   Contrarily, in non-cooperative games, there are no possibilities of imposed coalitions, and coalitions are self-enforcing. These games are studied using the non-cooperative theory which focuses on individual players rather than the group.

b) *Zero-sum Games*
A game in which each player's intention is contradictory to every other player's intention is defined as a zero-sum game [43]. In these games, the payoffs of a player are counterbalanced by payoffs of his opponents leading to a total outcome of zero. Due to an exact balance between the positive payoffs and the negative payoffs these games are referred as zero-sum games. This definition implies that when a player wins his opponents has to lose. Zero-sum games are also known as strictly competitive games.

On the other hand, a game where the aggregate payoff is greater than or less than zero is defined as a Non-zero sum game. Non-zero sum games can facilitate both cooperation and competition among the players.

c) *Static Games*
A static game is a single-shot game where all the players act simultaneously. In these games, a player chooses a plan of action with no prior knowledge of the plan of action chosen by any other player. This class of games is also referred as simultaneous games.

d) *Dynamic Games*
The games where players interact repeatedly are known as dynamic games. These games are also known as repeated or iterative games. The players in a dynamic game have some information regarding the actions chosen by other players and thus can adapt to demanding situations. These games can be acknowledged as a sequential form of a static game with either a finite or infinite iterations.

e) *Perfect Information Games*
A sequential game in which each player is assumed to be aware of all the past moves of each player is known as a perfect information game. In contrast, a game where at least one player is unaware of the past moves of at least one other player is known as an imperfect information game. By definition, all static games are games with imperfect information [4, p. 4].

f) *Complete Information Games*
In a complete information game, all players are assumed to have knowledge of every other player's strategies and payoffs, but not necessarily their actions. The fact that these games do not acknowledge the actions other players have already taken distinguishes them from the perfect information games. Incomplete information games are those where at least one player is unaware of possible strategies and payoffs of at least one other player. A dynamic game can be of complete or incomplete information [4, p. 5].

2.1.2 Players and Actions

A player is a principal entity of a game with decision-making abilities to choose actions. The players are the central decision makers and are rational with abilities to behave strategically maximising their utilities. A player can represent an individual, a machine, an organisation or a group of individuals within a game.

A player's move in the game is known as an action. It signifies a decision to execute a particular behaviour. The actions available to a player depends on the game environment, which is further defined by the motivation of each player of the game.

2.1.3 Payoffs and Utility Functions

Payoff represents the outcome a player receives on taking a particular action. The payoff for each action of a player is anticipated using a utility function.

The utility function is a mathematical representation which quantifies the payoffs of a player. It is defined by the factors influencing the game environment. These environment variables can alter the payoffs of a player independently or in various combinations. The payoffs are generally in the integer range of -x to x where -x $<$ x. Positive payoff denotes a gain whereas a negative payoff denotes a loss, and the payoff of 0 is neutral with no effects.

2.1.4 Strategies and Equilibria

A strategy is a plan of actions a player can practice during the game to achieve the desired goal. A strategy can either be a 'pure' strategy or a 'mixed' strategy. A pure strategy specifies a unique action to take in a situation. Whereas the mixed strategy refers to a specific plan involving a probability distribution over all the available actions.

These strategies can be further refined based on the resultant payoffs. If a strategy fetches a better payoff than all other available strategies regardless of the opponents' strategies, then it is known as a dominant strategy. A dominant strategy which always gives a better payoff than all other available strategies is a strictly dominant strategy. Whereas, a weakly dominant strategy gives a better payoff in at least one set of the opponents' strategies and as good a payoff as other available strategies for the rest of the opponents' strategies.

A game is assessed with a common assumption that players favour strategies maximising their payoffs. When all the players have made their decision and are reluctant in switching their actions as a change would reduce their payoffs, a steady state solution (equilibrium) of the game is achieved known as the Nash Equilibrium [23, p. 11]. The Nash equilibrium is the most famous solution concept, even though there exist many others [44, p. 9].

2.1.5 Representation of Games

Games can be represented in either Normal-form or Extensive-form depending on the timing of the interaction among players.

In normal-form games, all the players are restricted to choosing actions at the same time. These games are also known as simple games or strategic games and are composed of three elements: a set of players, a set of actions (or pure-strategies) available to each player and a set of payoffs each action will result for each player.

All static games are represented in this form, as a matrix presenting the players, the actions and the payoffs. A dominant fraction of this thesis investigates interaction among players using the normal-form games. The following definition is used to describe a normal-form game:

a) A set of players represented as $P = \{P_1, P_2, \ldots, P_m\}$.

b) Each player $i, i \in P$, has a set of actions A_i, also known as the information set, which consists of the actions available to player i. Thus, player i's action set is $A_i = \{a_{i1}, a_{i2}, \ldots, a_{ik}\}$, where $a_i \in A_i$ and k is the number of actions available to player i.

   Let $a = (a_1, a_2, \ldots, a_i, \ldots, a_n)$ be the list of actions chosen by each player. This list of actions chosen by each player is defined as the outcome of the game. The set a, referred as an outcome set, is a vector denoting that the order of choice of an action is of importance. For example, an outcome is a list of chosen actions where the first action in the list is the action chosen by player 1, the second action chosen by player 2 and so on. In contrast, the action set A has no consequence of ordering.

c) A utility function U defines the payoff of choosing an action for each player by assigning a real number to every outcome of the game. Formally, the utility function can be represented as $U_i(a_j) : V \rightarrow \mathbb{R}$ where a_j is the j^{th} action from the set of available actions A_i for the i^{th} player. V is an abstract representation of the expected outcome.

In extensive-form games, players have the flexibility to move at different times. In addition to the content of a normal-form game, an extensive-form game explicitly contains information available to a player while making a move. These games are generally represented as decisions trees where each vertex represents a point of choice for a player and each edge represents a possible action that a player can take. The final consequence of a game tree is the payoff to each player for each possible outcome. Sequential and dynamic games are usually studied using the extensive-form of representation.

2.2 Cybersecurity

Cybersecurity is the fabrication of countermeasures against perceived threats in a cyber situation. Robinson et al. [45] considered two influential components defining a cyber situation:

1. the actor, one who instantiate the attacks
2. the purpose of an attack

leading to unlawful activities that can potentially cause harm and distress, and are unacceptable in ethical terms. Tekes [46] defines cybercrime as: *"any illegal cyber activity or unlawful computer network action"*.

The intent behind an attack is crucial for any cyber situation. Some intentions behind malicious activities include gaining personal benefit through illegal means (crime [47]), achieving military objectives (warfare [45]), influencing a nation's politics through violence and fear (terrorism [48, 49]), causing psychological distress to others (cyber-bullying [50]), peer recognition, curiosity, and are often undecided in terms of ethical legitimacy [12, 14].

Klimburg and Tirmaa-Klaar [47] define cybersecurity as *"Cybersecurity encompasses the defence against all types of cyber attacks, and includes a number of related issues not normally associated with cyberwarfare or even foreign policy, including critical infrastructure protection, Internet governance, cybercrime, data protection, and others"*. The Figure 2.1 illustrates critical cybersecurity components of a security programme.

The term cybersecurity is often used interchangeably with the term information security due to a substantial overlap between them. Von et al. [50] distinguished cybersecurity from information security by stating that information security is a component of cybersecurity. Cybersecurity extends information security by including non-information based assets such as human factors. As an example cyber-bullying or illegal sharing of movies (piracy) which does not necessarily involve the loss of confidentiality, integrity, or availability of information but results in a direct harm to the well-being of a person. This study acknowledges and adopts cybersecurity as a comprehensive concept, as by most literature [24].

2.3 Application of Game Theory to Cybersecurity

A glance at the current literature shows that game theory has been receiving more and more attention of the research community and is been used to study a variety of security facets. Current research aims at applying game theory to complicated real-life situations supporting better decision-making [17]. The security-related game-theoretic research has focused on developing computational algorithms corresponding to novel problems and have stretched from utilising classic concepts to complex behavioural/cognitive modelling approaches.

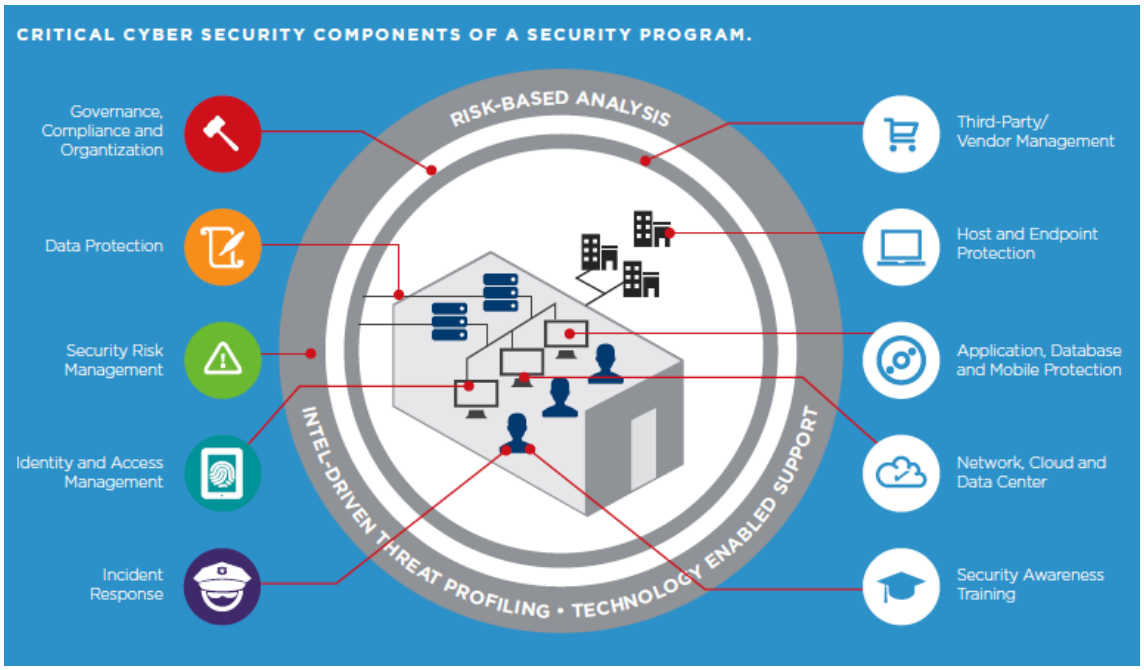

Figure 2.1: Illustrates critical cybersecurity components of a security programme by Mandient adapted from [3]. It displays the key facets of cybersecurity as Risk-based analysis, Intel-driven threat profiling and Technology-enabled support.

Merrick et al. [24] studied information warfare games to identify and model different types of information warfare operations. [26] noted that the strategic decisions in information warfare scenarios are economic in nature. Roy et al. [4] particularly studied game-theoretic solutions enhancing network security and presented a taxonomy for classifying the solutions. This work is extended by [51] through an extensive literature survey.

Manshaei et al. [25] provided a structured and comprehensive overview of game-theoretic models and approaches to address security and privacy problems in computer and communication networks. [22] studied the application of networking games in telecommunication and discussed mathematical challenges and methodologies involved in the application.

The attacker-defender games and interdependent security games are the most popular forms of games used in studying the security interaction scenarios [29]. The interdependent security game involves only defenders and aims at studying the interdependency effects on a player's security investment decisions. Laszka et al. [28] specifically focused on studying the interdependent security games and discussed security inefficiencies together with mechanisms to address the inefficiencies.

The attacker-defender games explicitly involve a malicious entity as a central decision-maker. A significant amount of research work has utilised game theoretic approaches to model interactions between attackers and defenders using Stackelberg framework and the games are known as Stackelberg Security Games (SSGs) [52, 30, 53]. A SSG is a sequential game where the defender acts first, the attacker observes the

defender's action and then act accordingly. This sequential approach is repeated over rounds to analyse repeated interactions between the attacker and the defender.

Grossklags et al. [39] characterised the social optima and Nash equilibria for different classes of defences and attacks using the weakest-link, sum-of-effort, and best-sort security games. They designed the weakest-target game "where the attacker will always be able to compromise the entity (or entities) with the lowest protection level but will leave other entities unharmed." By introducing the concept of free-riding (discussed by [54]) to the least protected entity in the weakest-target game of [39], Florencio et al. [36] stated that even though there are many economically profitable targets, profiting from many attacks are extremely difficult, associating the attacks to the economics of attacks [55].

A number of game-theoretic supported deception techniques have been proposed supporting defenders chances of successfully preventing attacks [56, 57]. While [58] have demonstrated how pretending to be a honeypot decreased the amounts of attacks. [59] studied dynamic adaptation of deceiving strategies by online deceivers in computer-aided communications using game theory and [60] has analysed the effects of extent of deception and timing of deception on attacker's decision to attack a computer network.

In modelling approaches bounded rationality has always been a concern [61, p. 1]. Researchers have been applying alternative approaches to address the bounded rationality of adversaries. One of the two approaches includes enhancing the defenders' chances of successfully defending against attacks by utilising robust optimising techniques avoiding adversarial modelling [62, 33, 30]. Whereas, the other alternate approach involves incorporating human decision-making models for computing defence tactics [63].

To address the bounded rational adversaries in repeated SSGs, [64] developed an adaptive behavioural model, SHARP, which considers adversaries' future adaptation in decision-making based on the successes or failures of their past actions. To this, Tambe et al. [65] discussed the challenges in applying game theory for security from computational and behavioural aspects and illustrated examples of successful deployment of game theory derived algorithms in real-life situations.

To understand the behavioural aspects of participants, [40] utilised the mini-max solution to determine parameters influencing the behaviour of attackers, defenders and users. While, [66] focused on understanding and modelling motivations, roles, and conflicting objectives of players using sequential games.

Yang et al. [63] proposed algorithms to devise defence strategies by predicting attackers, decisions. They utilised two fundamental theories of human behaviour, Prospect Theory and Quantal Response Equilibrium, to predict attackers' behaviour. The algorithms were evaluated using experimental data from human subjects generated in a simulated security scenario.

2.3.1 Why Game Theory?

Game theory is extremely useful in breaking complex real-life situations into highly abstract representations [23, p. 1]. It is used in analysing what could likely happen in a strategic interaction and justify suitable strategic moves. Moreover, it can be applied to formally describe a wide range of interactions which involves competitive situations (players with opposing interests), cooperative situations (players with aligned interests), and situations with mixed interests (players with neither fully opposing nor fully agreeing).

The generality, precision and expressive nature of game theory [27, p. 2] have advocated researchers to exercise game-theoretic approaches to analyse and motivate complex security decisions relating to real-life security problems [29]. In addition, a key advantage of game theory is to be able to evaluate a large number of possible threat scenarios [67] offering insights and perspectives to assess and address security threats. Other advantages of using game theory are the ability to assess suited actions, with the possible outcomes, against potential threats [4] and anticipate the expected behaviour of players through detailed strategic analysis [26] which considerably strengthens the decision process [68].

2.3.2 Game-theoretic Models

A game-theoretic approach involves at least two strategic players. The players confront each other and strategies are evaluated to achieve the well-defined goals. The strategic interactions involve common as well as conflicting interests and are modelled as non-cooperative or cooperative games. The non-cooperative game models focus on possible actions of individual players whereas the possible joint actions of the group of players are studies using cooperative game models.

The Figure 2.2 illustrates the basic classification of game models in game theory. The non-cooperative games are sub-categorised as static games and dynamic games, which could be further grouped with regards to complete and/or perfect information.

