Chapter 3

Overview of Game Theory Strategies

The central objective of this chapter is to position this analyze in the area of dynamic approaches. I will converse what the donation of this study is with respect to (1) a theoretical point of view along with (2) a content point of view (the dynamics of approaches). The chapter is hence separated into two parts. The first part inspects various theoretical perspectives on approaches. Further section will match these asymmetric concepts, argue what the experiment gaps are, and demonstrate the location and contribution of game theory. The second part of the chapter provides additional in depth to analysis: the dynamics of approaches. Here, I also review the correspondence, describe analysis gaps in Section 3.4.3, along with display what the contribution of this study will be for the dynamics of approaches. The chapter begins with a preface to the concept of an approach.

3.1 Corporate Approaches

3.1.1 Characteristics and objectives

The dynamic approach is a broad term which encloses frequent forms of organizational management. This analyze does not centralize on one appearance of approaches, but rather allots a common along with abstract perspective on approaches. Hence no cataloged description of approaches will be allotted. For additional study one can refer, Weimin (2009). An approach is various from a network communication, or participation of key key actors but the term encloses organizational forms such as equability joint ventures, approving agreements, co-operated product development projects, acquiring along with developing, and minority equability associations (Weimin, 2009).

To follow these approaches, one can say that the activities within an approach continue formerly autonomous (Weimin, 2009). This describes the difference among approaches as well as collaborators or participants. Also, coincidence brings about the key actors (actor is termed here as inline to UML representation) co-actively dependant on each other (Grünvogel, 2005); each business desires the other or others to accomplish a beneficial activity. This dependence is complex by the uncertainty the key actors face with reverence to the action of their key actors.
(Weimin, 2009). Additionally dynamic approaches are intentionally long term, as matched to a market activity. Associated to this long-term approach of related approaches, the conditions called dynamic approaches are often applied. In this analysis, for the sake of advantageousness, I will often apply the shorter term of ‘approach’. Although approaches are considered to be long-term, they are in principle temporal organizational forms (Martin, 2009).

The term approach is broad and encompasses different variations. First, one can make a distinction between single and multi-partner approaches. The former contains two key actors, while multi-partner approaches contain more than two key actors. Both are relevant objects to study. As most approaches are dyadic (Martin 2009), studying two-partner approaches is most relevant for real-life situations in operating system handling. However, multi-party approaches are also relevant since they are analytically more complex to study and more difficult to manage which will occurs in case of network’s cyber security (Weimin, 2009) (Chi Zhang, Jinyuan Sun, 2010). In this study, I will consider both single and multi-partner approaches.

Secondly, dynamic approaches can be horizontal along with vertical which means research will focus on generalized solution for cyber security with the help of mathematics. The difference relates to the kind of stakeholder’s enterprise allies with. While vertical approach directly buyer - supplier approaches, horizontal approaches are associations between businesses in the equivalent industry (Alpcan T. and Baser T, 2006), (Castro, M, Costa, M. and Harris, T., 2006), (Chang, H. and Atallah, M.J. ,2001). In horizontal approaches, businesses synchronize with their competitors as well as partners (Filar, J. and Vrieze, K.,1997). This kind of ‘competitions’ will acts as approach which is interesting as well as complicated to analyze. In this dissertation, one ideal will conduct more to vertical approaches, while the other patterns accept for coupled horizontal and vertical approaches.

In common, businesses appearance approaches to begin affixed account. More definitely, various excuses for developing approaches can be discriminated: to appropriation economies of caliber, to addition access to accurate assets, to allocate risks, along with for the action of bilateral lobbying (Ganzfried, S. and Sandholm, T., 2009). Economies of scale assign to efficiency benefits captured through cooperation. In the last decade, a change has taken place from these more approved cost-driven approaches to knowledge-intensive approaches (Hansen.E.A., etal, 2004). This cooperates with the second drive for approach assembly; acquiring
access to the assets of assistants. Belongings can assign to absolute tangible goods, but also to skills as well as market approach. Along with domains of approach key actors, products as well as benefits can be acted along with set of business which could not have been mature alone. These kinds of approaches are labeled co-development along with co-marketing approaches. Additionally, activities can teach collective the access to these assets along with application details thus gained access in their own technology. The next thought for creating approaches is to reduce risk. If complete systems is unstable or are insecure for processing, an apocalypse to acceptance with this is assigning the risk. Mutually collective lobbying intimates the conception of standing strong together. Definitely when new technology is comprised, arranging a standard is critical. Similarly, operating system can choose to except in an approach to allocate a process execution with the idea that there will be appropriate resource allocation to maintain secure and deadlock free operation of whole system.

2.1.2 Fit among key actors

Depending on what encourages a system to appearance a dynamic approach, its decisions for a process execution will decide.( Bernstein et al. ,2004) have mature a theory of fit which describes on which circumstances approach associates should pursue for a good result. They denote a fit as a commanding as well as efficient way (Lye, K. and Wing J., 2005). The following circumstances can be the case:

- deadlock - In an operating system, a deadlock is a situation which occurs when a process or thread enters a waiting state because a resource requested is being held by another waiting process, which in turn is waiting for another resource. If a process is unable to change its state indefinitely because the resources requested by it are being used by another waiting process, then the system is said to be in a deadlock.

- Starvation

- Indefinite wait state

- Over burdened process
• Network failure

Within this account, a variation is brought among strategic on the one hand and four other types of process situations on the other hand.

A dynamic strategy is the event needed to begin an approach. To capture a deadlock, agents need to allot mutual accessorized process. For resource intensive confederations, complementarily few responsible resources along with abilities are always working in background. Although for approaches that are consistent up for efficiency analyzes, a strategic suit might not individual call for complementarily, but may also need uniform key actors. Hence, only if a deadlock arises, there will be need of a mathematical logic to resolve it.

Once alike a strategic suit occurs, alertness will be assigned to the other four processes: Starvation, Indefinite wait state, Over burdened process, Network failure and operational, along with system resources. For these, closeness is expected as asymmetries between key actors on these processes would contrarily affect the period along with dictatorial operating of approaches (Roy, S., 2010).

Not all mathematical logics will be equivalently considerable in each approach. In an efficiency-driven approach, deadlock situation might be less applicable than in an approach set up for discovering. Additionally an abnormality of one process can be appeased by parallels on other processes. In short, a starvation situation of process is critical for each co-operation as it is regularly the reason approach is allocate up in the early place. Network, operational, along with human responsible processes perform additional role in the system efficiency as well as advantageous acting of an approach (Sagduyu, Y., 2009).

3.1.3 System performance in-line with business models

Although dynamic approaches have been constructed additional commonly in current decades, the number of approaches that have collapsed belatedly has not compressed (Shoham, Y., Powers, R., and Grenager, T. 2007), Rather, activities face actual complexities capturing the caliber synergies that can result from approaches (Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V., 2010). These establishments denote the consequence of research on approach activity. This
area briefly consults this area of research. The assumption of approach action is not only acquiring more attention in approach research, but it can also be characterized as problematic as researchers disagree how to describe as well as allocate approach activity.

First, there are various procedures to describe approach activity. One alert for a high approach activity could be survival or approach interminability. On the one hand, an enduring approach might refer to achievement. Durable confederations allot key actors convenience to understand as well as behave optimally in the approach. On the other hand, an inconveniently closed approach does not intimate approach failure, nor does an approach with a long period approach fulfillment. Together, approach durability allocates many indications for the activity of approaches but cannot be the only indicator.