We utilise two players, non-cooperative static games to study the decision-making behaviour of operators and attackers. As such, this thesis does not cover cooperative games and non-cooperative dynamic games.

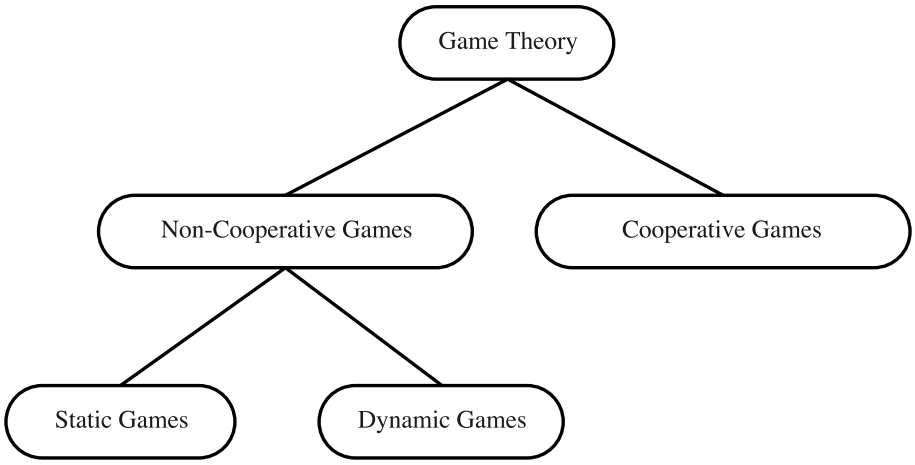

Figure 2.2: Basic Classification of Game Models adapted from [4]. Based on the conflicting or aligned interests of the players, the games are modelled as Non-cooperative or Cooperative games.

2.4 Summary

In this chapter, we have presented the basic concepts of game theory, cybersecurity and the application of game theory to cybersecurity. Further, we have discussed the reasons behind utilising game theory for modelling security interactions. In the last section, we looked into types of game-theoretic modelling approaches. In this thesis, we utilise the non-cooperative modelling approach for analysing the game environments discussed in the next chapter.

3 Games Environment and Research Method

This chapter formulates the game environment used in studying the strategic interactions of attackers and operators. Furthermore, we describe the research methodology utilised in this research, how this research is extending the existing state-of-the-art, and present the existing methods for improving the security standards of operators.

3.1 Players Categorisation

The telecommunications domain involves several players, as introduced by Clemm [69], such as the Network Equipment Provider (NEP), software vendors and Mobile Network Operators (MNO). The NPE sells hardware like base stations, storage resources and other networking resources. The software vendors provide corresponding software to run on the networking resources. The MNO builds the network and provides services through the network like firewall, Mobility Management Entity (MME), Home Location Register (HLR), Domain Name Services (DNS), computation, and caching. In the rest of this report, only the MNOs are considered and are referred as operators. The Figure 3.1 illustrates targeted malware detections in EU nations between January and September 2016.

The interacting participants in the telecommunications domain can be broadly categorised into segments based on their characteristics such as roles, offerings, objectives, or on a combination of these. These participants, known as players, are the central decision makers. The players are categorised as operators (defenders), attackers and policy-makers.

1. *Operators*

   An operator is a defensive player aiming at successfully defending against malicious attempts. Operators have to balance their security-related investments against the security risks. Operators can have common as well as conflicting interests. The examples of operators are Elisa, Telia, Sonera, Orange, Deutsche Telekom and Vodafone. The operators set is represented as **O** and is a set of n players.

   $\mathbf{O} = \{o_1, o_2, \ldots, o_n\}$

2. *Attacker*

   An attacker is an offensive player aiming to compromise the target by attacking. They represent individuals or group with malicious intent causing discomfort to others. Attackers intent to breach their targets by paralysing, deteriorating, destroying, interrupting and deceiving [70] to acquire personal, sensitive, and valuable data. Acquiring others' data, attackers cause social, economic, and psychological discomfort [50]. The attackers set is represented as **Atk** and is a set of n players.

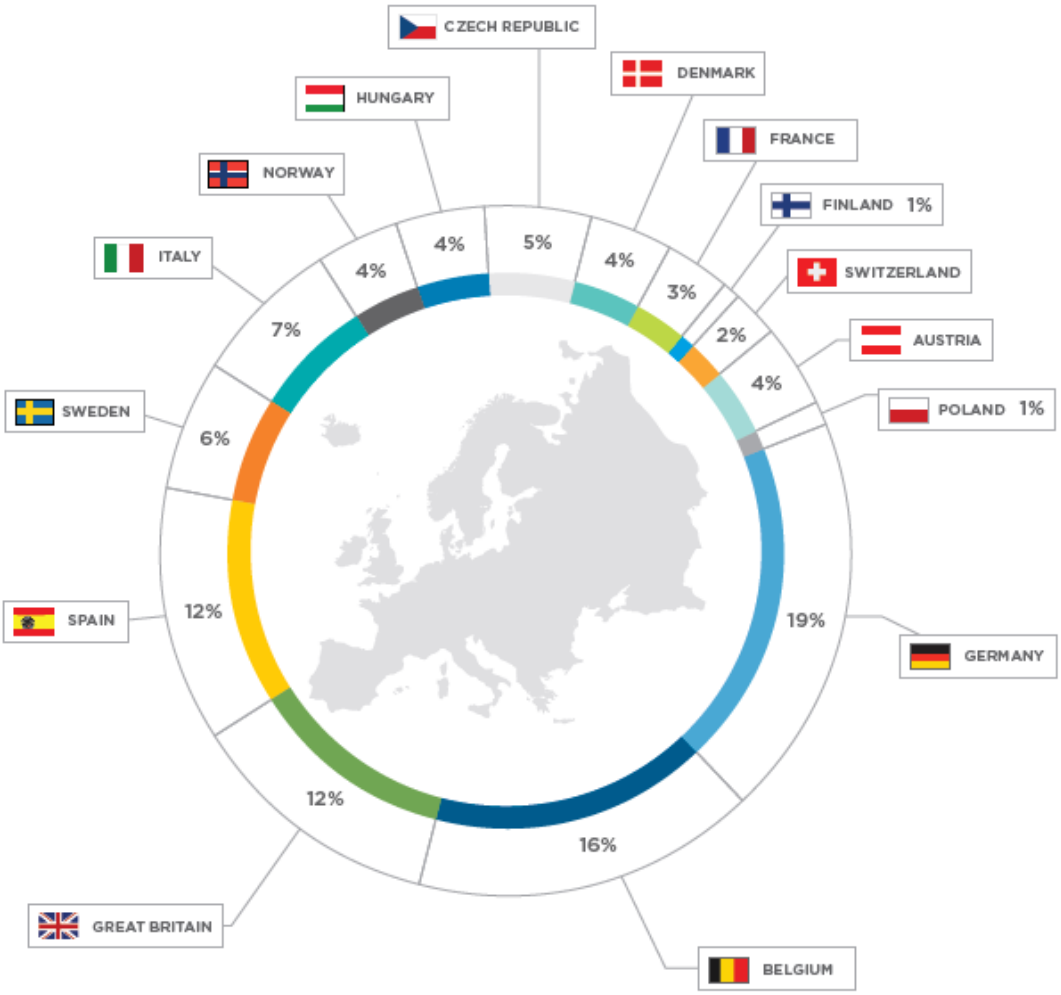

Figure 3.1: Illustrates targeted malware detections from January to September 2016 from all EU nations except Turkey and Russia adapted from [5]. It has also been noted that in 2016 hackers mostly targeted manufacturing, financial, telecom industries and governments in Germany, Great Britain, Belgium, Spain, Denmark, Sweden, Norway and Finland.

$$\mathbf{Atk} = \{atk_1, atk_2, \ldots, atk_n\}$$

3. *Policy-maker*

   Policy-makers are external influencers who set policies and laws. For example standardisation bodies such as European Telecommunications Standards Institute (ETSI), Global System for Mobile Communications (GSMA), Federal Communications Commission(FCC) and other government organisations. However, studying the policy-makers is beyond the scope of this report.

3.2 Attacker-Defender Games

An attacker-defender game involves at least a defensive player and an offensive player. Large varieties of security-related topics are studied using the static, two-players attacker-defender games [29, p. 337].

The repeated version of the security games are popularly studied using the Stackelberg framework and the games are known as Stackelberg Security Games [52, 53]. However, this study is confined to the static security games and does not cover the repeated security games. Furthermore, neither the security technologies on their capabilities to defend specific attacks nor the attacks based on their severity and classes are discussed in this thesis.

We define a security game as a static game between the operator and the attacker capturing the strategic interactions between them. An operator's goal is to maximise his chances of successfully defending against perceived attacks besides optimising the security investment cost. Whereas, the goal of the attacker is to successfully compromise a target while optimising the investment of resources. We study in Chapter 5 the interactions between attackers and operators.

3.3 Security Investment Games

A security investment game is a sub-game of a security game, played among operators. It represents strategically interacting non-malicious operators who can choose whether to invest or not to invest in security leading to a complete protected or unprotected state. We consider that the external threat is persistent and contagious.

An operator's goal is to maximise his chances of successfully defending against attempted attacks while minimising his security investment costs. Together with preserving his system's integrity, an operator should also make strategically optimal decisions for tackling competition.

On the nature of interaction among the operators, an operator's risk depends on his security investment decision as well as on the investment decision of some or every other operator in the interacting network. In chapter 4 we study bot cooperating and competing interactions between operators.

3.3.1 Types of Operators

In this section, we categorise operators on their capabilities for providing services as either an independent or a dependent operator. The Figure 3.2 illustrates the classification of operators.

The *independent operators* are ones with adequate resources to satisfy customers' demands without external dependencies. They, being self-capable of providing services, have the abilities to willingly take decisions. Whereas, the *dependent*

operators are ones with limited resources and rely on external collaborations for catering services. A dependent operator is further grouped, based on the degree of collaboration, as either a cooperating or coordinating operator.

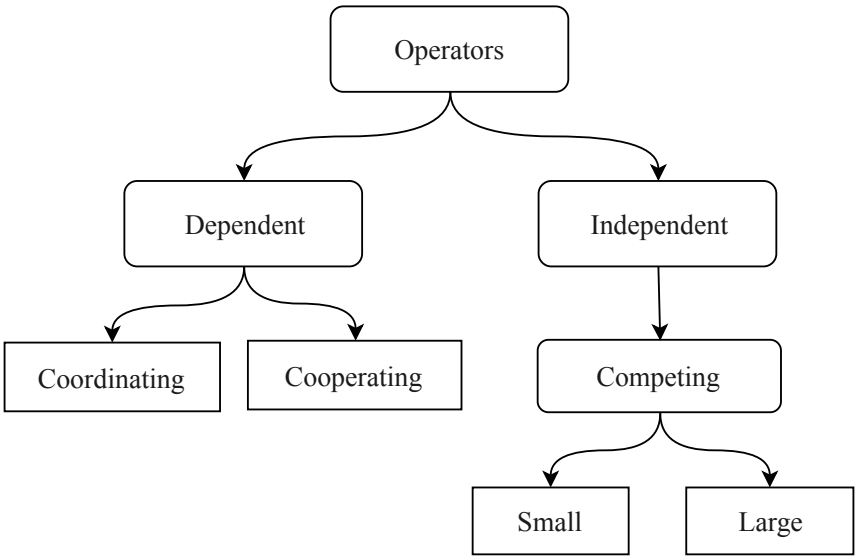

Figure 3.2: Illustrates the types of operators categorised on their capabilities for providing services. Dependent operators are ones with limited resources and have to rely on others for providing services while the independent operators are self-capable of providing services.

The *cooperating operators* represent an association of operators sharing resources; for example, an operator relying on others' infrastructural resources for providing services.

The *coordinating operators* are a subset of cooperating operators with agreements on only demonstrating specific responsibilities (e.g. implementing/investing in an agreed security technology) rather than sharing resources as described in [38].

The *competing operators* are independent operators and lack motivation for external collaborations.

As such, this report considers cooperating and competing operators as extensive units, and it does not cover interactions of further concentrated groups of operators. In the remainder of this thesis, cooperating and competing operators are attributed to as dependent and independent operators respectively.

3.3.2 Operators' Choices and Decision Space

In multiple self-interested player[1] scenarios, the choice of an action by a player influences the decision of other players. The effect of a player's action on other

[1] a self-interested player prefers a specific state of the world and acts accordingly to achieve the state [44, p. 1]

players is referred to as an externality [28]. These are captured as a cost to the player, but often cannot be fully compensated [29].

The externalities introduced due to investment in security influence operators' behaviour. An operator's decision can nudge a positive or a negative effect on other operators. In a positive externality, an operator's security investment decision benefits himself as well as other operators. This type of externality is typically exhibited in information security defences [28, p. 4]. Conversely, a negative externality inflicts counteractive effects on other players. These effects are studies through interactions across the categories of operators.

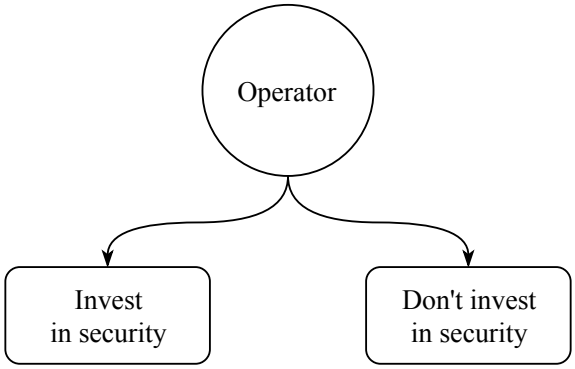

Figure 3.3: Illustrates the decision space of operators. For simplicity, the decision space only includes the choice of investing or not investing in security. Investment in security fetches complete protection against direct as well as indirect threats.

The ultimate choice of an operator in a security investment game is to decide whether to invest or not to invest in security technology. The Figure 3.3 illustrates the decision space of operators. We consider investment in security as discrete[39, 38, 71], providing insulation from all forms and classes of attacks.

In a discrete security investment model, a standard assumption is that when a player invests in security the overall risks is always zero providing perfect (also known as strong or complete) protection. The model proposed by Lelarge and Bolot [71] and the second class of problems in [72] assumed security investment leading to perfect protection.

3.3.3 Practices Improving Operators' Security Levels

The investment in security will positively enhance the chances of successfully defending against a range of attacks. However, the improvement in operators' capabilities to prevent attacks does not necessarily demand an increased security investment, rather can be achieved through additional practices. This section discusses some proposed mechanisms to enhance the level of security.

1. *Insurance*

   A means of enhancing the security levels is by sharing the risks. The risk-sharing reduces the chances of critical loss, and from the information security context, this is known as Cyberinsurance [28, p. 27].

   Recent research has been extensively studying cyber insurance. Insurance is a critical incentive enforcing players to invest in self-protection enhancing security [73]. However, the major issues with insurance are that it intensifies the adverse effects of externalities and discourages investment in security [38, 72].

   In contrary, Hayel and Zhu [74] proposed that implementing a robust cyber insurance policy can reduce the number of successful cyber attacks. The price of the insurance, coverage of the insurance, and the intensity of the attack defines the characteristics of the optimal insurance policy. It is noted that the optimal insurance policy advocate users in adopting suitable protection mechanisms and mitigating the risks. Further, the magnitude of loss, in case of successful security breach, can be limited by investing in protection such as a firewall, or in self-insurance such as provisioning backups [39].

2. *Liability, Bonuses and Penalties*

   Varian [54] proposed a way of achieving the socially optimal levels of investment by introducing the optimal penalty to the player with the lowest cost of reducing the probabilities of a successful security breach. Here, the socially optimal level refers to the Nash equilibrium. It is stated that the penalty should be equal to the total losses of other players.

   Sun et al. [75] introduced a penalty parameter to achieve the optimal level of security investment when reducing the investment cost is a constraint. The penalty parameter induces additional cost to the player failing to meet the socially optimal level (Nash equilibrium). It is noted that the optimal level of investment can be achieved by moderating the penalty value.

   Kunreuther and Heal [38] discussed that the public sector could ensure appropriate security levels by introducing a fine to players not investing in security, or providing players who have invested in security a subsidy encouraging better security.

3. *Regulations*

   Jiang et al. [76] introduced a social planner to monitor the optimum security levels in a competitive environment. The responsibility of the social planner is to ensure that each player invests at least the minimum required to achieve the socially optimal level. In addition, when a player fails to meet the requirements, he has to bear the total cost incurred by others due to his deviation.

   [38] proposed that third-party inspections with insurance can considerably

reduce the risk. Such management-based regulatory strategy can be used by the public sector in partnerships with the private sector, as a third party, to enforce regulations ensuring better security.

4. *Coordination and Cooperation*

   [38] discussed two decentralised coordinating mechanisms to enhance security levels in the context of airline security. The first mechanism proposed that an association of players could coordinate requiring every member to follow specific rules and regulations, including the adoption of specific security measures. Further, the association could decline business with non-members and players not satisfying the requirement. The second mechanism stated that players who have invested in security could announce publicly that they will not support business with players not adhering to certain security standards. This strategy might encourage defaulters to invest in security.

5. *Sharing of Security Information*

   Information sharing can enable in improving the socially optimal level of protection. Gordon et al. [77] stated that information sharing does not affect the levels of security, rather it assists in achieving the same level of security at a lower cost. It is noted that when players share information each tend to spend less on security that they would have invested without sharing information.

6. *Deception*

   Use of deception as a defence mechanism is a common practice in computer security [78]. The act of deception has been deliberately used to mislead hackers into predicted path aiding computer security [78, 79].

   One of the widely proposed methods of deception is the use of honeypots as camouflage for deceiving the attackers [56, 57, 80]. Beside honeypots, Yuill [78] have proposed methods for deceptive hiding by defeating the processes adversaries implement to discover hidden things. [58] demonstrated how pretending to be a honeypot decreased the amounts of attacks.

   In [39], the weakest player might be a strategic move to divert the attention of the attacker knowing that they will most probably attack the weakest link. Thus for the weakest player in the dependency chain, it might be economically beneficial to invest in self-insurance rather than investing in security as it is most likely that he is going to be attacked.

3.4 Research Methodology

In this thesis, we use a qualitative research methodology supported by existing literature. To precisely understand the strategic behaviour of operators in relation to security-related investments, we build our work (Chapter 4) on an existing research [38]. During this inductive process, our critical observation was that this field lacks extensive studies on attackers. To extend the facet, we utilise a novel approach to study the attackers' behaviour from a cybersecurity perspective (Chapter 5).

The security investment model captures the strategic decision-making behaviour of Telecoms operators (in Chapter 4) is a sub-class of the model proposed by Kunreuther and Heal [38]. They investigated the incentives behind security investment decisions in interdependency conditions where a degree of uncertainty from the direct and indirect risks affect the investment decisions.

The risk of being attacked is known as a direct risk, while the risk induced by another interacting player is the indirect/propagation risk. They studied the interdependent security investment games with two players and more than two players. The uncertainty of propagation risk from another player introduced ambiguity in investment decisions leading to an indeterminate solution for the games.

We assess a two-players security investment games acknowledging a positive indirect risk from other interacting operators. Together with the dependency situation, we extend the analysis to games played with strictly competing operators and when only a single-operator is depending on the other. Admitting an indirect risk for sure, rather than a probability, leads to a steady-state solution in the games. Moreover, it decreases the uncertainty towards investing in security. In particular, operators are more motivated to invest in security resulting in improved security levels.

The security games, in general, have been studied considering strictly bounded attackers presenting limited insights into their strategic preferences and behaviour. Besides technical aspects, very few works have shown interest in understanding behavioural and psychosocial aspects of attackers [40, 66].

Kasumastuti et al. [40] studied cyber attackers, defenders, and users using behavioural games with an intention to capture key parameters moderating their interactions. They analysed subgames of a three players game to study technological and psychosocial aspects of participants and proposed solutions using the mini-max rule. Besides, attacking and not attacking a target, the attackers have an additional option of not attacking and investing resources to enhance their capabilities strengthening future attacks.

We investigate security interactions acknowledging attackers as rational entities with strategies incentives. Our work studies attackers with extended strategies, rather than only attacking or not attacking, with an intention to understand their behaviour. Furthermore, we introduce a decision-flow model capturing the attack process from attackers' perspective. We envisage that utilising a decision-flow model, we can learn factors inducing specific behaviour and intuitively reason about a displayed

behaviour. Although the framework is established on assumptions, it facilitates a way of assessing security interactions from attackers' perspective and assist in understanding attackers' behaviour.

3.5 Summary

In this chapter, we defined the game environments as security games involving attackers and operators, and security investment games between operators. We then categorised operators as dependent and independent on their capabilities to provide services. Furthermore, we discussed mechanisms to improve operators' security levels. The last section described the research methodology utilised in this thesis and how this study is extending the current state-of-the-art.

The next chapter studies the security investment decisions of operators and their interdependencies utilising the categories of operators presented in this chapter.

4 Operators' Security Investment Decisions

This chapter focuses on understanding the strategic behaviour of operators with respect to security-related investments. We analyse the interactions between operators using security investment games capturing conditions influencing investment decisions. These particular games demonstrate the dependency effects on the operator's decision-making abilities. We then discuss how these dependency conditions can strategically aid the operators against attackers.

4.1 Payoff Structure

At any point of choice, an operator has to decide between investing or not investing in security. The choice of action defines the state of the operator as secure (complete protection) - if invested, or unprotected - if did not invest in security. An operator with protection will positively defend an attempted attack, whereas an attack will positively compromise an operator without protection. An attack is acknowledged as contagious and can transmit from one operator to other collaborators.

The payoff structure is determined by

- r is the available expendable resources for an operator to invest without involving any expenditure and loses,
- c is the cost of investment in security,
- l is the loss to an operator when it's system is compromised and
- l' represents the loss imposed by another operator.

The following sections evaluate the interactions between independent operators, followed by dependent operators utilising this payoff structure for the security investment games. In the payoffs matrices, the first value of a cell represents the payoff for the row player and the second value for the column player. For simplicity in evaluation, we consider r, c, l and l' to be scalar in nature.

4.2 Games with Independent Operators

The operators have to manage competition among other operators as well as with entities providing similar services, such as [81] which demonstrates direct competition for multimedia services between operators, and cable and satellite Pay-TV providers.

The following game explores a strictly competitive scenario between two independent operators (refer to the types of operators in section 3.3.1). An operator's investment in security can affect other competing operators, such as an operator with protection might be a less attractive target for the attacker and the attacker might prefer

targeting other competing operators [35].

		o_2: Invest	o_2: Don't invest
o_1	Invest	$r - c$, $r - c$	$r - c$, $r - l - l'$
	Don't invest	$r - l - l'$, $r - c$	$r - l - l'$, $r - l - l'$

Figure 4.1: Illustrates the payoff matrix for the security investment game involving independent operators. It presents the scenario where operators are strictly competing against each other.

The Figure 4.1 presents the payoff matrix for the security investment game between independent operators. From the payoff matrix, if both the operators invested in security, then each has to bear the cost of investment c which would provide them complete protection. If operator o_1 invested and operator o_2 does not invest (top-right chamber), then operator o_1 has to incur the cost of investment while operator o_2 has to bear the loss of direct breach and the loss of induced risk of breach. The lower left chamber contains the payoffs in the reverse situation. If neither operators invest in security, then both have to bear the loss of direct breach and loss of induced risk of breach.

For an operator to invest in security, the decision of investing has to be a dominant strategy. From the payoff matrix, the choice of investing in security to be a dominant strategy, it must be

$$r - c > r - l - l' \tag{1}$$

Solving the inequality 1, we obtain $c < l + l'$ which states that investment in security will be a dominant strategy for an operator if the cost of investment is less than the combined expected loss (direct and indirect loss). Similarly, if $c > l + l'$, then neither of the operators will be motivated towards investing in security.

Apart from the pure strategies, a mixed (randomised) strategy where the operators are indifferent towards their choice of actions can be achieved using the mini-max solutions. Under uncertain conditions, operators' best response would be a strategy maximising their payoff and minimising opponents' payoffs. To achieve the optimal strategy, operators must mix their choice of actions such that their opponents have no prefered choice of action.

Assuming there is no prefered choice of action and both operators have decided to randomise their strategy. An operator has decided to invest in security with a probability of p and not to invest in security with $1 - p$. To achieve the optimal strategy, the operator must mix the choices such that the opponent is indifferent

towards any choice of action. To achieve the optimal strategy,

$$\begin{gathered} U_{opponent}(\text{Invest}) = U_{opponent}(\text{Don't invest}) \\ p*(r-c)+(1-p)*(r-c) = p*(r-l-l')+(1-p)*(r-l-l') \\ c = l + l' \end{gathered} \tag{2}$$

In uncertain conditions, the operators are best responding to each other by investing in security an amount $c = l + l'$, in equation 2, equal to the combined expected loss. The induced effect l' is challenging to identify. The condition $c \leq l - l'$ defines investment in security on the possibilities of external influences introducing uncertainty.

The dependency of one's security investment decision on another player's decision reduces the incentives to invest in security [38]. The solution, thus, is undetermined with the possibility of the game terminating at either of the two Nash equilibria - when both operators invest (Invest, Invest) or when both operators do not invest (Don't invest, Don't invest). The independent operator invests in security expecting complete protection. In contrast, such external influences introduce additional contingency in the decision-making lessening incentives for investing in security.

4.3 Games with Dependent Operators

The telecom operators have to manage strategic alliances, partnerships, and fierce competition. For an operator to penetrate a new market, a known economically beneficent strategy is to form coalitions [82]. An individual operator cannot meet the financial and non-financial (e.g. competition) requirements of the new market. The collaborations facilitate sharing of resources complementing each other's requirements.

For example, the merging between Vodafone (UK) and Hutchison Essar (India) in 2007 [83] which paved way for Vodafone to enter the Indian market and for Hutchison Essar to expand their services in Europe. The pan-European strategic alliance between Swedish Telia, Dutch KPN, Swiss Telecom and Spanish Telefonica to meet new regulations, competition and growing demands of quality telecom services [84].

In such dependency conditions, the actions of an operator not only influences own payoffs but also affect other operators. The success of defending against attempted attacks, therefore, depends on a combined protection level determined by all the interacting players. In the two players games, if none of the operators has protection, every attempted attack will successfully compromise the whole system. We refer to the whole system as a network of systems formed due to shared dependencies among the operators. In contrast, if both the operators have invested in security, every attempted attack will be defended successfully.

The dependency relationship among the operators is indicated by an arrow where the tail representing the depending operator. A darker circle illustrates an operator with

protection in the relationship. The possible scenarios of the two players dependent games are:

4.3.1 Single Operator Dependent Scenario

This section studies the dependency scenarios involving only one operator with protection. The Figure 4.2 presents operator o_1 with protection is dependent on operator o_2 without protection.

When operator o_1 is attacked, having invested in security, he will successfully defend the attempted attack preserving the integrity of the whole system. Here, operator o_2's system remains protected even under attack without investing in security. Besides, being able to maintain the integrity without investing in security is be economically profitable resulting in a positive payoff.

On the contrary, when operator o_2 is attacked, being unprotected, will compromise the whole system. In this case, even if operator o_1 has invested in security will lose its system's integrity. Thus, incurring a larger negative payoff to the operator o_1.

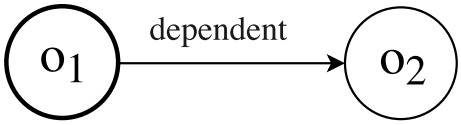

Figure 4.2: Illustrates the situation where an operator with protection is depending on an operator without protection.

The alternate possibility is when operator o_1 without protection is dependent on operator o_2 with protection. The Figure 4.3 illustrates this situation.

When operator o_2 is attacked, he will positively prevent the attempted attack preserving the integrity of the whole system. Here, operator o_1 remains protected even without investing in security acquiring a positive payoff. Whereas, operator o_1 when attacked will compromise only its system rather than the whole system.

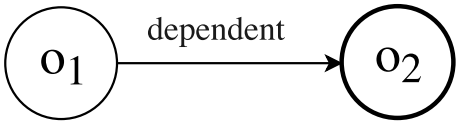

Figure 4.3: Illustrates the alternate situation to Figure 4.5 where an operator without protection is depending on an operator with protection

Acknowledging the choice of investing in security is a decision to be made by operators, the following security investment game is played capturing the dependency effects in a single-operator dependent situation. The Figure 4.4 illustrates the payoff matrix

o_{dnt} \ o_{dng}	Invest	Don't invest
Invest	$r-c$, $r-c$	$r-c-l-l'$, $r-l$
Don't invest	$r-l$, $r-c$	$r-l-l'$, $r-l-l'$

Figure 4.4: Illustrates the payoff matrix for a security investment game with only one operator being dependent on the other.

of the security investment game where the operator o_{dnt} depends on the operator o_{dng}.

The integrity of operator o_{dnt}'s system relies on own security investment decision and the decision of operator o_{dng}. From the payoff matrix in Figure 4.4, if both the operators invested in security, then each has to bear the cost of investment c which would protect them from direct and indirect risks.

If operator o_{dnt} invested and operator o_{dng} does not invest (top-right chamber), then operator o_{dnt} has to incur the cost of investment, loss on breach l and the loss from the risk of breach l' from operator o_{dng} as operator o_{dnt} is dependent on operator o_{dng}. The operator o_{dng} has to only bear the loss l as there is no propagation risk from operator o_{dnt}. This propagation risk l' represents the negative externality in dependency cases.

The payoffs in the lower left chamber are when operator o_{dng} having invested in security will successfully prevent direct as well as indirect attacks. If neither operators invest in security (lower right chamber), then both have to bear the loss of own system being compromised along with the loss due to the risk of contagion from the other operator when attack.

From an economic perspective, it is natural to accommodate a known cost rather than an obscure cost. Thus, the operator o_{dng} has a prefered strategy of investing as the cost of investment is comprehensible rather than not investing which introduces an uncertain loss. For operator o_{dnt} to invest in security, it must be

$$r-c > r-l \quad \text{and} \quad r-c-l-l' > r-l-l' \tag{3}$$

Solving these inequalities in 3, we obtain $c < l$ and $c < 0$. The condition of investing in security with the investment being less than zero, $c < 0$, is unrealistic, as a cost of investment cannot be in the negative, introducing uncertainty. While $c > l$ operator o_{dnt} would favour not to invest in security, which is a natural condition. The ambiguity leads to an undetermined solution and the possibility of the game terminating at either of the two Nash equilibria - when both operators invest (Invest, Invest) or when both operators do not invest (Don't invest, Don't invest).

4.3.2 Interdependent Operators Scenario

This section analyses an security interdependency scenario between the operators. The Figure 4.5 represents the interdependency scenario. The operators being interdependent, any successful attack, irrelevant of the target, will compromise the whole system. Based on an operator's security investment decision the payoffs are determined under compromised conditions.