Another mechanism of certifying approach activity is to focus on approach affects:

• Strategy building for whole system
• Financial outcomes
• Role of key actors

Complete three assumptions refer to entices an approach carries for the assistants: the ambitions of the approach, along with new education. Although these affects might have been accomplished for key process actors, this does not assure that the approach was an accomplishment in the sense of cooperative, as well as creative relationship between different processes. It also seems critical to check how the process behaved.

Yet another factor of a beneficial activity is approach stability (Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V., 2010). Approach instability is described as “... a major conversion that was unplanned along with premature from the perspective of either one assistant ...” (Littman, 1994). Approach instability is inefficient because it is injurious for at least one process; the approach has not evolved as was arranged and awaited (like the case of process starvation). A consistent approach hence refers to an approach with no major unplanned as well as undesired conversions. The approach evolves to the satisfaction of the key actors.
A second assumption associated to approach behavior is how to calibrate the idea. A distinction is frequent acted between the type of the security as well as the grade of the approach. An approach might capture its aims on a co-operative level, but a key player process might be discouraged with its individual accomplishments. Inversely a key player process might be comfortable with an approach due to of, for example, the discovering chances it has had, while on a complete level the approach might have collapsed to achieve its goal. Along with converges differ on allocating approach activity for operating system process with objective measures alike as schedule allotments versus conceived activity by all processes offered by operating system.

Although the idea on approach activity should be accepted, the centrality of this examine is not clearly on calibrating or elaborating approach behavior. Although insights allotted in this analyze can control to a beneficial understanding of approaches, as well as in this mechanism help system administrators to correct approach performance of computer operating system as well as network topology.

3.2 Overview of theoretical perspectives on approaches

This section demonstrates an abstract of varying theoretical perspectives on strategic approaches. An explanation will be allocated of the rationale of each detached theoretical perspective. Based on this review, in previous section, it will be consulted what the analysis gaps in the area of operating system security and performance of network are also based on that, clashed what kind of contribution game theory can make.

Most theoretical literature on approaches is determined in the multi-disciplinary area of approach. Agenda analyzes key choices for the complete activity on how to adjust a computer system’s behavior (Roy, S., Ellis, C., Shiva ,2010); (Sagduyu, Y.E. and Berry, R. and Ephremides, A. 2009). As with the tactics, the composition on approaches are multi-disciplinary in nature along with emphasis on economical and cyber security circumstances to more behavioral results.

This domain consults the following perspectives on strategic confederations:

• Operational cost
• Resource allocation
• Security Strategic theory
• Cyber Security Related Factors
• Mathematics with game theory approach

The first four perspectives are the more approved approach conceptions as well as will be displayed from more moderately oriented to more practical oriented.

These academic perspectives have been determined due to of their common circumstance in cyber security approach analysis as well as due to they are accompanied to represent the main flows of analysis in the web application security field. Of course, developing a decision between the frequent approach applications affects to ignore others, as, for ideal system concept, cyber security theory, as well as software learning.

3.2.1 Operational cost

According to system cost economics, efficient system’s principle for acquiring higher security with is to reduce costs (Littman, M. L. 1994. ) In other words low security system gets hacked and that is most costly for any company, hence it is better to invest in good security development. The comparatively low cost system protection can be developed using mathematical logic using game theory. During the decision approach that a company undertakes when developing activities, the level of damages is the only rationale behind this choice (Roy, S., Ellis, C., Shiva ,2010).

To complete an activity, a business can apply several decision governance approaches. (Shandilya ,2010) explains a simultaneous activity, as a security provider, as well as a security seeker system. Others along with acquire core solutions, which of course do not bring about operational costs, but development costs along with direction costs . Different considerations
there for determining the best security provision as each differs in scenario of operation and hacker attacks.

According to the activity cost architecture, collective approaches are a process to bypass inconvenient assignments. A security activity can be inefficient in two ways. First, a hacker attack acts as a business threat for others. Furthermore, system security can be inefficient or can just collapse. Allocated these activity defeats as well as subordination assumptions, the operational charges for providing cyber security can be high. Causing system infection via hacker can be inconvenient if the system has, for simulation, little evidence, technology, or manpower to monitor the definite service. In other words, the development amounts will be relatively high. (Shandilya, 2010) also acquires wholly claimed investments along with gains into account. Few argue that adding over another system controls to actual system charges as well as, moreover, the initial security adds much more assets than it desires hence it acquires over a whole information technology business.

Consequently if computational developments charges are high, businesses are unsuitable, as well as acquisitions except spill-over costs, approach might be the most capable choice. Through system admin rights, key actors have a mutual contract towards the approach. Both parties bonus or lose by the behavior of the cooperation; they determine themselves in a mutual hostage position (Lye, K. and Wing J. 2005), Although this mutual dependence can command to opportunistic activity, the unilateral dependence of the beginning security provider business in acquisitions is bypassed in this method. Moreover, through approaches, systems can abstain expect to internalize many behaviors that does not belong with the core system of the administration. Of course, approaches also produce charges, such as monitoring costs, management costs, as well as search cost. But an approach might be an advantageous acquisition than other approaches if it controls to the most proficient behavior of providing cyber security.

3.2.2 Resource allocation

In this section, I consult resource-allocation view as well as resource-dependency concept. Whereas the resource-allocation view is extended an object oriented concept describing
competitive heterogeneity among operating systems and networking, resource-dependency concept centralizes on belongings as a means to exert authority.

**Resource-allocation view**

In the last two decades, the resource-allocation view has become a commonly approved concept in tactics analysis describing a system’s activity. The concept is an acknowledgment to the external aim of earlier conceptions (Heifetz, Aviad, Martin Meier, and Burkhard C. Schipper, 2013) While Clerk clarifies activities of security businesses through their position in the web applications as well as the architecture of the software program (ex. Facebook), the resource-allocation view poses that there is an association among the belongings of a application along with its activity (Facebook provides social networking which needs high security level). What a software application acquires or has access to checks what it accomplishes.

The beginning point of the resource-allocation view is to account the software application as a bundle of social assets. Resources are all the assets, abilities, methods, education along with knowledge coordinated by the web application, as well as are a caliber source of economical advantage for the application owner. The caliber of competitive benefit a resource yields for the application owner is conditional on how essential, scarce, imperfectly imitable, as well as needing in direct alternatives the belongings are. Valuable assets approve application owner to improve application level efficiency along with effectiveness. A resource is insufficient if it is odd in the market of a application owner’s current as well as caliber competitors (just like happened with Orkut due to entry of Facebook). Inimitability describes that information asymmetry continues alike that resource cannot be acquired or recreated by other companies without a cost disadvantage. And lastly, it matters whether assets are substitutable or in irrelevance words, whether competitors have a dynamic duplicate.

Although the resource allocation view is averagely determined to describe competitive heterogeneity among businesses the concept can also be applied in the approach area (Lye, K. and Wing J., 2005); (Roy, S.Ellis, C., Shiva, S, 2010); (Berry, R. and Ephremides, A. 2009). The
core argument is that approach assembly is affected by a company’s direction to accept or achieve a competitive resource profile. In this mechanism, companies have attention to key actors’ resources to complete an best competitive resource features in which the amount of their security assets are amplified. According to (Martin G ,2009), the resource-allocation approach circumference can account for (1) the likelihood of approach assembly brought by company’s resource features, (2) a company’s preferences admiring the architectural features of the approach, as well as (3) approach activity through the effects of security resource alignments. We can think over facebook account hack by hacker. Cyber crime branch can trace the I.P. address of hacker but if there is no security for this then application will lose its popularity. Hence here we can consider resource allocation in terms of user, application, security provider, hacker as well as cyber crime officials. We can directly focus on these key actors as a part of hack and find game. Refer fig 2.1 for more clear idea about resources need to consider.