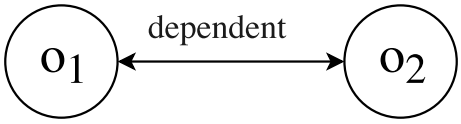

Figure 4.5: Illustrates the situation where operators are interdependent on each other. The interacting operators are protected only under the condition where both invest in security.

The Figure 4.1 presents the payoff matrix for the interdependent security investment game. From the payoff matrix, if both the operators invested in security, then each has to bear the cost of investment c which would provide them complete protection. If operator o_1 invested and operator o_2 does not invest (top-right chamber), then operator o_1 has to incur the cost and the risk of propagation breach l' from operator o_2 since operator o_2 is without protection. The operator o_2 has to only bear the loss l as there is no propagation risk from operator o_1. If neither operators invest in security, then both have to bear the loss of own system being compromised together with the loss due to contagion from the other unprotected operator on an attack.

		o_2: Invest	o_2: Don't invest
o_1	Invest	$r-c$, $r-c$	$r-c-l'$, $r-l$
	Don't invest	$r-l$, $r-c-l'$	$r-l-l'$, $r-l-l'$

Figure 4.6: Illustrates the payoff matrix for a security investment game with interdependent operators.

For a conclusive decision to invest in security, it has to be a dominant strategy. From the payoff matrix in Figure 4.1, the choice of investing in security to be a dominant strategy, it must be

$$r-c > r-l \quad \text{and} \quad r-c-l' > r-l-l' \tag{4}$$

Solving these inequalities in 4 we obtain $c < l$ which states that investment in security will be a dominant strategy for an operator if the cost of investment is less than the

expected loss. Similarly, if $c > l$, then neither of the operators will be motivated towards investing in security.

Using similar calculation as in the games with independent operators section (in section 4.2), to achieve the optimal (mixed) strategy,

$$\begin{gathered} U_{opponent}(\text{Invest}) = U_{opponent}(\text{Don't invest}) \\ p * (r - c) + (1 - p) * (r - c - l') = p * (r - l) + (1 - p) * (r - l - l') \\ c = l \end{gathered} \tag{5}$$

The operators are best responding to each other when the cost of investment in security is equal to the expected loss, from equation 5, leading to a less desired state known as the weak Nash equilibrium. The conditions of investing in security, as a dominant strategy, $c < l$, and as the best response, $c = l$, lead to a steady-state solution in the game, Nash equilibrium, and the game terminates by both operators investing in security (Invest, Invest). Thus, considering a definite propagation risk reduces the uncertainty in the investment decision and motivates operators to invest in security.

This model is a sub-class of the model proposed by Kunreuther and Heal [38], in which the investment decision is influenced by the uncertainty in the direct and indirect loss. The uncertainty of risk introduced by other players reduces the incentives to invest in security. Besides, a tighter bound on the cost of investment, $pl < c < pl - pql'$, defines the security investment decision. Here, p and q are the probabilities of direct and indirect loss respectively.

The constraint of determining the cost of investment on the induced effect is challenging (as seen in the independent operators and single-operator dependency scenarios) and introduces uncertainty in the game, and the solution is undetermined with the possibility of the game terminating at either of the two Nash equilibria - when both operators invest in security or when both operators do not invest in security.

From an economic perspective, the decision of investing in security has always been a concern [85, 72], and the uncertainty in successfully defending while having invested in security magnifies the challenges in making security investment decisions.

The payoff matrices (in Figure 4.4 and 4.6), describes that a dependent operator's investment in security does not ensure protection against malicious activities. Besides the issue of contingency in security investment, dependent operators face the problem of free-riding.

Free-riding [54] is a situation where players avoid investing in security and depend on other players' security efforts to protect themselves. Players free-ride on the positive externality created by the security investment decision of another player. A consequence of free-riding is underinvestment in security [28, p. 4] leading to a lower combined protection level facilitating exploitable opportunities to attackers.

4.4 Strategic Analysis

The games show that the weaker operators are always in danger and investment is security is critical. As investment in security does not assure protection for a dependent operator, it is at least safer to rely on operators with security measures, rather than on operators without security.

It is financially beneficial for weaker operators to not to invest in security and depend on operators with protection, free-riding on the stronger partner. Similarly, it is profitable for stronger operators to not invest in security and only allow operators with protection to be dependent on them. Here, the stronger operators can free-ride on the positive externalities created by security investments of depending operators.

From a strategic perspective, these conditions favour operators to divert the attention of attackers knowing that the attackers will most likely attack the operator with the lowest protection. A strategic move would be using an operator as a decoy to receive all attacks protecting other operators depending on him. Thus, perceiving the most likely point of attack, the operators would be strategically ahead of the attackers.

In particular, it might be economically beneficial for the weakest player in the dependency chain determining that he will be attacked, thus investing in self-insurance rather than in self-protection, as stated in [39]. These strategic results when combined with other aspects of an operator's business, particularly the financial aspects, has influential effects upon budgetary and other economic choices, not to mention the reputation.

Ultimately, investment in security is always at operators' advantage. However, operators should not compete against security, rather security should be a collaborative effort making a breach harder for attackers.

4.5 Summary

In this chapter, we studied the security investment decisions of independent and dependent operators and the interdependencies effects on the decisions. We then demonstrated conditions for investing in security for each category of operators. Further, we presented how these dependencies conditions can be used as strategic moves by the operators in deceiving the attackers.

However, to be able to make better security decisions threat modelling can be used as a foundation for security requirements [86]. Besides, instead of just investing in security with the expectation of successfully defending against attacks, an efficient way could be to understand the attackers preferences, anticipate their strategic behaviour and devise security measures counteracting their attempts. The next chapter essentially centres on studying attackers' behaviour by assessing security interactions from attackers' perspective.

5 Attackers' Behaviour and Strategies

This chapter focuses on understanding the strategic behaviour of attackers. We start by admitting attackers have strategic incentives aiming towards maximising their returns and present a decision model as a cognitive walkthrough capturing the attack process. From this model, we derive a generalised attack framework categorising the total effort required during the attack process. Using the attack framework, we evaluate and optimise attack strategies against the different categories of operators.

5.1 Attackers and Attacks Classifications

Attackers are entities with malicious intentions. Their primary motive is to obtain personal, sensitive, and valuable data by compromising a target such as a telecom operator. Leveraging the acquired data, attackers cause social, financial, and psychological distress [50].

Based on the motives, objectives and threats behind attacks, attackers are categorised into various kinds, as Parker [87] categorised them on the threat levels as a terrorist, criminal, foreign government, foreign military, non-state combatant and business. From a psychological perspective, Rogers [88] classified hackers depending on their expertise (from novice to experienced), areas of interests (software, hardware, etc.) and behavioural patterns.

From an economic perspective, Herley [55] classified attacks as scalable and targeted attacks and pointed that the economics of attacks determines an attack strategy. For a scalable attack such as Distributed Denial-of-Service (DDoS) attack [89], the required effort is disproportional to the number of targets. Whereas, for targeted attacks such as LTE location tracking attacks [90], the effort depends on each target. Thus, suggesting specific attacks must be on targets with higher than average expected value.

Hausken [35] noted that the expected returns of an attack regulate the strategic choices of attackers, as likely as it defines the decision of investing in security for defenders. Although, for a profitable attack, attackers need to differentiate viable from non-viable targets and determine which viable target to attack from the expected returns [91].

[13] classified attack strategies on probable types of attacks such as

- attacks on a single target
- attacks against multiple targets
- consecutive attacks
- random attacks
- attacks involving a combination of intentional and unintentional impacts

- attacks with incomplete information
- attacks with variable resources from a broader literature survey.

However, the barriers in aptly modelling adversaries are due to the lack of credible information on potential adversaries, and the interactions being extremely complicated and extensive [33]. Moreover, speculating the intentions behind attacks from the available security encounter data, which mostly includes security breach data [92] and data from decoys such as honeypots and honeynets [93] is challenging. This problem exaggerates when predicting the human behaviour administering a strictly bounded rationality [94], especially while addressing the human adversaries. Moreover, the difficulty in identifying, confirming and quantifying the intents further limits our understanding of cyber attacks and adversarial behaviour.

We, humans, are bounded rational rather than being perfectly rational [95] due to a myriad of cognitive and situational constraints. Behavioural game theory [61] has been utilised to gain a comprehensive view of the strategic choices of humans.

Behavioural game theory differs from the traditional game theory by utilising "experimental evidence and psychological intuition" [27] to predict human behaviour. From a security perspective, [96, 65, 97] have demonstrated improvement in the predictability of attackers' behaviour by using behavioural/cognitive modelling in repeated security interaction environments. In the following section, we utilise a behavioural approach to capturing the strategic choices of attackers during the attack process with an intention to understand their behaviour.

5.2 Behavioural Analysis

It is economically infeasible for operators, being a deficit of resources, to invest in high standard defences securing each system. They need to devise effective strategies and tactics balancing the cost of security investment against the risks [98]. Similarly, attackers have also limited resources to invest and need to act strategically optimising their investment and maximising their utility [36].

The expected return from attacks moderates their strategic choices; particularly the motivations [35], signifying attackers do have strategic preferences and aim towards maximising their desired gain [55]. Moreover, [99] demonstrates that attacks are results of cooperation among participants which reconfirms that attackers have strategies.

We study attackers' behaviour acknowledging that they have strategic incentives to attain their utilities while minimising their effort during the attack process. This assumption eases the strictly bounded rationality of attackers and facilitates a unique way of analysing the interactions, in contrast to the only choice of attacking and not attacking options utilised in traditional game-theoretic modelling approaches [29, p. 336].

In particular, it facilitates examining diverse attack strategies involving conditions when attackers do not react - ignore or watch the target; diverging from the traditional approach where the attackers follow a prescribed action of invariably attacking the target.

Introducing strategic attackers into the game environments expands the possibilities where an action could bear latent objectives and motives challenging the efficacy of the proposed defence strategies [1]. As an illustration, consider the case of a Distributed Denial-of-service (DDoS) attack [89], where the attacker attempts to prevent an operator from delivering information or services by clogging the network.

A game-theoretic strategy for the operator against a strategy-less attacker would be to invest resources in countering the attack with full capacity to minimise the damage. The attacker being strategy-less, the attack would precisely be an attempt to harm the existing state of the operator. In contrast, for a rational attacker with strategic priorities, the DDoS attack might be merely a probing attack to assess the strength of the operator. It could be a small diversion depleting the operator's resources and flooring conditions to perform a powerful targeted attack.

The Figure 5.1 presents a glimpse of the extended decision space of attackers with a diverse choice of actions. This decision space is on a macro level with no further characterisation of attacks based on the severity of attacks and dependencies between attacks.

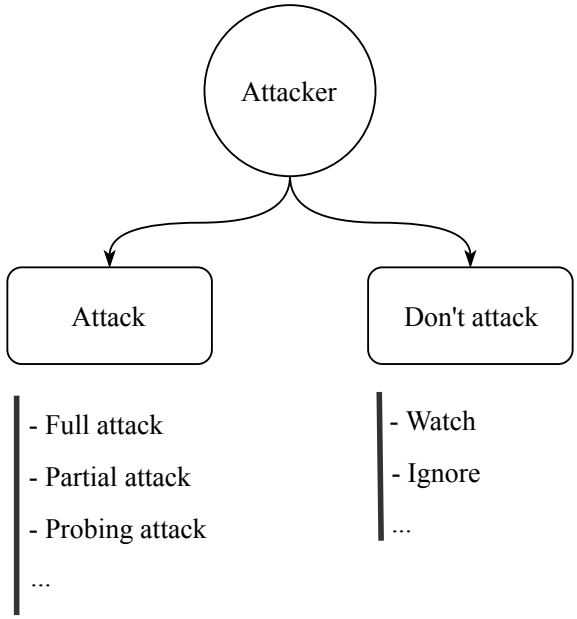

Figure 5.1: Illustrates the decision space of attackers adapted from [1]. It presents an extended choice of actions available to attackers rather than simple attacking or not attacking considered in traditional game-theoretic security modelling approaches.

The choice of not attacking the targeted operator does not necessarily mean that the attacker has simply ignored the target and operators are not under threat. In order

to have a comprehensive understanding of attackers' viewpoint, there is a need to acknowledge possible implications of such behaviour. In simple terms it could be a strategic move of the attacker to not attack and observe operators' reactions (also known as passive attacks [100]). Moreover, attackers could probe the operators with intents to induce specific behaviour.

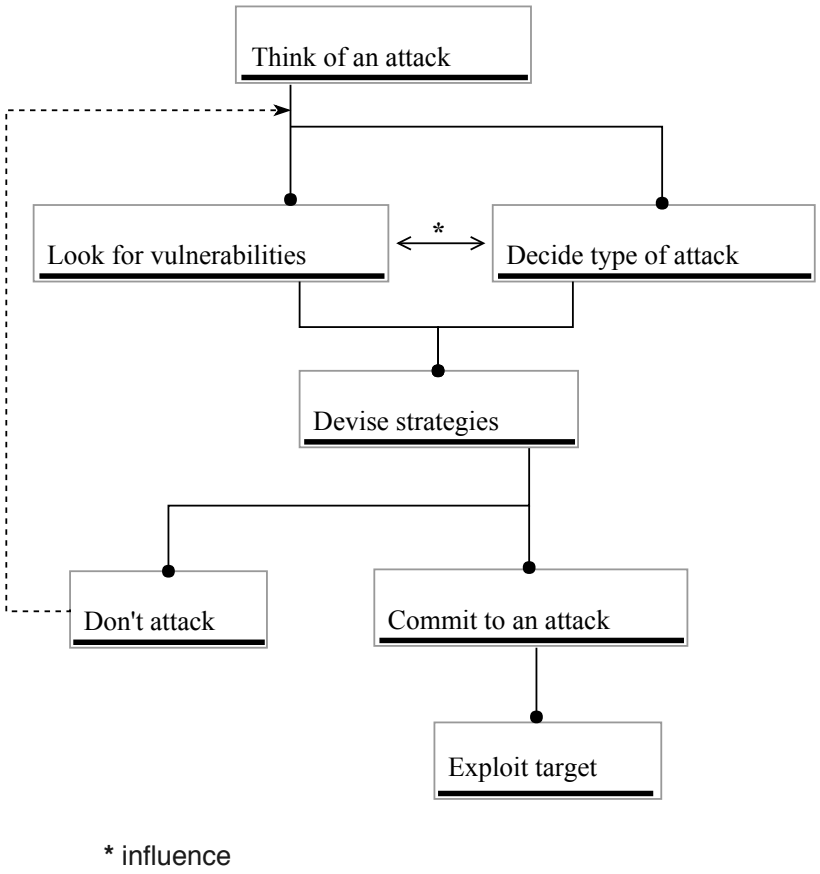

Figure 5.2: Illustrates the decision-flow model of attackers adapted from [1]. It captures the cognitive walkthrough of an attack process from attackers' perspective.

Figure 5.2 presents a decision model capturing the choices of attackers during the attack process. This model represents the cognitive flow of attackers during the attack process. The lowest level of the flow represents the definitive actions which include either attacking or not attacking. These low-level actions are dependent on the higher-order goals. The states become increasingly abstract as we ascend towards the higher levels. These higher order abstract states could be disintegrated further into transitional stages aptly expressing precise interaction scenarios.

The cognitive process initiates from the thought of an attack and terminates on a definitive decision of either attacking or not attacking. The choice for an attack is supported by either searching for vulnerabilities to breach or choosing a specific attack to perform within the attacker's capabilities. There could be numerous other decision-flow paths to select based on the context of an interaction.

The attacker's motive behind an attack latently or precisely influences the choice of intermediate paths. The subsequent steps descending the flow involves determining attack strategies and deciding on whether to attack. The lower level decisions demonstrate specific behaviours [101] and game theory could be used in studying these behaviours [26]. Further, these behaviours could be used to infer the higher order objectives and intentions driving such behaviour [101, p. 2]. An understanding of the intents and motives will support better reasoning for estimating attackers' behaviour and comprehensively predicting their behaviour.

5.3 Attack Framework

The attack process can be characterised, based on the decision model (refer to Figure 5.2), into stages requiring different effort in performing the attack which can be broadly characterised as **Searching effort** and **Breaking-in effort**. The Figure 5.3 displays the attack framework illustrating the effort required in the attack process.

The Searching effort inculcates effort requiring in choosing a target, gathering information regarding the target and scanning vulnerabilities to breach. While Breaking-in effort involves the effort requiring to compromise the target. An expected value from a successful attack can be derived summing all the effort requiring in the attack process. The expected value is a critical determinant moderating attack decisions [55, 28].

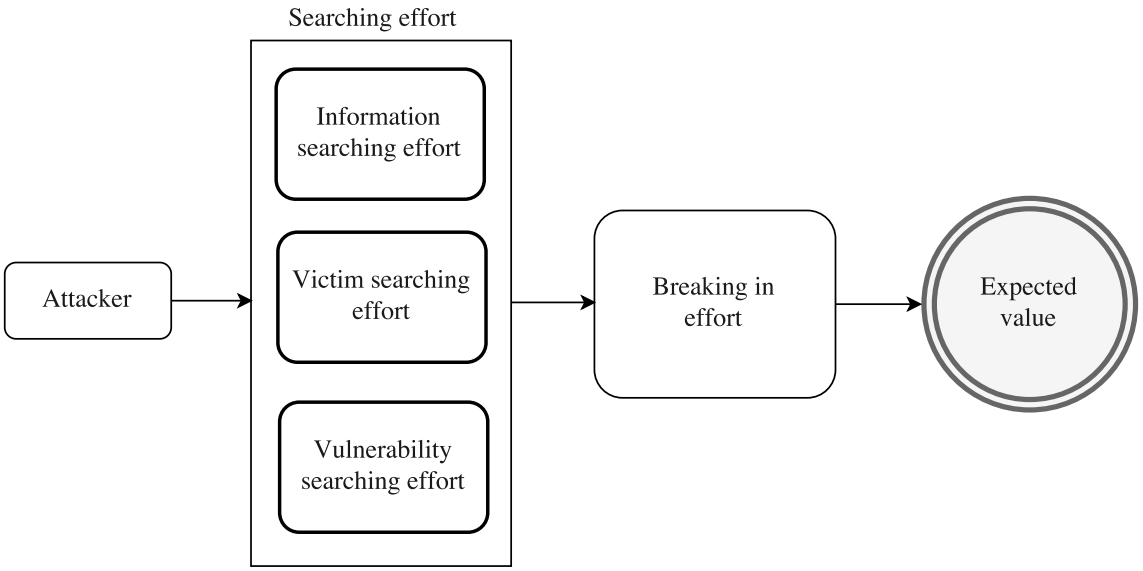

Figure 5.3: Illustrates the attack framework derived from the decision-flow model in Figure 5.2 adapted from [1]. This framework disintegrates the abstract states of the decision-flow model into effort required in the attack process facilitating a way of quantifying and modelling them.

Mapping the decision model, in Figure 5.2, into the attack framework, in Figure 5.3 transforms the abstract states of the decision model into modellable units. These modellable units can be utilised in quantifying the expected utilities of the attackers

unveiling their incentives aiding in an improved understanding of the attackers' decision-making behaviour.

Furthermore, the attack framework facilitates in evaluating and enhancing attack strategies by optimally regulating the overall effort required in compromising a target which further strengths the efficacy of attacks while optimising attackers' effort.

5.4 Optimising Attack Strategies

A crucial factor affecting players' decision is their inability to assess the environment which introduces uncertainty in their decisions [28, p. 35]. Uncertainty due to lack of complete and perfect information against an operator could hamper attackers' decision. For example, attackers might have information about alliances among operators but gaining information regarding an operator's investment in security and on what specific security might be challenging. Due to this the attack process involves a certain degree of uncertainty. However, the attack process eventually converges to a point when the attacker has to choose between attacking or not attacking the target.

The Figure 5.4, illustrates the expected payoffs of an attack against a targeted operator in uncertain conditions. As mentioned earlier, the investment in security is discrete, protecting from all forms and degrees of attacks. The insecure implies a successful breach resulting in a positive payoff for the attacker while the secure represents the alternate. The gray box represents additional conditions on the decision of not attacking the target and exploring these conditions are beyond the scope of this work.

Apart from uncertainty, a critical challenge attackers face is in identifying potential targets such that an attack would yield something [91]. To sustain, it is crucial to distinguish viable from non-viable targets such that an attack is worth performing. Moreover, to gain from an attack, the attacker must decide which operator to attack, successfully compromise the operator, and leverage the accessed resources.

In particular, attacks are not worthwhile if the gain is not at least as good as the cost of performing the attack. As a concrete example, let's consider a telecommunications domain with N operators, among which N_c operators share security dependencies and N_n independent operators compete against security. It is an extremely expensive task for attackers to choose a viable target from such an intertwined mesh of operators. As such, the number of systems under each operator is not included as it magnifies the complexity by many folds. Possible tactics attackers might adopt addressing this situation are

1. randomly choosing a target operator and attempt breaching the operator's defence. This approach demands a substantial searching effort and could include a large breaking-in effort. This adds further uncertainty to as the attacker is doubtful regarding his abilities to successfully compromise the target.

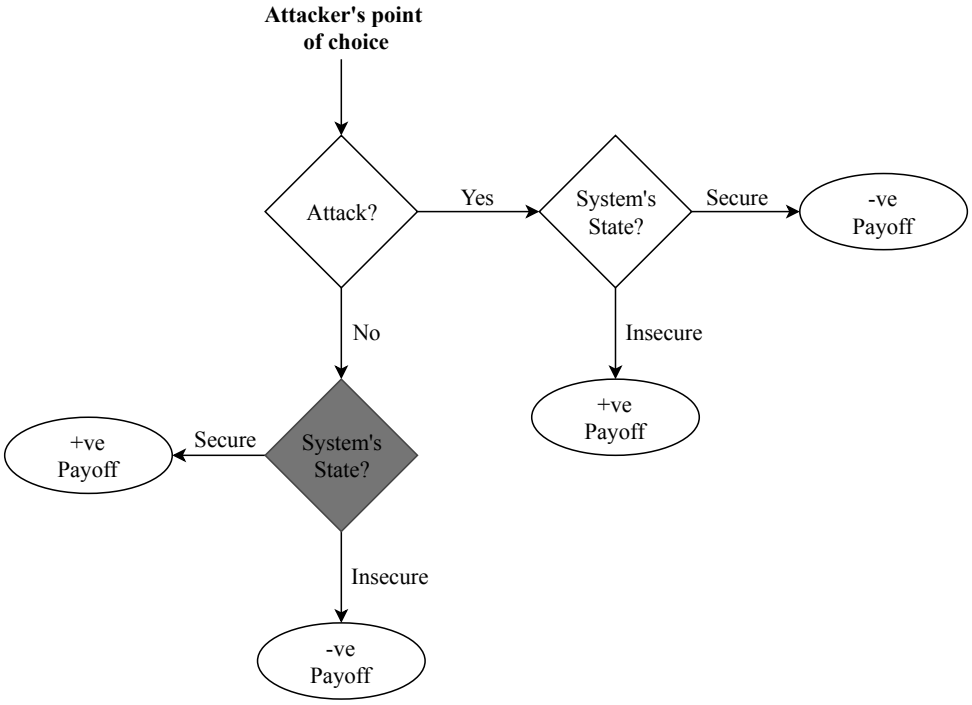

Figure 5.4: Illustrates the expected payoff for the attackers' decision of attacking or not attacking an operator adapted from [1]. Lack of complete and perfect information on a targeted operator introduces uncertainty in attackers' decision process. Here, if the target is protected an attack will fetch a negative payoff else the alternate. The gray box represents additional conditions on the decision of not attacking the target. However, exploring these conditions are beyond the scope of this work.

2. search for a specific vulnerability and then attempt breaching it. This approach would involve a substantial searching effort but a small breaking-in effort, as the attacker can surely exploit the vulnerability. Even though this approach involves high searching effort, chances of successfully compromising the chosen operator are very high.

The expected Utility (U) represents the probable payoff an attacker will receive on successfully compromising a targeted operator. Based on the attack framework in Figure 5.3, the expected Utility for an attack is the difference between the overall cost of performing an attack minus the expected gain from a successful attack and is represented as

$$\begin{aligned} U = cost(&Information\_searching \ + Target\_searching + \\ &Vulnerability\_searching \ + Breaking\_in) - expected\,Value \end{aligned} \tag{6}$$

where from [55],

$$cost(Information\_searching) < cost(Target\_searching)$$

Gathering and sharing of security-related information is one of the key factors improving cybersecurity in both cooperating [102] and non-cooperating [103] environments. Gordon et al. [77] noted that information sharing assists in achieving security at a lower cost while promoting the socially optimal levels of investment. However, it is a known fact that the proposed information by defenders supports attackers in devising attack strategies.

The following analysis illustrates how by utilising commonly available knowledge on operators can assist attackers in planning optimal attack strategies. Utilising the available information reduces the information-searching cost to a static cost C_i rather than a variable cost. However, attackers have to bear the vulnerability-searching costs C_v as a common cost irrelevant to any choice of target. t is the choice of a target from the set of operators.

In a cooperating environment, the state of an operator is not only influenced by his decision but also by other cooperating operators' decisions (refer to chapter 4 for further details). Knowing a set of operators (N_c) are cooperating, the attacker can refine the target-searching scope from N operators to N_c operators, where $N_c < N$, reducing the searching effort to an extent. The expected Utility (U_c) for attacking dependent operators is

$$\begin{aligned} U_c = C_i + cost(Breaking\_in) + \\ C_v \sum cost(Target\_searching) N_{c(t,-t)} \\ - expected\ Value \end{aligned} \tag{7}$$

In a non-cooperating environment, an operator's security investment might encourage competing operators to invest in better security measures. It might, therefore, also increase the likelihood of attacks on competing operators as the attacker will prefer a victim will lower resistance (described in Section 4.2).

Identifying operators are competing would reduce the victim-searching effort considerably, as it is economically beneficial to attack the losing operator. Reduce in victim-searching effort could facilitate attackers in reallocating additional resources for vulnerability-searching, and breaching the target. The expected Utility (U_n) for attacking independent operators is

$$\begin{aligned} U_n = C_i + cost(Breaking\_in) + \\ C_v \sum cost(Target\_searching) N_{n(t,-t)} \\ - expected\ Value \end{aligned} \tag{8}$$

The desired gain G represents the minimum amount of gain the attacker would want from an attack. From an economic perspective, an attacker would prefer the attack that maximises G. That is, from a range of available attack strategies, the attacker

would prefer the strategy that maximises U minus G. This expresses co-existence of several classes of attacks on a point of attack. The expected payoff and the desired gain from an attack would moderate the decisions of the attacker. As

$$\text{decision} \cong \begin{cases} \text{Attack}, & \text{if } U \geq \text{G} \\ \text{Don't attack}, & \text{if } U < \text{G} \end{cases}$$

The attack framework is a reusable design capturing the attack process. It could be utilised in many situations assessing the attack process. In the simplest case, it could be used in categorising attacks based on the effort required (eg: resource, time) to compromise a system, similar to Figure 5.5 which illustrates a threat matrix categorising the malicious actors on their technical capabilities and potential impact they could cause through attacks [2].

The attack framework could also be used in incorporating and extending the existing models such as [40], where the attacker has the option of not attacking and investing resources to enhance his capabilities. This characteristic of attackers could be further extended using the attack framework as an investment made towards improving capabilities refining the searching effort or breaking-in effort, or both. Besides, the attack framework facilitates an additional dimension to classify the attacks.

5.5 Summary

In this chapter, we examined the attackers utilising a behavioural approach. We considered attackers as rational entities and built a decision model capturing the choices of attackers during the attack process. We designed a reusable attack framework from the decision model which disintegrated the effort requiring in the attack process. Utilising this attack framework, we further proposed attack strategies optimising attackers' effort against dependent and independent operators.

[2] Refer to Figure A1 and A2 in Appendix A.1 for further details on the scales

Threat Actors	Verticals								Risk Rankings	
	Financial Services	Retail	Legal	Energy	Healthcare	Tech/ Entertainment	Telecom	Gov't/ Military	NGOs/Civil Society	Capability	Potential Impact
China			X	X	X	X	X	X		Tier 6	Catastrophic
Five Eyes*				X			X	X		Tier 6	Catastrophic
Iran	X			X			X	X		Tier 4	Moderate/ Severe
North Korea	X			X		X	X	X		Tier 4**	Severe
Russia	X		X	X		X	X	X	X	Tier 6	Catastrophic
Disruptive/ Attention-Seeking Actors						X		X		Tier 3	Moderate
Cybercriminals	X	X	X		X	X	X			Tier 4	Severe
Hacktivists	X	X		X		X	X	X	X	Tier 3	Moderate
Jihadi Hackers	X					X		X		Tier 2	Negligible

* Non-threat nation-states of the U.S. and its allies represent the high-water mark for top-tier nation-state cyber capabilities. Risk assessments should measure adversarial nation-states against these top-tier actors when estimating cyber capability.

** Although assessed as a Tier 4 actor, North Korea is a unique case, as the state is able to marshal state resources as necessary, which may enable capabilities which are generally ascribed to higher tier actors. North Korea in particular is likely capable of using destructive and highly disruptive attacks in kinetic conflict scenarios to support military objectives — a key differentiator of Tier 6 actors.

Figure 5.5: Illustrates a threat matrix categorising malicious actors based on their capability and the potential impact they could cause through attacks adapted from [6]. Here, the capability of an actor indicates the technical knowledge (sophistication) measured on a six-point scale where the 'Tier 1' represents the extremely limited technical capability and 'Tier 6' the most sophisticated. The levels of potential impact are measured on a five-point scale with 'Negligible' representing the attack where damages are most unlikely and 'Catastrophic' representing attacks which could cause complete paralysis and/or destruction of critical systems and infrastructures.

6 Discussion: Need to Gain Adversarial Perspectives

Protecting and securing systems is emerging priority of modern information-driven economy. Given that complete protection is unlikely and the implications of evolving threats (results of smarter attacks); it is imperative that operators need to significantly reassess their security decisions. This chapter highlights the methods of application of the core concepts of this thesis and future research directions.

One critical component to explicate the basic objective is 'trust'. Trust is an essential component of computer systems [104], but trust demands a reason for belief, and this belief bases itself on the 'expectation' of how a trustee will behave or perform [105]. Computer systems have well-defined actions and prescribed outcomes displaying identical characteristics as the bounded rational players in games. The key essence of this thesis that is to understand the behavioural characteristics of players can thus be applied to study the responses of systems defining trust on them.

We demonstrate an application of this in the second paper (from the list of original publication) which reasons on administering trust on systems; particularly amidst the elements of ETSI's Network Function Virtualisation Reference Architecture, based on their behavioural characteristics. It presents a trust metrics where the most trusted system is the one with identified characteristics [2].