![Figure 3.1: Resources participants in social networking application](image)

Within the common resource rationale, a distinction is frequently acted between assets as well as abilities (Rubinstein, Ariel , 1991), which agrees to the types of tangible as well as intangible domains. Tangible revenues are, for prototype, constructions and development assets
like computers, along with manpower. Intangible resources or capabilities are non-physical as well as details based, alike as know-how, intelligent property rights, trade secrets, abbreviates along with authenticates, databases, information in the public domain, networks, as well as the culture of the organization. Another critical dissimilarity among tangible revenues along with aptitudes is their transferability as well as location-specificity. Scratchily discussing, abilities are additional location and person-related and more complicated to deliver any security aspects. Allocated that intangible resources are scarcer, harder to copy, and often requiring in direct alternates, these factors give the business in common the most competitive benefit.

Many security flows have been derived from the resource-allocation view. The security provision is like a stream as well as focuses on the role of capabilities. Another development of the resource rationale is the knowledge-representation view of the company’s security view. This stream of investigation known sure as it is an abnormal knowledge-bearing entity. Therefore, it is accepted that business form network security approaches to discover from their key actors’ abilities as well as information. How well a company can learns during hacker threats approach depends on its absorptive capacity, which applies to the ability of a company to acceptable knowledge brought through an proper security approach (Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V. 2010), Several analyzes have focused on the education aspect of approaches.

**Security Strategic theory**

**Security Strategic** conception additionally emphasis on the inferiority along with role of resources as matched to the object oriented resource-allocation view. A basic acquisition is that to capture a company’s activity, which is most important. In detail focus to the concept that activities consist of a bundle of assets, resource-dependency conception also believes that company’s security approach is depends on their willingness for input of resources, as well as interaction with the various network resources is due to hacker threats. In other words, company’s revenues are collaborative and are for development, marketing and also for asset security. These associations among social networking companies (Orkut, Facebook, Linkedin)
begin security power associations among them and their ideas for secure networking; coordinating these resource interdependencies are vital.

According to resource- **Strategic** concept, businesses have the two reasons for creating strategic approaches: to acquire secure approach than other company’s critical resources as well as to amplify market control regarding number of clients. With respect to the initial analysis, if domains are not secure, rigid to copy, rare, as well as not substitutable, they cannot be acquired easily through the market as well as hence approaches can be more difficult to achieve. In this way, key actors in an approach become mutually dependent on each other’s resources. Hence expect to acquire expedients extrinsically constructs interdependencies among web resources. This leads to the second reason for approach development; a company can choose resource-dependencies to amplify its efficiency in social networking area. On the one hand, approaches can be applied to gain benefits by controlling existing resources like operating system processes. On the other hand, approaches can be conducted to minimize threats to organizational autonomy as well as even minimize others’ attacks over application system. Here we can anatomies Facebook application as, either we can provide security checks like user location detection (so we can trace from where user accessing web application) or we can build game theoretical mathematics to get entries for all users.

A software business will not acquire all its security through external ways. A software business will focus on constructing an insufficient key capital internally along with will cooperate with others to gain access to additional co-active resources (Martin, 2009). In this way, a software business can guard itself from becoming an unessential player, which may happen if all its revenue become obsolete or are duplicated by other companies.

The difference among the resource-allocation view as well as resource-strategy conception is that the former focuses on inner assets; companies expect a profile of scarce along with essential (internal) resources to be competitive. As consulted above, dynamic approaches can be a behavior to achieve this. Although resource-strategy theory converges exclusively on resources that compulsory be acquired externally. In this way, approaches lead to resource-strategy structures as well as become a secure mechanism.
3.2.3 System security theory

The study is focused over security against external cyber attacks, it is important to analyze the basic theory behind this strategy. In resource-dependency concept, the focus is on the surroundings of the company is critical. Competitive strategy’ accounts the industry in which a company seeks as the key factor for analyzing the company’s application security. More specifically, the industry can be characterized by its competition through the underlying economic architectures out of which we focused on very specific security aspect. Amongst other substances, the number of competitors in a social networking software business is appropriate, as well as the amount of caliber entrants, clients, and service providers. The activity of a social networking software business is directed towards authorizing the balance of resources in the industry as well as improving its own competitive position.

Many authors have applied this rationale to describe approach assembly. According to the W3C, approaches are constructed due to social networking software businesses want to elaborate their competitive rank vis-à-vis their rivals. This does not only infer advancing a company’s own competitive position, but companies also aim at neutralizing or denying flows of competitors. Moreover, companies apply approaches to gain market power along with to increase their speed to networking market. The analytical affects display that activity indeed applies approaches to gain market access as well as authority the market structure.

3.2.4 Economic perspective

Network communication charge economic concept considers resource-allocation theories, as well as strategic activity theories are averagely characterized as additional economic mechanism to approaches. Strategic approaches are began for excuses of optimization along with efficiency; coupled to have the most efficient activity (networking cost economics), to optimize the competitiveness of a resource circumference (resource-allocation view), to accumulate expedients efficiently (resource-strategy theory), or to have the best dynamic position (dynamic behavior theory). However, to get the rationale of approach assembly, such calculative cost-benefit analyses are deficient. As already partially described in the section on resource-strategy theory, many factors play a role in approach assembly. Beside the role of command as well as
system security efficiency (resource-strategy theory), other applicable attempts include reputation, trust, as well as social networks. Together, not only economic approximations are acquired into account when describing approaches, but also more social as well as relational ones. Therefore, as a conclusive stream of analysis, placed in the more sociological tradition, I will discuss the economic perspective along with social network perspective on approaches.

In common, attention for coordination has grown according to this perspective; a relationship among key actors amplifies, augments, deteriorates, as well as is circumstantially closed through duplicate relational interactions. These relational activities are not subject to accurate clarifying, but rather serve as a feel of liability to the approach (Shoham, Y., Powers, R., and Grenager, T., 2007); (Kearns, M. and Singh, S., 2002) Approach components are not only centralized on economic gains as well as domains, but are also aware that relational factors such as trust along with commitment to application users are applicable.

This perspective is below directed towards explaining a rationale behind approach assembly, but rather on (relational) factors that contribute to the activity of an approach. "Game Theory (Stanford Encyclopedia of Philosophy)" describes that relational caliber helps coupled as the input along with output of an approach. As input, relational quality helps to construct the approach accomplished; it helps as an antecedent for approach activity. Nevertheless, one can also consider the level of relational quality as allocation for output. How accomplished was the approach; did the key actors have a good relationship? We need to dry-code pseudocode for analysis with game theory. The sample dry code for single user suspicious hacker is in figure 2.2.

**Main Procedure Cyber_Game**

- **Hand out each player's initial IPAddress.**
- **Decide which player is online.**
- **Repeat**
  - **Call Procedure Cyber_Move for next player.**
  - **Decide if this player must drop out.**
- **Until all key actors except one have dropped out.**
- **Declare the surviving player to be the winner.**

**Procedure Hacker_Move**
Begin one's move.

Throw the connection.

Capture suspicious move like sql injection.

If the token landed on "Catch IPAddress of hacker,"
then go there immediately.