Contemporary research has inadequate empirical evidence to indicate 'intent' and 'motive' behind attacks. The attack framework described in Section 5.3 can be used in categorising attacks around different dimensions. It would also help in gaining insights into the purpose of attacks.

However, to be able to predict expected behaviour of attackers in a realistic way requires a profound understanding of their behavioural characteristics. It demands a multi-disciplinary approach with efficient application of concepts from behavioural psychology, behavioural economics and cognitive science. Understanding attackers characteristics will support us to better assess the emerging threat vectors, vulnerabilities and fabricate comprehensive mitigation tactics supporting effective risk decision-making.

Having explored the motives behind attackers action; we aim at extending the application of the model described in Section 4.3 and Section 5.3 to deceit games (described in Appendix A.2) to determine the deceit failure point in a repeated interaction scenario.

Figure A9 represents the deceit failure point for a simple security deceit game. In the repeated deceit game, one likely outcome is that attackers may learn about the deceit and use multiple strategies such that the propensity of each attack becomes more successful. If the rate of success of attackers over a period of time is greater than the improvement of deceit strategy of operators, then the attackers will eventually discover the deceit. We define this point as the 'deceit failure point' where the deceit

strategy fails and attackers effectively win.

This game-theoretic argument is based on the premise of strong assumptions such as the knowledge players possess, actions sets and sequence of interaction. These assumptions help to reduce the complexity and uncertainty of real-life interactions such that they are computationally feasible to model. However, during this dimensionality reduction valuable information in lost and we are restricted to a tiny exploration area of the solution space. A facet of our future research is to design the evaluation environment in an intuitive manner acknowledging the psychological and economical aspects of security [106].

To model player behaviour, repeated games would be an ideal choice because real-life players have to interact repeatedly with partners and competitors. [28] states that repeated games assist in determining efficient equilibrium. However, every attempted attack might not be with an intention to acquire financial targets. For example, for a novice attacker gaining experience or reputation might be the foremost priority. Secondly, the attack process might end on an attempted attack. By contrast, this might be completely different in the case of an experienced attacker.

When such personality traits, as identified in [88]; the multiplicity of attack reasons especially the passive attack strategies, disconcert and unsettle security modelling approaches, particularly the Stackelberg approach [52]. The Stackelberg approach proceeds on a simplistic assumption that attackers always follows defenders and most likely attack.

When the psychological and personality aspects are reflected, it raises a number of research questions and challenges the traditional approach used in modelling cybersecurity situations. For example;

a. Is every interaction between an attacker and defender a repetitive process or is it a single-point interaction which ends on an attempted attack? Further, is using repetitive modelling approaches to model cybersecurity interactions an ideal choice?

b. By heavily investing in defending critical systems, are defenders appraising attackers around which particular system is most valuable to them? How would the knowledge of knowing the most valuable system influence the choice of attack strategies and the preference of system to be attacked?

c. A commonly adopted defensive strategy is deception. Is deceit a strategy for lack of resources or is it for lack of information? How do attackers behave acknowledging that an operator has deceiving characteristics?

This thesis argues attempts to delve deeper into these questions by substantiating that each interaction is unique, with a unique set of parameters characterising and moderating it. Modelling these unique interactions under common grounds is highly ineffective and leads us to a 'one size fits all' strategy that often fails as seen in the above mentioned Stackelberg approach. These unique situations require context-based modelled and using only game-theoretic concepts restricts the analysis to a

larger extent through biases, heuristics, and convenience.

This preliminary exploration will guide future studies in aptly modelling behavioural aspects of both attackers and defenders; help to design context-based scenarios intuitively by applying attack trees, defence trees, cognitive modelling, categorising players on intellectual traits and past experiences, and empirical data. Furthermore, this would help in comprehensively modelling the behavioural aspects of the participants supporting better security decision strengthening cybersecurity.

7 Conclusion: Security should be a Social Synergy

The telecommunications systems being inherently distributed and collaborative in nature presents a myriad of attack surfaces and threats. To this, the lack of adequate information on evolving threats and the inability to decisively predict adversaries' actions add challenges in prominently assessing situations and executing suited security decisions. This thesis investigated circumstances and factors influencing the strategic behaviour of Telecoms operators and attackers using game theory to understand their decision-making criteria to assist cybersecurity.

In chapter 4, we examined security investment games displaying the interdependency effects of security investment decisions on operators' behaviour. The exploration reconfirmed that investment in security does not necessarily guarantee protection against threats; existing, perceived and future threats. Besides financial aspects, operators need to contemplate their relationships with other operators as well as the indirect risks while security decision-making. Acknowledging these factors, we illustrated conditions encouraging succinct security investment decisions. Further, we discussed the financial and strategical aspects of dependency conditions among operators and how these conditions could aid in planning effective countermeasures.

Chapter 5 speculated the cybersecurity environment from attackers' perspective to gain insights into their strategic preferences. We assessed the environment acknowledging them as rational entities contrary to the strictly-bounded rationality of attackers in traditional game-theoretic approaches. In particular, we modelled attackers' characteristics with an extended set of choices available to them.

A decision-flow model has been designed capturing the choices of attackers during the attack process. An outcome of this is a generalised attack framework representing the effort required during the attack process. Utilising the framework, we proposed attack strategies optimising attackers' effort in achieving their utilities as it is a key parameter moderating attackers' decisions.

The results are still on a hypothetical level due to the complexities in modelling decision-making processes of humans. Moreover, lack of consistent temporal data and each security incident being unique advances the challenges in modelling human adversaries. In particular, the limitations in decisively inferring the intents, motives and other factors guiding attackers' actions from the existing security encountered data. Nonetheless, through this work, we are probing the foundations for drawing inferences about attackers' characteristics based on the empirical evidence from [1, 8, 90]. Especially their strategic behaviour from the context of cybersecurity.

Our initial inferences from this work exhibit that taking into consideration and admitting that attackers have incentives and strategic preferences imply operators; defenders in general, need to envisage how they apprehend attackers. Ultimately, investment in security is critical. However, operators should not compete against each other concerning security rather security should be a collaborative effort depreciating the chances of successful attacks.

References

[1] S. Panda, I. Oliver, and S. Holtmanns, "Behavioural modelling of attackers' choices," in *The Annual European Safety and Reliability Conference (ESREL 2018)*, 2018, accepted for publication.

[2] I. Oliver, S. Panda, K. Wang, and A. Kalliola, "Modelling nfv concepts with ontologies," in *the 21st International Conference on Innovation in Clouds, Internet and Networks (ICIN 2018)*, 2018, accepted for publication.

[3] C. McLellan. (2018) Cybersecurity: How to devise a winning strategy. [Online]. Available: http://www.zdnet.com/article/cybersecurity-how-to-devise-a-winning-strategy/

[4] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–10.

[5] FireEye. (2017) Cyber threats: A perfect storm about to hit europe?, cyber risk report 2017. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf

[6] Flashpoint. (2017) Business risk intelligence - decision report. [Online]. Available: https://go.flashpoint-intel.com/docs/BRI-Decision-Report-2017-End-of-Year-Update

[7] Symantec. (2017) Internet security threat report 2017. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[8] S. Holtmanns, Y. Miche, and I. Oliver, "Subscriber profile extraction and modification via diameter interconnection," in *International Conference on Network and System Security*. Springer, 2017, pp. 585–594.

[9] US-CERT. United states computer emergency readiness team. Accessed: 2018. [Online]. Available: https://www.us-cert.gov.

[10] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[11] J. Franklin, A. Perrig, V. Paxson, and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants." in *ACM conference on Computer and communications security*, 2007, pp. 375–388.

[12] S. Gordon, "The generic virus writer," in *Proc. Intl. Virus Bulletin Conf*, 1994, pp. 121–138.

[13] K. Hausken and G. Levitin, "Review of systems defense and attack models," *International Journal of Performability Engineering*, vol. 8, no. 4, pp. 355–366, 2012.

[14] S. Gordon, "Virus writers: The end of the innocence?" in *10th Annual Virus Bulletin Conference (VB2000), Orlando, FL*, 2000.

[15] P. T. Leeson and C. J. Coyne, "The economics of computer hacking," *JL Econ. & Pol'y*, vol. 1, p. 511, 2005.

[16] N. Christin, "Network security games: combining game theory, behavioral economics, and network measurements," in *International Conference on Decision and Game Theory for Security*. Springer, 2011, pp. 4–6.

[17] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge University Press, 2011.

[18] Microsoft. (2017) Security intelligence report 2017. [Online]. Available: https://www.microsoft.com/en-us/security/intelligence-report

[19] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[20] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior," in *Proceedings of the 3rd ACM conference on Electronic Commerce*. ACM, 2001, pp. 38–47.

[21] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[22] E. Altman, T. Boulogne, R. El-Azouzi, T. Jiménez, and L. Wynter, "A survey on networking games in telecommunications," *Computers & Operations Research*, vol. 33, no. 2, pp. 286–311, 2006.

[23] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT press, 1994.

[24] K. Merrick, M. Hardhienata, K. Shafi, and J. Hu, "A survey of game theoretic approaches to modelling decision-making in information warfare scenarios," *Future Internet*, vol. 8, no. 3, p. 34, 2016.

[25] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, p. 25, 2013.

[26] D. A. Burke, "Towards a game theory model of information warfare," AIR FORCE INST OF TECH WRIGHT-PATTERSONAFB OH, Tech. Rep., 1999.

[27] C. F. Camerer, *Behavioral game theory: Experiments in strategic interaction*. Princeton University Press, 2011.

[28] A. Laszka, M. Felegyhazi, and L. Buttyan, "A survey of interdependent information security games," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, 2015.

[29] J. S. Merlevede and T. Holvoet, "Game theory and security: Recent history and future directions," in *International Conference on Decision and Game Theory for Security*. Springer, 2015, pp. 334–345.

[30] J. Pita, M. Jain, M. Tambe, F. Ordóñez, and S. Kraus, "Robust solutions to stackelberg games: Addressing bounded rationality and limited observations in human cognition," *Artificial Intelligence*, vol. 174, no. 15, pp. 1142–1171, 2010.

[31] R. Anderson, "Why information security is hard-an economic perspective," in *Computer security applications conference, 2001. acsac 2001. proceedings 17th annual*. IEEE, 2001, pp. 358–365.

[32] S. Shiva, S. Roy, and D. Dasgupta, "Game theory for cyber security," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*. ACM, 2010, p. 34.

[33] J. Pita, R. John, R. Maheswaran, M. Tambe, and S. Kraus, "A robust approach to addressing human adversaries in security games," in *Proceedings of the 20th European Conference on Artificial Intelligence*. IOS Press, 2012, pp. 660–665.

[34] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness," *Journal of Artificial Intelligence Research*, 2011.

[35] K. Hausken, "Income, interdependence, and substitution effects affecting incentives for security investment," *Journal of Accounting and Public Policy*, vol. 25, no. 6, pp. 629–665, 2006.

[36] D. Florêncio and C. Herley, "Where do all the attacks go?" in *Economics of information security and privacy III*. Springer, 2013, pp. 13–33.

[37] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13–23, 2016.

[38] H. Kunreuther and G. Heal, "Interdependent security," *Journal of risk and uncertainty*, vol. 26, no. 2-3, pp. 231–249, 2003.

[39] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure?: a game-theoretic analysis of information security games," in *Proceedings of the 17th international conference on World Wide Web*. ACM, 2008, pp. 209–218.

[40] S. Kusumastuti, J. Cui, A. Tambe, and R. S. John, "A behavioral game modeling cyber attackers, defenders, and users." Research paper presented at the AAAI Spring Symposium, Stanford University, Palo Alto, 2015.

[41] J. Von Neumann and O. Morgenstern, "Game theory and economic behavior," *Joh Wiley and Sons, New York*, 1944.

[42] G. Owen, *Game theory*. Academic Press, 1995.

[43] J. Von Neumann and O. Morgenstern, *Theory of games and economic behavior*. Princeton university press, 2007.

[44] K. Leyton-Brown and Y. Shoham, "Essentials of game theory: A concise multidisciplinary introduction," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 2, no. 1, pp. 1–88, 2008.

[45] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Computers & security*, vol. 49, pp. 70–94, 2015.

[46] R. O. Tekes, "A common architecture for cyber offences and assaults-(organized advanced multi-vector persistent attack): Cyber war cyber intelligence, espionage, and subversion cyber crime," Ph.D. dissertation, Master's Thesis, University of London, London, UK, 2011.

[47] A. Klimburg and H. Tirmaa-Klaar, "Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the eu," *European Parliament*, 2011.

[48] M. Conway, "What is cyberterrorism?" *Current History*, vol. 101, no. 659, p. 436, 2002.

[49] K. Curran, K. Concannon, and S. McKeever, "Cyber terrorism attacks," in *Cyber warfare and cyber terrorism*. IGI Global, 2007, pp. 1–6.

[50] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97–102, 2013.

[51] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 472–486, 2013.

[52] D. Kar, T. H. Nguyen, F. Fang, M. Brown, A. Sinha, M. Tambe, and A. X. Jiang, "Trends and applications in stackelberg security games," *Handbook of Dynamic Game Theory*, pp. 1–47, 2017.

[53] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*. International Foundation for Autonomous Agents and Multiagent Systems, 2009, pp. 689–696.

[54] H. Varian, "System reliability and free riding," in *Economics of information security*. Springer, 2004, pp. 1–15.

[55] C. Herley, "The plight of the targeted attacker in a world of scale." in *WEIS*, 2010.

[56] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Security and Communication Networks*, vol. 4, no. 10, pp. 1162–1172, 2011.

[57] N. Garg and D. Grosu, "Deception in honeynets: A game-theoretic analysis," in *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC*. IEEE, 2007, pp. 107–113.

[58] N. C. Rowe, E. J. Custy, and B. T. Duong, "Defending cyberspace with fake honeypots," 2007.

[59] H.-M. Chou and L. Zhou, "A game theory approach to deception strategy in computer mediated communication," in *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on*. IEEE, 2012, pp. 7–11.

[60] P. Aggarwal, C. Gonzalez, and V. Dutt, "Cyber-security: Role of deception in cyber-attack detection," in *Advances in Human Factors in Cybersecurity*. Springer, 2016, pp. 85–96.

[61] C. Camerer, T. Ho, and J. Chong, "Behavioral game theory: Thinking, learning and teaching," *Advances in Understanding Strategic Behavior: Game Theory, Experiments, and Bounded Rationality: Essays in Honour of Werner Güth. Palgrave MacMillan*, pp. 120–180, 2004.

[62] R. Yang, C. Kiekintveld, F. Ordonez, M. Tambe, and R. John, "Improving resource allocation strategy against human adversaries in security games," in *IJCAI Proceedings-International Joint Conference on Artificial Intelligence*, vol. 22, no. 1, 2011, p. 458.

[63] T. H. Nguyen, R. Yang, A. Azaria, S. Kraus, and M. Tambe, "Analyzing the effectiveness of adversary modeling in security games." in *AAAI*, 2013.

[64] D. Kar, F. Fang, F. Delle Fave, N. Sintov, and M. Tambe, "A game of thrones: when human behavior models compete in repeated stackelberg security games," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 2015, pp. 1381–1390.

[65] M. Tambe, A. X. Jiang, B. An, and M. Jain, "Computational game theory for security: Progress and challenges," in *AAAI spring symposium on applied computational game theory*, 2014.

[66] T. Ryutov, M. Orosz, J. Blythe, and D. von Winterfeldt, "A game theoretic framework for modeling adversarial cyber security game among attackers, defenders, and users," in *International Workshop on Security and Trust Management*. Springer, 2015, pp. 274–282.

[67] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "Challenges in applying game theory to the domain of information warfare," in *Information Survivability Workshop (ISW)*. Citeseer, 2002.

[68] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Game theory meets information security management," in *IFIP International Information Security Conference*. Springer, 2014, pp. 15–29.

[69] A. Clemm, *Network management fundamentals*. Cisco Press, 2006.

[70] D. Ventre, *Information warfare*. John Wiley & Sons, 2016.

[71] M. Lelarge and J. Bolot, "A local mean field analysis of security investments in networks," in *Proceedings of the 3rd international workshop on Economics of networked systems*. ACM, 2008, pp. 25–30.

[72] G. Heal and H. Kunreuther, "Interdependent security: A general model," National Bureau of Economic Research, Tech. Rep., 2004.

[73] M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 1494–1502.

[74] Y. Hayel and Q. Zhu, "Attack-aware cyber insurance for risk sharing in computer networks," in *International Conference on Decision and Game Theory for Security*. Springer, 2015, pp. 22–34.

[75] W. Sun, X. Kong, D. He, and X. You, "Information security investment game with penalty parameter," in *Innovative Computing Information and Control, 2008. ICICIC'08. 3rd International Conference on*. IEEE, 2008, pp. 559–559.

[76] L. Jiang, V. Anantharam, and J. Walrand, "Efficiency of selfish investments in network security," in *Proceedings of the 3rd international workshop on Economics of networked systems*. ACM, 2008, pp. 31–36.

[77] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[78] J. Yuill, D. Denning, and F. Freer, "Using deception to hide things from hackers: Processes, principles, and techniques," 2006.

[79] J. D. Division, "Joint doctrine for military deception: Joint pub 3-58," *Joint Education and Doctrine Division*, 1996.

[80] L. Spitzner, "The honeynet project: Trapping the hackers," *IEEE Security & Privacy*, vol. 99, no. 2, pp. 15–23, 2003.

[81] L. Aidi, J. Markendahl, K. Tollmar, and G. Blennerud, "Competing or aligning? assessment for telecom operator's strategy to address ott tv/video services," in *Moving Forward with Future Technologies: Opening a Platform for All, the 19th ITS Biennial Conference*, 2012.

[82] C. Hill, "International business: Competing in the global market place," *Strategic Direction*, vol. 24, no. 9, 2008.

[83] K. S. Reddy, V. K. Nangia, and R. Agrawal, "Farmers fox theory: does a country's weak regulatory system benefit both the acquirer and the target firm? evidence from vodafone-hutchison deal," *International Strategic Management Review*, vol. 2, no. 1, pp. 56–67, 2014.

[84] A. van Marrewijk, "Crisis in the transition of telecom alliance unisource," *Journal of Managerial Psychology*, vol. 19, no. 3, pp. 235–251, 2004.

[85] A. Fielder, S. Konig, E. Panaousis, S. Schauer, and S. Rass, "Uncertainty in cyber security investments," *arXiv preprint arXiv:1712.05893*, 2017.

[86] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Symposium on requirements engineering for information security (SREIS)*, vol. 2005, 2005, pp. 1–8.

[87] D. B. Parker, *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons, Inc., 1998.

[88] M. Rogers, "A new hacker taxonomy," *University of Manitoba*, 2000.

[89] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[90] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for lte networks using the interworking functionality," in *IFIP Networking Conference (IFIP Networking) and Workshops, 2016*. IEEE, 2016, pp. 315–322.

[91] C. Herley, "Why do nigerian scammers say they are from nigeria?" in *WEIS*, 2012.

[92] ZDNet. (2017) Biggest hacks leaks and data breaches. [Online]. Available: https://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2017/

[93] D. Watson and J. Riden, "The honeynet project: Data collection tools, infrastructure, archives and analysis," in *Information Security Threats Data Collection and Sharing, 2008. WISTDCS'08. WOMBAT Workshop on*. IEEE, 2008, pp. 24–30.

[94] C. F. Camerer, T.-H. Ho, and J.-K. Chong, "A cognitive hierarchy model of games," *The Quarterly Journal of Economics*, vol. 119, no. 3, pp. 861–898, 2004.

[95] H. A. Simon, "Theories of bounded rationality," *Decision and organization*, vol. 1, no. 1, pp. 161–176, 1972.

[96] J. R. Anderson, *How can the human mind occur in the physical universe?* Oxford University Press, 2009.

[97] V. D. Veksler and N. Buchler, "Know your enemy: Applying cognitive modeling in security domain," in *Proceedings of the 38th Annual Conference of the Cognitive Science Society*, 2016, pp. 2405–2410.

[98] M. Jain, E. Kardes, C. Kiekintveld, F. Ordónez, and M. Tambe, "Security games with arbitrary schedules: A branch and price approach." in *AAAI*, 2010.

[99] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu *et al.*, "Click trajectories: End-to-end analysis of the spam value chain," in *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE, 2011, pp. 431–446.

[100] Y. Liang, H. V. Poor, S. Shamai *et al.*, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[101] M. J. Lewis, "Hierarchical decision making." in *STIDS*, 2013, pp. 162–165.

[102] K. Hausken, "Security investment, hacking, and information sharing between firms and between hackers," *Games*, vol. 8, no. 2, p. 23, 2017.

[103] M. Khouzani, V. Pham, and C. Cid, "Strategic discovery and sharing of vulnerabilities in competitive environments," in *International Conference on Decision and Game Theory for Security*. Springer, 2014, pp. 59–78.

[104] S. P. Marsh, "Formalising trust as a computational concept," 1994.

[105] D. Gambetta, "Can we trust trust?" *Trust: Making and breaking cooperative relations. Department of Sociology, University of Oxford*, pp. 213–237, 2000.

[106] B. Schneier, "The psychology of security," in *International Conference on Cryptology in Africa*. Springer, 2008, pp. 50–79.

[107] F. Cohen and D. Koike, "Misleading attackers with deception," in *information assurance workshop, 2004. Proceedings from the fifth annual IEEE SMC*. IEEE, 2004, pp. 30–37.

[108] S. Murphy, T. McDonald, and R. Mills, "An application of deception in cyberspace: Operating system obfuscation1," in *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2010, p. 241.

[109] N. C. Rowe and H. S. Rothstein, "Two taxonomies of deception for attacks on information systems," 2004.

[110] M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in *Human System Interactions, 2009. HSI'09. 2nd Conference on*. IEEE, 2009, pp. 624–631.

[111] J. J. Yuill *et al.*, "Defensive computer-security deception operations: Processes, principles and techniques," 2007.

[112] F. Cohen, "A note on the role of deception in information protection," *Computers & Security*, vol. 17, no. 6, pp. 483–506, 1998.

[113] M. H. Almeshekah and E. H. Spafford, "Cyber security deception," in *Cyber Deception*. Springer, 2016, pp. 25–52.

A Appendices

A.1 Threat Matrix Scales

Tier 1	The cyber actor(s) possess extremely limited technical capabilities and largely make use of publicly-available attack tools and malware. Sensitive data supposedly leaked by the attackers are often linked back to previous breaches and publicly-available data.
Tier 2	Attackers can develop rudimentary tools and scripts to achieve desired ends in combination with the use of publicly-available resources. They may make use of known vulnerabilities and exploits.
Tier 3	Actors maintain a moderate degree of technical sophistication and can carry out moderately-damaging attacks on target systems using a combination of custom and publicly-available resources. They may be capable of authoring rudimentary custom malware.
Tier 4	Attackers are part of a larger and well-resourced syndicate with a moderate-to-high level of technical sophistication. The actors are capable of writing custom tools and malware and can conduct targeted reconnaissance and staging prior to conducting attack campaigns.
Tier 5	Actors are part of a larger and well-resourced organization with high levels of technical capabilities such as those exhibited by Tier 4 actor sets. In addition, Tier 5 actors have the capability of introducing vulnerabilities in target products and systems, or the supply chain, to facilitate subsequent exploitation.
Tier 6	Nation-state supported actors possessing the highest levels of technical sophistication reserved for only a select set of countries. The actors can engage in full-spectrum operations, utilizing the full breadth of capabilities available in cyber operations in concert with other elements of state power, including conventional military force and foreign intelligence services with global reach.

Figure A1: Illustrates the capability scale for the threat matrix in Figure 5.5 adapted from [6].

Negligible	Damages from these attacks are highly unlikely or are unable to adversely affected the targeted systems and infrastructure. Such incidents may result in minor reputational damage. Sensitive systems and data remain intact, confidential, and available.
Low	Attacks have the capacity to disrupt some non-critical business functions, and the impact is likely intermittent and non-uniform across the user-base. User data and sensitive information remain protected.
Moderate	Attacks have the potential to disrupt some core business functions, although the impact may be intermittent and non-uniform across the user-base. Critical assets and infrastructure remain functional, even if they suffer from moderate disruption. Some non-sensitive data may be exposed. Actors at this level might also expose sensitive data.
Severe	Cyber attacks emanating from this actor set have the capacity to disrupt regular business operations and governmental functions severely. Such incidents may result in the temporary outage of critical services and the compromise of sensitive data.
Catastrophic	Kinetic and cyber attacks conducted by the threat actor(s) have the potential to cause complete paralysis and/or destruction of critical systems and infrastructure. Such attacks have the capacity to result in significant destruction of property and/or loss of life. Under such circumstances, regular business operations and/or government functions cease and data confidentiality, integrity, and availability are completely compromised for extended periods.

Figure A2: Illustrates the potential impact scale for the threat matrix in Figure 5.5 adapted from [6].

A.2 Attacker vs Deceiving Operator

In this work, we perform a behavioural game-theoretical investigation on deception in cybersecurity from an attacker's perspective with an intention to determine attack strategies strengthening the chances of successfully compromising a target. The

examined scenario illustrates a deceit game between an attacker (cyber criminal, hacker) and a telecommunication operator (defender) considering the operator to be deceiving.

Being deficit of resources, it would be economically infeasible for an operator to invest in high standard defence technologies securing each and every system. An effective solution is to devise strategies and tactics to optimally invest resources which would include estimating how much investment in a particular security technology would be optimal or when would it be optimal to invest in a particular security technology.

However, an operator can save a lot of money by deliberately falsifying his actual state with respect to the actual implementation of a particular security technology. The operator being deceptive might influence the behaviour of the attacker, as the attacker might not attack believing the operator has defences - eventually being a victim of the deceiving strategy! The deceiving nature of the operator causes uncertainty in the choice of an action for the attacker as reliable information regarding the state of the operator cannot be derived from the proposed state. Additionally, considering an attacker would always prefer to maximise his chances of successfully compromising a targeted system, so, what would be an effective strategy for the attacker in deceptive conditions?

A common practice in computer security is to hide things from an agent, computer, or human. Use of firewalls, access-controls, and encryption are common forms of hiding through denying information [78]. Use of deception is another means of hiding information extensively used in military and has found its way into computer security and information protection [107] [108] [109].

Deception, as stated by [110], is distorting one's perceptions of reality. Deceptive strategies when deployed can aid the deceiver by placing the target at a disadvantage. One of the most widely accepted definitions of computer-security deception is from Yuill [111] stating computer security deception as "planned actions taken to mislead attackers and to thereby cause them to take (or not take) specific actions that aid computer-security defences". In this paper, the definition of deception we are using is falsely disclosure of investment in a particular security technology than the operator (defender) has actually made.

A wide variety of deception techniques have been proposed for defending computer networks and information systems. One of the widely proposed methods is the use of honeypots as camouflage for deceiving the attackers [56] [57] [58] [80]. Beside honeypots, Yuill [78] have proposed methods for deceptive hiding by defeating the processes adversaries implement to discover hidden things. Cohen [112] studied deception as a means to protect information system and [107] have shown how it can be used to guide the path of an attacker. Rowe et al. [109] have provided taxonomies of deception methods in cyberwar and [110] have used these taxonomies in exploring types of deception related to cybersecurity for control systems.

Advantages of deception based security mechanisms have been proposed by [113]. While [58] have demonstrated how pretending to be a honeypot decreased the

amounts of attacks. [59] studied dynamic adaptation of deceiving strategies by online deceivers in computer-aided communications and [60] has analysed the effects of extent of deception and timing of deception on attacker's decision to attack a computer network.

From the above literature review on deception in computer security, [56] [57] [59] and [60] have employed game theoretic approaches to devise strategies favouring the defenders. Game theory, being a mathematical modelling tool, has been widely used to study a variety of security scenarios in computer networks, communications and information security [4] [24] [22] [25] [51] for exploring and addressing security vulnerabilities, and understanding decision-making behaviour of concerned participants.

Our work differs from the research discussed above by studying the behavioural aspects in a deceiving cybersecurity interaction environment and evaluating the interaction from an attacker's perspective considering the telecommunication operator (defender) to be of deceptive nature. This paper extends the assessment of the interaction environment by supplementing it through hierarchical decision analysis tree and have provided further research directions in refining the strategies by understanding the psychological aspects of an attacker against deceiving operator.

A.2.1 Security Game

		$O_{investment}$	
		Truth	Lie
Atk	Attack	$r-c-l,\ r-c$	$r-c+g,\ r-l$
	Don't attack	$r,\ r-c$	$r,\ r$

Figure A3: Illustrates the payoff matrix for the security deceit game.

$r-c-l>r$ and $r-c+g>r$

Solving these inequalities we obtain $c+l<0$ and $c<g$

whereas for the operator to lie

$r-l>r-c$ and $r>r-c$

Solving these we obtain $c>l$ and $c>0$

Apart from the pure strategies, a mixed (randomised) strategy where the players are indifferent towards their choice of actions can be achieved using the mini-max solutions. Under uncertain conditions, an operator's best response would be a strategy maximising his payoff and minimising his opponent's payoff. To achieve the optimal strategy, the operator must mix his choice of actions such that the attacker has no prefered choice of action. Assuming there is no prefered choice of action and

both players have decided to randomise their strategy, and the operator has decided to be truthful regarding his investment in security p_o times and lie with $1 - p_o$. The operator's best response would be a strategy maximising his payoff and minimising the attacker's payoff. To achieve the optimal strategy, the operator must mix the choices such that his opponent is indifferent towards his choice of actions. To achieve the optimal strategy,

$$\begin{aligned} U_{Atk}(Attack) &= U_{Atk}(Don't\ attack) \\ p_o * (r - c - l) + (1 - p_o) * (r - c + g) &= p_o * (r) + (1 - p_o) * (r) \\ c &= gp_o - l(1 - p_o) \end{aligned} \tag{A1}$$

For the attacker to attack

$$\begin{aligned} U_O(Truth) &= U_O(Lie) \\ p_a * (r - c) + (1 - p_a) * (r - c) &= p_a * (r - l) + (1 - p_a) * (r) \\ c &= p_a l \end{aligned} \tag{A2}$$

A.2.2 A simple example

		$O_{investment}$ Truth	Lie
A	Attack	-1, 1	1, -1
	Don't attack	1, 0	-1, 1

Figure A4: Illustrates the payoff matrix for a simple security deceit game.

Due to the variability in the nature of the operator, it is harder for an attacker to decisively opt an action making the decision process a stochastic process. Figure A5 presents the stochastic decision model of an attacker against an deceiving operator. The grey boxes represent the stages where an attacker has to make mission-critical decisions based on the proposed status of the targeted operator.