Else if the token landed on "first time visitor"
then email verification and follow its instructions.

Else

follow the usual rules for the Facebook (post comment, share, tag photo, etc.).

End one's move.

A critical element of the exchange in approaches which affects approach activity is faith. Trust refers to the expectations that key actors have on each other’s behavior, such that key actors will be for simulation expectant along with non-opportunistic. A various way of phrasing this is to say that trust intimates the choice to rely on the approach partner, by approving one’s faith to be determined by the other. A common discovering in approach analyzes is that accomplished approaches exhibit trust, while failed approaches need aspire (Salant, Stephen W., Sheldon Switzer, 1983); (Rabin, Matthew, 1994). As trust has to construct between key actors, it can account for approach activity, but to a below amplitude for approach formation. It is however accepted that trust performs a role in repetitive approach formation among companies. In other words, if businesses have subsequently been engaged in approaches along with built up trust, this might affect their future inter-organizational behavior. In this way, trust might describe social networking business decision.

When analyzing the social security between social networking application businesses, one can also choose the security grade of a network of businesses instead of the level of the approach as well as its members. This perspective is chosen in social network theory of approaches. The network application answers the interactive factors of the internet market. An establishment consists of a set of companies approximately adhered to one another. These associations form a social network and shape the business as well as its approaches. More
definitely, the social security of a company or client affects its popularity as well as usability. Menon allocates many examples of the role of a network. A social network allows businesses to determine new approach opportunities, as well as hence the network influences how often along with whom approaches are formed. Additionally if two companies form an approach, their position as well as proximity in the network may detect the type of governance decided. In contrast to the previous theoretical approaches outlined, the social network approach is less concentrated on describing the formation of approaches. It rather serves as an approach or mechanism for mapping the network of relations of a service provider company.

3.2.5 A game theoretical perspective on approaches

Roy admitted in 2010 that, “game theory has oddly been conducted in a domain where it could naturally be (business strategy decisions)” (Sagduy Y, et al 2009) This section displays an overview of the contributions in the area of approaches which have so far chosen a game theoretical approach.

To characterize compactly game conception, it is described as a mathematical calculation access to social interactions. Although game theory consists of many asymmetric connections each with its own dissimilar assumptions along with theories, there is an average rationale basic the concept. It is important that key actors are believed to be unitary actors who act so that they maximize their benefit. The outcome of an interaction between key actors is however determined by the alternatives brought by all entering key actors in the collaboration, which constructs them interdependent. Hence, to maximize its usefulness a player also acquires the decisions of the other key actors in the game into describe. Many various conceptions have been built on this basis. One common element in these theories is their architecture; game theory predicts under which conditions there is a certain acquisition.

In definite, one division into couplings of game theory is significant for this analysis: the non-cooperative conjunction as well as the cooperative branch. In the dissociable branch, key actors deal with the task of choosing an agenda without being able to make cohering acceptances. Here, concurrence is seen as one between many approaches from which key actors can determine. In essence, it is under analysis below which clauses key actors have the incentive
to decide the tactics (role can be security provider, hacker or end user). Dynamic games are a part of this non-cooperative junction.

In the tactical concept, key actors can prepare binding agreements. Actually, the basic assumption is those key actors cooperate since the games are designed to make cooperation enticing. The set of key actors in such games consist of more than two key actors (n-player games). Given this, the challenge is which decisions will appearance from the set of n key actors as well as how the decision members will distribute the bonuses of the decision. To determine these queries, decision theories have been formed.

Further, each observation has its own accumulations concerning what kind of choices the key actors have. These vary from acquiring the maximum payoff to rationally allocating power, abducting policy aims, or teaming up with determined associates. A more complete along with in-depth conference of game theory is exposed in the further two chapters.

In conflict to the perspectives described above which all have constructed towards a quite cohesive rationale for approaches along with method of company approaches, the role of game theory in approach analysis has been much below uniform. Instead of one cohering rationale for approach assembly, researchers choosing a game theoretical perspective have performed on autonomous aspects of approach formation with certain games as well as models from game theory. More differently, two groups of analyzes can be discerned in game theoretical composition on approaches.

The first collection of components is combined by (Chi Zhang and Jinyuan Sun, 2010), which all analyzed approach buildup strategies. These studies display the role of the competition in the market, the arrangement along with exclusiveness of approach assembly, as well as game theory for liner forwarding approaches. Part of those studies adapts same theory.

The second group of studies concentrates on the activity of key actors during the approach. Those examines consider an approach as a strategic game with commitment along with opportunism as a social dilemma and the research with a closing option as well as blends the social dilemma with approach activity (Seema V. Lathkar; U.B. Jangam, 2013). While this second group is quite congruous in theme as well as social dilemma converge, the first group is
additional diverse in theory determination as well as rationale for approach formation. The following two sections give an abstract of both groups of analyzes.

**Mathematical logic build-up & Game theory implementation approach**

To examine the assembly of approaches, (Chi Zhang and Jinyuan Sun, 2010) focus on the choice of a company to enter an approach from the perspective that this choice is acquired to be initially based on the competitive causes in the social networking market. They therefore choose a dynamic game form allocating along with actual simulations. For the choice of companies to set up an approach, Chi Zhang and Jinyuan Sun oppose a sole central cost-benefit application, but solution analyzing the behavior of the other benefits in the information technology industry. Such competitive dynamics are, for prototype, started competition in the industry brought by approach construction along with the caliber degradation for a company which does not participate in an approach. This describes why the model of Chi Zhang and Jinyuan Sun predicts that weak companies are more likely to form approaches despite little gains. If companies in the industry form approaches, the competitive pressures for the others will increase and they will therefore feasibly decrease if they do not co-operate in an approach.

Weimin found diversity in approach construction in the industry, but also found that many of these approaches had to reorganize along with acquisitions among businesses from various approaches which destabilized the approaches. Their goal is to apply cooperative game theory to analyze the assembly of these approaches. The analysis although does not put any additional views than clarifying the concept of cooperative games along with displaying couple of scenarios. Since no existing exercise or analytical approvals take place, their conclusions are bordered to the concept that the liner social networking market is well clarified by the core acquisition. The core solution is a conventional behavior to discriminate among the frequent solutions in a cooperative game as well as is clarified further.

The most formal approach is determined in Chang, H. and (Atallah, M.J., 2001) which relates the software security with mathematical implementation. His formal analysis examines two extreme kinds of cooperation: on the one which have the positive externalities on businesses outside the acceptance as well as which might persevere from free-riding, along with on the other
hand cost-reducing approach which has the negative externalities for non-members. Serene considers variations in group of those two extreme forms in his prototypes. By analyzing desired procedure of companies in those two asymmetric types of cooperation below different clauses, accounts on a more regular level can be drawn.

A first follower of Serene is that accompanying assembly of controls to a cohesive collection of members. Concurrent assortment refers to conceiving the cooperation at once with all members, while in arranged formation the group forms additionally; businesses can merge later. For trial, this sequential order of formation directs to adaptable trials as every company has the impulse to free-ride on the decision of other trial-members. Non-members can advantage from the externalities from such trials. However, if formation is coincident, the decision to associate has to be acquired before one perceives if the trial will positively form (enough members) as well as before one knows whether the externalities can be abused.

For cost-reducing approaches, an important factor behaves to be the broadness or exclusivity of the approach. An open membership means everyone can join (can open account to facebook), as matched to additional exclusive approach which can excludes companies. Serene accepts that open membership of cost-reducing approaches controls to efficient approaches, while confidential membership leads to multiple curtailed, inefficient approaches which compete with each other. A final conclusion is that the level of cooperation is desired to be higher when negotiations are bilateral.

**Game theoretical perspective: behavior of key actors during the approach**

A second theme which has been dealt with in game theoretical approach research is the evolution of the approach and more specifically, the behavior of key actors during the approach and the consequences of this individual micro behavior on the macro level of the approach. Once an approach has set off, each company wants to achieve the potential value of the approach by committing to the approach necessary condition for approach success. However, the benefits of the approach are shared by its members, so each member will have a strong incentive to compete for a large portion of the benefits. In short, companies face a dilemma between commitment and opportunism. Such a dilemma is modeled with a strategic game form. Each company has the
incentive to be opportunist and behave in a non-loyal and self-interested way, but if all companies lack commitment by not contributing to the value creation in the approach, a collectively undesired situation is the result. This structure of the dilemma between commitment and opportunism closely resembles the prisoner’s dilemma from game theory. Different authors have therefore modeled an approach with such a prisoner’s dilemma, a more general social dilemma or a public goods appeal. This dilemma is analyzed further in Section.

Figure 3.3: Initial situation and non-cooperative and cooperative solutions of the baseline model. Source: Online.

Few researchers focus on another aspect of company’s behavior during the approach: Live the approach. They argue that modeling an approach as a prisoner’s dilemma neglects the exit option that is available to key actors. They therefore propose a game in which approach key actors have three strategies at their disposal: commitment, opportunism, and exiting. In the (Wing J et al. article, 2005), a computer program and simulations, in combination with theoretical insights, show how key actors should behave when both high and low payoffs exist for exiting. When the payoff for exiting (that is, the reward for leaving) is relative high compared to the other payoffs in the game, the incentive to leave the approach is great. In that case, companies should be intolerant of misbehavior on the part of their partner. Approach termination will already take place after a small number of occasions of opportunism. If, by contrast, the payoff for leaving is low, companies should be more tolerant since the benefits of the approach may
exceed the benefits of exiting. Approach termination is only to be expected after a series of problems has occurred.

The final theme addressed is approach performance. (Wing, 2005) uses game theory to study the performance of approaches, and relates the individual behavior of key actors as studied in a social dilemma to the collective level of the approach. He defines performance as the degree to which companies fulfill their strategic needs and attain indirect, spill-over effects from the approach. In his study (2005), empirical results show support for the idea from game theory that a long time horizon promotes reciprocal cooperation.

Additionally the expected association among considered opportunism by key actors along with approach activity was indeed accepted by the data. In a second study, (Wing, 2005) finds support for a correlation among game academic configuration along with approach behavior. Here, however, Wing defines game theoretical structure as the model of payoff, a long shadow of the future, along with the number of key actors, based again on the prisoner’s dilemma. In line with the articles that study the balance of cooperation along with competition, Wing shows the link among this balance along with approach performance. Finally, Wing can accompany the role of game theory, but also answers that game theory alone cannot “... capture the rich complication of real-world strategic approaches”.

3.3 Lagging points of research on approaches

In this section, the facts of the perspectives already consulted will be matched and, in this way, many analysis gaps will be defined. The concepts will be paralleled on three issues: their level of research, the nature of the conceptions (i.e. domain of companies), as well as what the conceptions aim to clarify. It is accepted that more gaps in the approach literature exist, but these will not be consulted in this study. It has been chosen to focus on three issues to be able to zoom
in as well as really deal with those gaps. Those specific three issues have been determined as they are considered the most important differences among the conventional theoretical perspectives and game theory. With this similarity and the derived analysis gaps, it is shown what game theory can contribute. The defined investigation gaps are an experiment agenda for the simulation chapters.

3.3.1 Depth of analysis

The starting major variation among the theoretical perspectives is the grade of analysis determined. To attain a collective picture of phenomena, it is beneficial to adapt many types of analysis. Approaches have also been examined with different levels of experiment. The resource-allocation rationale clashes on the level of the company. By choosing the resource profile of a company profile, as well as reasoning from this configuration, approaches are set up according to resource needs along with dependency connections. Network communication cost economics chooses the level of the network communication. It is conflicted which approach is accounted most efficient for a network communication. The strategic activity perspective analyzes the company relative to its circumstance. The key thing is to aim at the best competitive establishes relative to competitors. Finally, the relational approach also studies companies in approaches relative to their environment. Here, the relations between companies in an approach or the whole network around a company (social network theory) are key factors. Together, several conceptions apply the company as level of analysis, while other theories take the company and its relations as their starting point. The arguments are all made by taking the company as focal point; why do companies form strategic approaches and what is the role of a company’s social circumstance?

However, what the total affect of an interaction between detached companies are, persists understudied. The collective result of an interaction refers to the aggregated level, also identified the macro or multi-actor level. So far, the focus has been on the impulse of separate companies, but not what occurs if these companies start collaborating with one another. Can all companies in an industry achieve their approach motivation goals? Given the decisions of companies, how can a detachment of companies across approaches be determined that fills all companies?
Approaches are the affect of interactions between companies. Hence it is natural to pay alertness to businesses, as they are the conceiving blocks of the collaboration. Such theory has although neglected acquiring these constructing blocks to analyze the collective level; the result of the interaction. For multi-user approaches definitely this interaction can be complicated. Because of the issue of interaction between businesses which are creating along with controlling an approach merits attention.

**Lagging point 3.1** Approach have not allotted consequential strategies to interaction among businesses when constructing along with controlling approaches.

Adding the level of key actors as collective level to prototype the result of their collaboration is the core architecture of game theory. More definitely, in game theory, all key actors’ actions together control to a common affect, which allots each key actor to change their approach to manage this result? Similarly, from such a game perspective anyone can reason from the collective level and analyze how single key actor modifies this result.

With a game theoretical application, one can analyzes how rationale autonomous practice might control to collective irrational affects. Furthermore, game theory is efficient to deal with complication resulting from many key actors. Experiencing this complexity and discovering solutions to such interactions are one main task of game theory. The aim is to develop game solutions that appease a whole group of key actors irrespective of its size and to analyze under which clauses such an acquisition contains. Insights from game theory can therefore be applied to analyze the aggregated level of companies’ collaboration controlling to approach assembly, carefully in multi-user approaches.

**3.3.2 Mathematical Logic and Insight of Theory**

The other issue focusing on a difference among traditional approach and game theory is the insight of the theory. The more conventional approach perspectives are theories with a general rational. This means that the resource allocation views and resource utilization theory explain the activity of a company via its resources. Network communication cost economics argues that all behavior of companies is described through reasons of efficiency. Dynamic
behavior theory focuses on at cost locations. Entirely the relational perspective analyzes that relational factors matter. In other words, those theories offer general ideas on approach assembly and approach activity. These regular concepts can of course be applied to arrive at more singular propositions, to empirically test the ideas. These theories are mainly applied to discover and analytically cyber-laws of business.

In contrast, game theory has a different focus. Game theory is capable of making concrete predictions and, more specifically, of showing under which conditions which results will occur. As seen in previous section, game theory in approach research has so far mainly shown the conditions under which a committed strategy may be more rewarding than opportunistic behavior in an approach. In other words, game theory is more aimed at making predictions or forecasting a result, given certain conditions. Although one could argue that the more traditional theories also work with assumptions and conditions under which the theory holds, the main differences between game theory and more traditional approaches are the degree to which these conditions are being made explicit and the number of conditions underlying the theory. Game theory can be distinguished through its transparency concerning conditions and the relatively large numbers of conditions. Although general laws and regularities can also result from game theory, these only hold under a quite large set of conditions which are made explicit in the theory.