Under these uncertain conditions, there exists no preferable pure strategy the attacker can implement. Game theory suggests that for the best response a player should devise a strategy maximising his payoff and minimising his opponent's payoff. From the payoff matrix, Figure A4, there exist no preferable choice of pure strategy and to achieve an optimal strategy a player must mix his choice of actions such that it removes any incentives of choosing one action over the other for his opponent. Further, considering the deceiving nature of an operator, let us assume that the attacker perceives that the operator is truthful regarding his investment in the security with

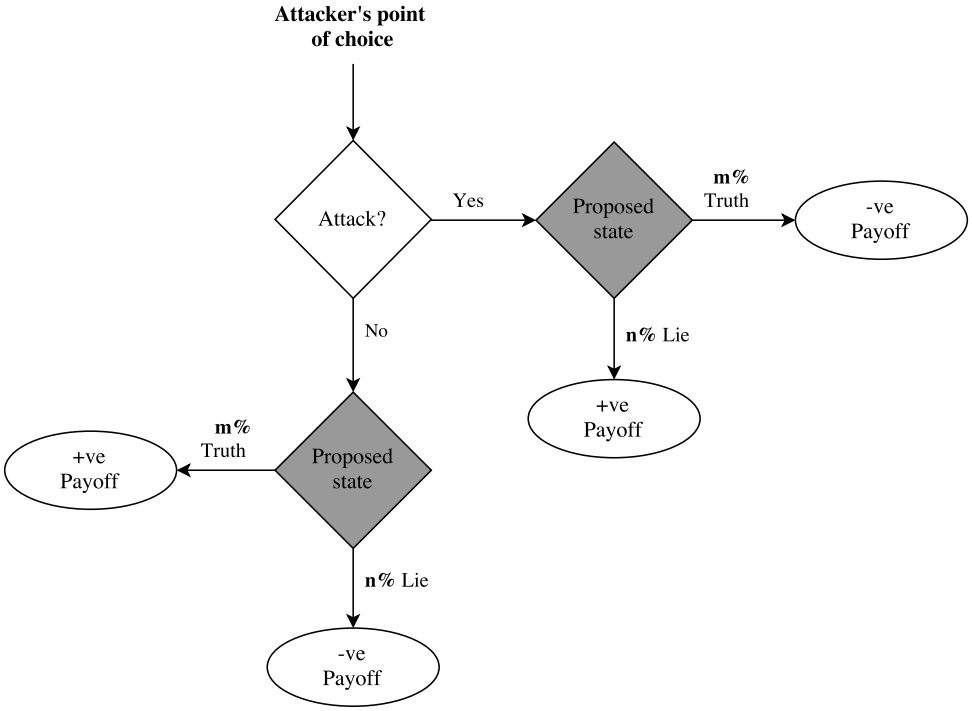

Figure A5: Illustrates the decision model of attackers' with imperfect information allocating certain probabilities to address the uncertainty in conclusive decision-making.

a probability of m and lying about his investment in the security with a probability of n, irrelevant of the proposed status by the operator. Where

$$m + n = 1; \quad 0 \leq m, n \leq 1 \tag{A3}$$

Attacker's strategy to make the operator indifferent to his choice of actions, perceiving that the operator is truthful regarding his proposed status with a probability of m can be represented as

$$\begin{aligned} U_O(Truth) &= U_O(Lie) \\ 1 * m &= (-1) * m + 1(1 - m) \\ m &= 1/3 \end{aligned} \tag{A4}$$

Thus, the attacker must choose to attack with a probability of 1/3 and not to attack with a probability of 2/3 to make the operator indifferent towards his choice of actions. The operator's payoff against this mixed strategy of the attacker is 1/3, irrelevant of any choice of action.

Similarly an operator would want to devise a strategy to maximise his payoffs by balancing the extent of deceit. To achieve this, the operator must make the attacker

indifferent to his choice of actions. Operator perceiving that the attacker will attack, the mixed strategy can be represented as

$$\begin{aligned} U_A(Attack) &= U_A(Don't\ attack) \\ (-1) * m_o + 1 * (1 - m_o) &= m_o + (-1) * (1 - m_o) \\ m_o &= 1/2 \end{aligned} \tag{A5}$$

Thus, the operator can maximise his payoff by truthfully proposing with a probability of 1/2 and falsely proposing with a probability of 1/2. Attacker's payoff against this mixed strategy of the operator is 0, irrelevant to any choice of action.

From the attacker's perspective, if the operator anticipates the frequency of certain types of attacks is more then certainly he will invest in security raising his defences against such attacks. This would be a highly undesirable situation for an attack on his chances of successfully compromising the system will be slim, motivating him to figure out mixed attack strategies keeping the operator unalarmed.

Whereas, from the operator's perspective, a higher security level will certainly decrease attacks. But, investing in defences for all the systems would be economically infeasible for operators even though it might be a higher desirable state from a security perspective. A means of economically benefiting strategy would be to persuade an attacker in believing that he has invested in defences, while have not invested in reality. However, the operator needs to know the extent to which he should be deceiving such that it is optimal and the attacker still believes him.

Figure A6 presents an opponent's payoffs for the probabilities of choice of actions by a player where the attacker believes the operator is truthful and the operator believes that the attacker will attack. Point B represents the maximum payoff the attacker can reach by minimising the maximum payoff of the operator for being truthful. Whereas, point C represents the maximum payoff an operator can achieve by minimising the maximum attack payoff of the attacker (represented as point A). The triangle ABC represents the solution space obtained from the computed mixed strategy of the players.

Using similar evaluation, Figure A7 presents an opponent's payoffs for the condition where the attacker perceives that the operator is lying regarding his investment in security and the operator perceives that the attacker will not attack.

The triangle KML represents the solution space obtained from the computed mixed strategy of the players. Point L represents the maximum payoff the attacker can reach by minimising the maximum payoff of the operator for lying. Whereas, point M represents the maximum payoff an operator can achieve by minimising the maximum payoff of the attacker for not attacking (represented as point K). Combining the solution spaces from Figure A6 and Figure A7, the area PQRS in Figure A8 represents the solution space for the deceit interaction scenario.

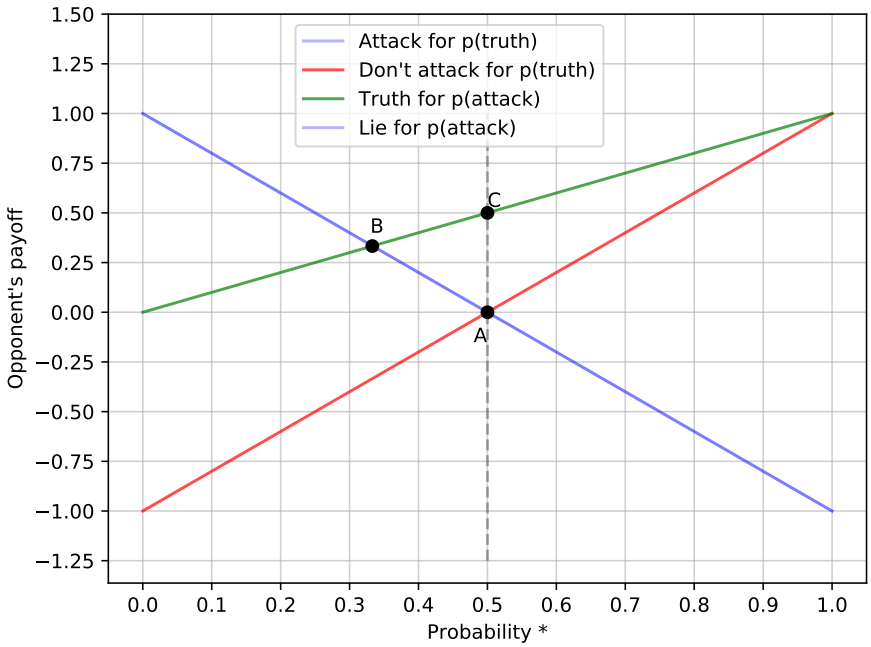

Figure A6: Illustrates the opponents' payoff structure for the scenario where the attacker believes that the operator is truthful and the operator believes that the attacker will attack.

A.2.3 Deceit Failure

The previous sections have presented the games and payoffs as points in time. In an extended scenario, these games are played in more dynamic environments over time with the payoffs changing according to local circumstances. We can use the models presented here to explore particular points that may (or may not) occur and from these, understand the conditions, or if not, the circumstances that lead to these solutions.

Figure A9 presents the analysis of point in time which we term of deceit failure. As a game progresses one outcome is that it is likely that the attacker learns about the deceit and varies his or her strategy such that attacks become more successful. If the rate of success of the attacker over time is greater than the improvement of deceit strategy of the telecoms operator then eventually the attacker will discover the deceit. It is at this point that the operator's deceit fails and the attacker effectively 'wins'.

The rate of change of the area can be used to determine the efficacy of the strategy. A threshold value can be assigned which would indicate the level of success of a strategy and this can be used to determine the actual investment point for an operator.

This work has described so far the games and work in now continuing on characterising the above scenario - albeit using linear equations for simplicity at this time. However, we have provided the characteristics that show when an attacker's belief in the deceit is failing. Understanding this is critical for the operator to understand in making the security technology decision.

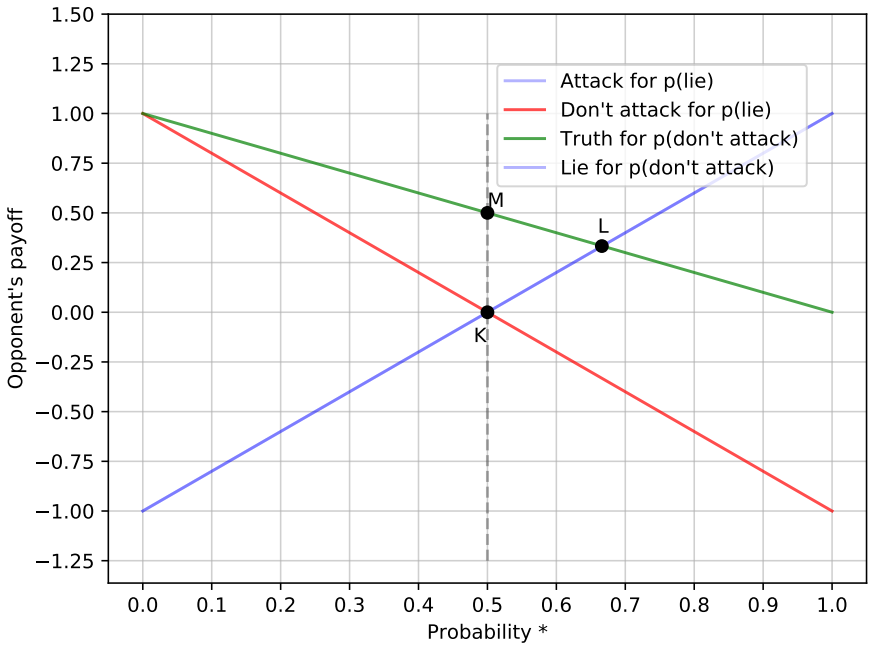

Figure A7: Illustrates the opponents' payoff structure for the scenario where the attacker believes that the operator is lying and the operator believes that the attacker will not attack.

We have seen from our previous SS7/Diameter examples such characteristics develop with some telecommunications operators and that the rate at which the deceit failure point is reached in both exceptionally rapid in time as well as in the solution spaces. For some operators we can also show situations where the current state of the system is already *after* the deceit failure point and that at this stage any investment in the deceit strategy is purely cosmetic leading to another set of failures with similar characteristics, ie: ultimate failure of the company.

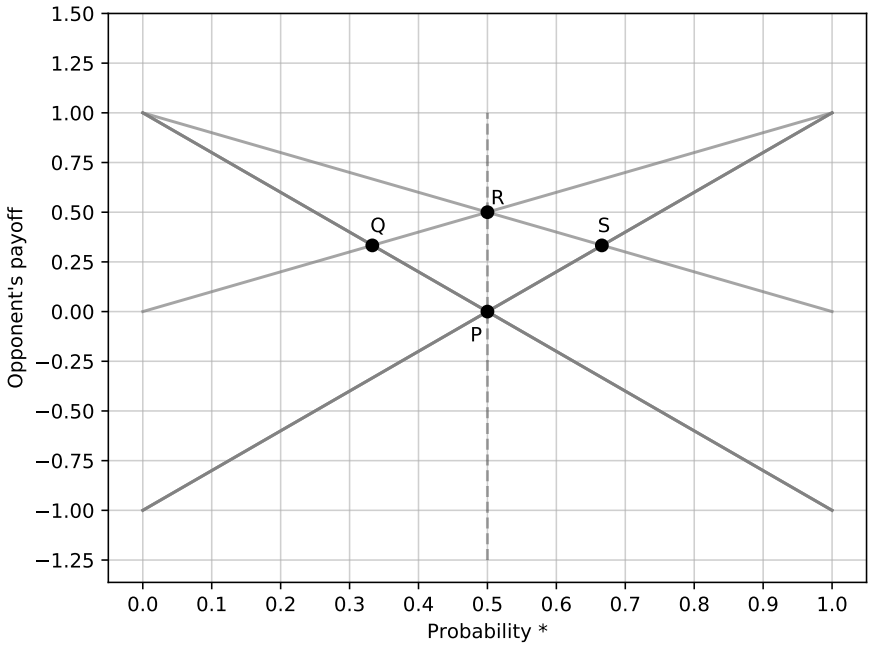

Figure A8: Illustrates the solution space for the deceit interaction.

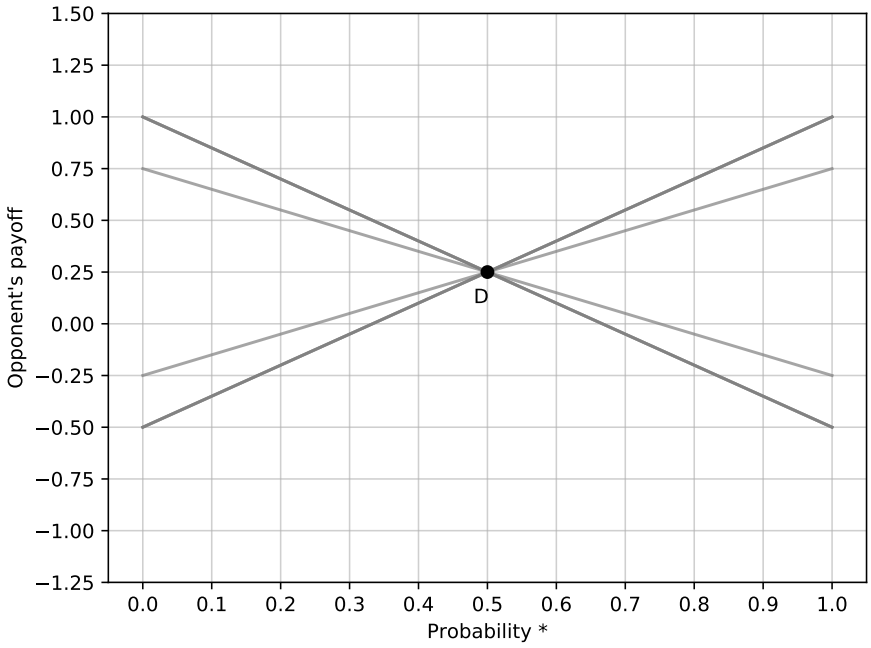

Figure A9: Illustrates the analysis of the solution space in Figure A8 to the point of deception failure.