These kinds of predictions are related to the more formal, deductive, and abstract nature of game theory as compared to the other theoretical approaches. First, game theory adopts a more formal and deductive approach to the study of social phenomena. The theory arrives at hypotheses, propositions, and conclusions by deductive reasoning and carefully building a theory as a set of primitive terms, definitions, axioms, and theorems (axiomatic method). This is a different approach than the other theoretical perspectives on approaches. These theories are not built according to the axiomatic system and are less formal. Furthermore, game theory is able to abstract complex situations by neglecting details and identifying the essentials of such a situation. Instead of trying to give a complete explanation (almost a description), game theory reduces and focuses.

When considering the research aims defined in this section and previous section, an approach that abstracts from description and aims at many necessary factors are considered. The
issues on the research agenda are complex and have received little theoretical attention. As will be seen previously, the cyber game approaches has received relatively much attention from more popular management literature. In other words, given this set of more descriptive studies, there is rather a need for a theory that, even more than other theories, aims at grasping the essentials of the object of study by neglecting details. (Shoham, Y and Powers, R., 2007) also argue that game theory is therefore better equipped to handle the complexity of the world of business than other approaches. Besides these advantages, it would also enrich and mature the study of approaches if a more formal approach were to be developed. Such a formal approach is currently lacking the field.

3.3.3 Overview of theories

Finally a difference among the concepts is what they describe. In the more economic concepts, such as activity charge economics, resource considerations, along with strategic activity theory, the emphasis is on the rationale behind approach assembly. The conceptions clarify under which clauses the advantages of approaches outweigh the disadvantages. Strategic approaches are set up if businesses can fulfill efficient network communications require for domains, can apply resources as power means, or achieve a competitive place. The resource-allocation view cannot only clarify why as well as when businesses form confederations but also an associate with a company to chooses along with the performance of the approach (Martin, 2009). The relational perspective is not directed towards describing why approaches are formed. Rather, it focuses on clarifying approach behavior. The social network appeal does not focus on why approaches are formed, but allows a more general behavior for mapping the environment and applications of a company. In this way, specimen can be clarified how accomplished approach is, or what kind of approach will be formed. Hence, the additional conventional approach considerations analyze why approaches are set up, below which occurrences they are valuable, which key actors to determine, and why approach achieve or fail.

A natural follow-up of the information about why businesses set up approaches along with why some approaches are more beneficial is the question ‘How are approaches developed?’ and Which process is appropriate?. It is relevant to discover more about the mechanism of
approach construction, because information about why approaches are formed along with why some approaches are more advantageous will become more essential if one also knows how to accomplish as well as form such approaches. As a comparison, it is essential to know why any absolute company is making profit, why certain people are healthier than others, along with why some cows give more milk. However, educated how to develop such a high profit, how to fitted more healthy, along with how to acquire more resourceful cows are even more useful. Supplemental term, the ‘how’ knowledge is highly related to the efficiency as well as behavior issues. One could even consider ‘knowing how’ as the next step after ‘knowing why’. Moreover, it seems natural to study approaches in an active way due to approaches take time to be set-up along with inconclusively broken, along with might exist for many years. Approaches are not static, but are the affect of a mechanism in which cooperation is formed, evolves, and is closed. This process also affects the behavior of the approach (Lye, K. and Wing J., 2005); (Alpcan T. and Baser T., 2006).

From the key of the art of approach concepts, it can be assumed that approach conception has not paid much alertness to the ‘how’ issue. I therefore introduce the following analysis gap:

**Lagging point 3.2** Approach compositions has not paid consequential concentration to the mechanism that leads to approach assembly.

Examining how approaches are developed assigns to the dynamics of approaches. Generally discussing, the cyber game approaches are appraised to be understudied. No collective and complete theoretical architecture work on these dynamics has been conceived yet. To review cautiously what the analysis gaps in this area are, I will first present an overview of examines on the basic architecture of approaches in the next section. Moreover, I will argue what game theory can help to these investigation gaps.

**3.4 Literature review: Mathematical Game Theory Logic**

However most analyzes on approaches adapt a static perspective (it has become more average to consider an approach as an active process). This section reviews a determination of
those additional dynamic approach examines. Based on this review, in previous sections, the analysis gaps in this domain of research will be displayed.

In this examine, the design of dynamics assigns modulates that take place within a software system (Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu, Q., 2010), more definitely, approaches between companies. The task at hand is to characterize as well as remove the behavior of and within approaches in arrange to be more definite about the evolution of an approach. What causes this motion to continue? What affects the mechanism? Although time is infinitely divisible (Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu, Q., 2010), I adapt a division of duration into periods since “... very compact time-steps give a good approximation to a continual liquid time” (Game Theory, Stanford University). In this way, the arrangement of different stages of a process can be examined. Why do modulate take place, what boosts them? In other words, responses are found for the dynamics.

Hence the activity is to focuses on motion of and within approaches. I will divide the discussion of the composition on the cyber game approaches into two parts:

• Lift cycle of approach.

• Multi-user approach.

The beginning kind of dynamics refers to the conversions of the game approach from approach generation, evolution, along with completely termination. The second game approach shows dynamics that take place within the approach between key actors. These variations in the two kinds of dynamics are in line with the seminal behavior (Basar, Tamer, et al., 1995) They examine the dynamics of inter organizational associations as repetitive areas of negotiation, contract, along with actions. This cycle is coherent many times during the assembly, management, as well as termination of the game approach life cycle.
3.4.1 Game Life Cycle

The game life cycle approach accounts an approach as an abnormal as well as predictable arrangement of key roles like hacker, system or end user. Different categories of approach phases have been consulted in the literature (Martin, 2009).

Based on collected references the following category has been chosen in this analyze:

• Building Game

• Management of Game

• Termination of Game

Assessing the strategic game approach literature, game development has been compensated more as the question of why games are set up than as how they are set up. The analyses mentioned here are exceptions to this. In general, game approaches for cyber security are accounted to start with arrangements at the level of the company. Companies envision a benefit that can only be captured through a key actor ship. Businesses can have different strategic excuses for beginning a key actor ship, and these have been implemented expansively in approach literature. After companies have internally accounted expect to form an approach, the key actor selection phase takes place. Companies look for caliber key actors who meet their expected needs. Companies direction at approaches that lead to a strategic fit, but key actors also strive for, amongst others, cultural, organizational, as well as confidential fit.

The development phases at business level are accomplished by negotiations between activities. These negotiations can again be broken into two phases: agreement on the requirement of the various securities as well as agreement within the group of factors about the specifications of the cyber security approach. During the addition type of negotiations, key actors have to except on a multitude of approaches. Examples are the organization form as well as business prototype of the approach, technological patterns, as well as the number of investments each partner will construct. Via investments, companies develop a formal commitment to the approach in clauses of financial, human, and physical along with intelligent assets (Alpcan T. and Baser T., 2006).
Once the formal negotiations have accomplished as well as assistants beginning developing investments, the approach sets off as well as inputs the management phase. The development starts, employees are selected for module development and money will flow from key actors to the cyber security upgrade.

The main task in this phase is to control the game approach. Game approach commanders should keep approach building up to hopes as well as monitor the approach output. Also, security authorities have to adapt to both external along with internal pressures on the implementation feasibility of approach (Alpcan T. and Baser T., 2006) This evolution phase is often analyzed as the phase in which the key actors truly begin to interact. In that sense, one could consider the system behavior, the subject of the consequent section, as the events in the evolution phase. However, this view ignores that security dynamics take place over the complete life of the approach; key actors also cooperate during negotiations as well as termination phases.

The closing phase of game approaches is end of process life cycle. As mentioned earlier, approach termination only infers approach downfall if the termination is premature along with key actors (O.S. Processes) also perceive it as in similar way (Martin ,2009). If an approach was object-oriented and the task was achieved to the fullness of all key actors, termination might be a feasible as well as non-problematic last stage of the approach. But most often, approach can be problematic too and may relate with pain and distress.

Review on the complete phase of approaches focuses on why game approaches collapse in some circumstances. Although learned why game fail is valuable knowledge, it says little about the mechanism the game goes through. Additionally although the issue of game failure is an ongoing throughout the approach, it can better be seen as the outcome of an approach also can therefore be established as a post-termination phase. So, if we want to get a beneficial insight into the gravity of the approach we need to know how approach termination takes place. The discipline of game termination has acquired little attention in the approach composition.

An exception to these there are few articles that posts how approaches evolve before they are closed: (Hansen ,2004). The article by Denny clarifies the way to approach when appear and how key actors can assistance the approach. During the game approach, an ongoing assessment is acted concerning whether the game is still meeting the requirements of the application key
actors. An expectation shortfall can be the forewarning of approach termination as it is apt to trigger partner activities. For assessment aim, it is relevant whether the key actor’s attribute the shortfall to external events or to internal arrangements involving operating system firewall behavior. External events refer to common users or hackers as well as surrounding factors, and internal conditions for example the perception of balanced donation as well as the pace of bilateral information. Furthermore, do key actors’ plan the deficit as an efficiency or shortfall? (Hansen, 2004) work out four types of acknowledgments to contemplation shortfall combing these two approaches. The possibilities of approach closure are higher when the conceived discontinuity is of an equity nature (Hansen, 2004). If companies have considered terminating the association, the next types are the public disclosure of the failure (hacker attack) as well as conforming division activities (Dasgupta, 2010).

The discussion of the life cycle approach has so far explained one life cycle: cyber security game evolve from start-up, game management and game termination. However an approach along with its members also passed before the approach is conceived. The extent to which this shared game approach key actors authorize their activity within the game is suitable in this context. Several studies examine the authority of previous relations between key actors on game activity. A critical discovery is that key actors, who are familiar with one another from earlier relations, might be less prone to opportunism within an approach. (Dasgupta, 2010) for example find strong empirical experimentation for their hypotheses that a prior history of web business connections between peers within a game leads to a greater effectiveness of the connection. It might be easier to refrain from opportunistic along with selfish flows if a system perceives its processes better as well as can even trust him. (Myerson, 2013) also finds that a prior history among key actors in an approach perceived opportunism. Even if there has not been any relationship in the past, the fame of a partner might play a role. Few researchers argue that, the reputation of a software company might play a critical role in identifying the willingness of others to cooperate. Dasgupta also constructs the link between web business reputations along with opportunistic activity. According to other reviews, reputation has indeed assured to play a role for businesses as well as for game background formation.
3.4.2 Roles of Key Actors

In addition to the study of the life cycle, game approach also challenges system security during its daily operating system booting. These security threats assign to the level of the key actors in the approach. (Gintis ,2009) consider an organizational security as “… a mechanism that is consistently monitored as well as protected by the activities along with analyses of individual user visiting web application” and the relation is “… likely to emerge increasingly with small businesses …”.

During the life cycle of the game approach, game security approach companions cooperate coherently. During those interactions, key actors monitor each others’ performance as well as events occurring. The role of key actors is to coherently observe, discover, as well as behave securely during an attack. In other words, the key actors appear in ongoing assessment of the game strategies as well as its system environment. After such assessment, key actors may want to act to restore a checked imbalance of the relationship. Web application cannot always expect whether their activities will have a positive or negative effect. The adjustment of web applications over time affects to associate among the company, its circumstance, as well as the approach (Hansen, E.A. and Bernstein, D.S. and Zilberstein, S. ,2004 ). Considered in this way, game approach for web security provision is an understanding cycle in which companies coherently adjust their activity along the way. One may call this adjusting behavior command among key actors.

Couple of clauses like external hacker attack possibility plays a role in this mechanism. I will first consult the internal clauses, as well as then concisely referral the role of external outcomes. According to (Castro and Costa ,2006) an approach is characterized as a set of internal charges which certify the internal system of the strategy. A review of much literature specifies the following list of internal conditions:

• Operating System Firewall Protection

• Web application usability

• Internal User Security provision

• SQL Injection kind of security
In addition, other internal factors which might perform a role are, web communication, learning of key actors and adopting wrong use of system. I concentrate on the four points mentioned above in further chapters.

Such factors may affect the stability of game. A need of operating system firewall protection, too much or too little web application usability, unequal internal user security provision, or an uneven SQL injection security all may command to a lack of constancy within the game approach. As a consequence, game key actors will celebrate these circumstances cautiously along with may want to try to adjust them during their life cycle. As cyber game for security has already been consulted capacious in Section 4.2.4, I will focus here on web application usability, internal user security provision, and SQL injection security.

Web application usability assigns to the adaptive masteries of companies. As clashed above, the game is a discovering duration that key actor’s behavior. Each user checks, realizes, along with behaves in order to improve the asset of internal charges as well as external events. Nevertheless, too much extensibility controls to a lack of hardness as a lack of attaching mechanisms, a weak security configuration, as well as too little irreversible commitment, as well as vice versa. Hence, the level of adaptability chose by a partner should be corrected.

The equality and contract along with opportunum is critical in game building, since this equivalence can also degrade the consistency of approach (Chang, H. and Atallah, M.J., 2001) Attempted businesses act in similar way that they pursue mutual interests as well as average benefits of the game approach. Opposite behavior is opportunum, in which key actors only act in their own interest as per predefined software code strategy with others (Ganzfried, S. and Sandholm, T., 2009). Again, these both actions should be compensated; too much opportunum controls to approach failure, along with too much commitment by a one process directs to free-riding by the other process (starvation condition of operating system process-one process will wait for finishing of tasks by others). As seen in 3.2.5, this equality has often been examined with a game-theoretical perspective.

A decisive internal factor inspected to be critical in the process dynamics of game approaches is the match of efforts within game (Hansen, E.A. and Bernstein, D.S. and Zilberstein, S., 2004); (Hu, J. and Wellman, M. ,2003); (Wu, Q., Shiva, S., Roy, S., Ellis, C., and
Datla, V. 2010). Filar write: “... most web alterations arise due to asymmetry in the user intension association ...”. Intension refers to the acreage to which a user is affiliated on the approach, the number of decisions a user has the outside the approach, as well as the subordination of the approach on the user. In this way, each company within an approach has a clear idea of application (like Facebook is for advertisement, social hub etc.), which certifies the balance of usability within game approach. On uninterrupted sequence, this balance of usability can be more identically detached or the usability balance can be asymmetrical with one or more common users. During the approach, both central constructions and external constituents can influence the balance of usability. In short symmetric usability alikeness is more likely to direct to a consistent approach.

Besides these internal problems, the dynamics among key actors are also affected by external circumstances. External events assign to events relevant for the complete game approach or one of its key actors. In game approach, a partner adopts to changes in the circumstance as well as to the game approach context of the company. These external events are alert for the hasty changes during game approach causing them unpredictable. The external events also make approaches below controllable.

3.4.3 Proposed Plan

I will now plan conclusions concerning the composition on the game approaches as well as set up of several topics on the analysis agenda. Further I will display what the role of game conception can be for the described research orientation with respect to cyber securities for social networking. In the inspection, coupled different approaches to the cyber game approaches have been differentiated: the cyber game approaches as well as the approaches within operating system process evaluation.

In common, the cyber game approaches with a life cycle application have acquired additional attention in popular business literature (Lye, K. and Wing J., 2005) than in scientific literature. The academic perspectives displayed earlier do not play any role in this argument. Hence, one can except that in average too few scientific examines have researched the discipline of approach formation (Roy, S.Ellis, C., Shiva, S.,2010);( Berry, R. and Ephremides, A., 2009).
This was also explained in previous section. The main conventional approach perspectives have not examined how an approach is developed.

Concentrating on phases within the life cycle, the second phase, cyber game approach, is a subject that has acquired quite some attention in bookish literature (Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V., 2010). However, scientific analyzes on the first as well as last phase are insufficient. The challenge concerning why approaches are constructed and ended is much more documented than how they are formed as well as closed.

To further formulate consideration on the cyber game approaches, this study concentrates on the cyber game approach execution, thereby neglecting the cyber game closure. The capacity of that is that game conception is beneficial equipped for analyzing the process of approach formation. This does not mean that the closure phase is accounted of less criticality; it directly does not get the concentrate here. For this stage of approach formation, the following explores remain unanswered. What the securities are at performing during approach formation? More definitely, consider the following arrangements: How does game determine key players? What is the procedure of key player decision that cyber game go through? How can allowances be reached in approach negotiations? What is the role of various ways of conceiving an approach?

It is conflicted that cyber game concept should be brilliant of analyzing the mechanism of approach establishment, more than or at least in a various way than the other approach appeals also implementation approach for decision making. As will be seen in Chapter 4 on decision theory, game theory encloses frequent concepts clarifying the development of decisions. Part of these concepts is dynamic. The non-dynamic decision designs are also favorable as they centrality more than the approach applications on how cooperation arises, as well as can be exercised for further theory as well as simulation construction. Since decision concepts were not arranged definitely for the area of approaches, there will be a need for further sample constructing so that the theories can apply to the area of approaches. In brief, the decision junction of cyber game theory attempts many static and dynamic concepts which can be exercised as beginning point for further establishment of active approach models. An additional reason to apply decision conception is that many researchers consider this connection to be additional appropriate to business than non-cooperative game conception (Wu, Q., Shiva, S.,
Roy, S., Ellis, C., and Datla, V., 2010). As described earlier, game theory is more directed at rationalizing, thereby complementing the descriptive formulation.

In addition, many approaches also have a phase ‘alpha; the phase that leads an approach. Many articles have inspected the affect of previous connections on opportunism, as well as others have shown that reputation might play a role (Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu, Q., 2010); (Shoham, Y., Powers, R., and Grenager, T., 2007.) Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V., 2010); (Myerson, Roger B. *Game theory: analysis of conflict*, 2013). However, the consequence of previous interactions might be inspected more in depth acquiring other affects into account. Not much is known on what authority passed interactions may have on behavior of key players within an approach. Do key actors act unequally if they have cooperated before? In brief:

**Lagging point 3.3** Approach study have not paid critical alertness to the affect of interactions between key actors before an approach on their activity during the cyber security game approach.

The second type of cyber game approach in the examination is the relation between the key players of the approach. The composition on this kind of approaches has become quite cohesive along with extensive over the decade. There is formulation on many circumstances of the internal equality. New directions of analysis will expect to lead to security aspect of these game models. For ideal approach study we need to know, what is the affect of a compression in security during an approach on the three other issues? Will less security control to more cyber attacks? Or, what is the consequence of random approach on the commitment of key actors? To sum up, these intrinsic approaches have been extensively certified, but approach assessment of the affects of their evolution is needed. We can conclude this like:

**Lagging point 3.4** The cyber security is a new concept and need to analyze with consideration of key actors in game.

To implement this analysis aim, I will apply the approach of cyber security games, a partition of non-cooperative game concept. In cyber security games, key actors cannot make annexing arrangements along with the result of the interaction is dependent on the determination of each autonomous player. The non-cooperative coupling is sometimes called object oriented
game conception [40] due to of the focus on key actors’ agent as denotes to reach an outcome. Game approaches are a way to monitor the activities or behavior of key actors. Additionally in contrast to cooperative game theory, it is not compulsorily on cooperation, but on behavior of actors in any kind of interaction. Here, the approach, as the collaboration between key actors sharing in, is further analyzed. The issue is not who will build an approach, but rather how key actors in an approach behave. The affect of the interaction is conditional on the brittle balance among key actor’s activity. Recall that appropriates issues of behavior is security, flexibility, and secures output, amongst others. In such circumstances, no chief authority maintains the interaction, nor do formal binding agreements play a role (Basar, Tamer, et al., 1995). Therefore, to model such activities, the theory of cyber security games is the best choice as binding agreements are not taken into account, but the focus is on analysis checklist. Additionally affecting approach of games to study key actors behavior is in line with early analysis. Finally, since the dynamics of strategic games are well-developed, it is easy to build active standards. Cyber security games as well as their approaches are consulted in Chapter 4.

For the sake of collectivity, it should additionally be mentioned that the back-and-forth among the two types of approaches has been understudied. Applicable challenges would be whether key actor approaches differ in subsequent stages of the approach as well as how events during the life cycle affect on key actors roles. However, tackling this lagging analysis points is beyond the scope of this analyze.

3.5 Conclusion

This chapter has focused two aims: to study the literature. What factors need in the composition on the cyber security approaches? These attempts have been denoted in four research lag points. Previously, the question is what a game and decision perspective on approaches can offer matched to other theoretical studies.

In this chapter, it has been conflicted that cyber security game concept can advance to the defined analysis. Conversations for this position were determined in the category of researches of cyber security theory. Game theory examines interactions by coupling the micro as well as macro grade. This perspective has needed approach composition so far. Furthermore,
game theory can analyze how approaches are developed as well as how key actors collaborate within approaches. Due to game theory is approaching to be accomplished to deal a more active perspective on approach fabrication along with approach key actor activity. Both approaches have not acquired consequential attention in the literature so far. Additionally, the abstract approach of cyber security game theory is awaited to shed light on the complication of the game theory approaches. This should focus an additional descriptive application.

However from the overview on game academic examines on approaches (subsection 3.2.5) it can be concluded that common game concept has so far not helped expansively. Most approach analyzes applying a game theoretically has applied the no branch of game theory. The security games adapted have mainly been applied to check the activity of approach players during the approach. Those analyzes are conducted for the existing study area as well as will also be applied in this study to built new prototypes.

Although based on the reviews, I can say that the generation of approaches along with the procedure controlling to formation are carefully understudied in approach analysis. How approaches are formed has not acquired considerable attention in scientific composition. Determining a game perspective, approach assembly can best be analyzed with decision theory which possesses a classic set of tools along with theories for examining approach formation. Furthermore, game conception can offer many applications of active decision concepts.

Due to the eventual of a game deployment to approaches lies in studying the mechanism of approach assortment with a decision concept. Till date no researcher has focused over cyber security yet. In the Chapter 6, I will explain this concept.